GENILDA OLIVEIRA DE ARAUJO

LOTTUSEG: UM PROTOCOLO SEGURO PARA LOTERIA DIGITAL

FLORIANÓPOLIS

2003

UNIVERSIDADE FEDERAL DE SANTA CATARINA

PROGRAMA DE PÓS-GRADUAÇÃO
EM CIÊNCIA DA COMPUTAÇÃO

Genilda Oliveira de Araujo

LOTTUSEG: UM PROTOCOLO SEGURO PARA LOTERIA DIGITAL

Dissertação submetida à Universidade Federal de Santa Catarina
como parte dos requisitos para a obtenção do grau de mestre em Ciência da Computação.

Prof. Dr. Luiz Carlos Zancanella
(Orientador)

Florianópolis, Fevereiro de 2003

LOTTUSEG: UM PROTOCOLO SEGURO PARA LOTERIA DIGITAL

Genilda Oliveira de Araujo

Esta dissertação foi julgada adequada para obtenção do título de Mestre em Ciência da Computação, Área de Concentração em *Sistemas de Computação*, e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina.

Prof. Fernando Ostuni Gauthier, Dr.
Coordenador do Curso

Banca Examinadora:

Prof. Daniel Santana de Freitas, Dr.

Prof. Luiz Carlos Zancanella, Dr.
Orientador

Prof. Nelson Lopes Duarte Filho, Dr.

Prof. Ricardo Felipe Custódio, Dr.

Há homens que lutam um dia e são bons,
há outros que lutam um ano e são melhores,
há os que lutam muitos anos e são muito bons,
mas há os que lutam toda a vida e estes são imprescindíveis.
(Bertold Brecht)

A meus pais e irmãos.

Agradecimentos

Aos meus pais, Erivaldo e Geny, pelo apoio e incentivo dado desde o início, quando fazer mestrado era apenas um plano e Florianópolis uma ilha distante. Ao longo destes últimos dois anos, seu amor e carinho, apesar da distância, foram ingredientes essenciais para a realização de mais este sonho.

Aos meus irmãos, Daniela e Erivaldo Filho, dois grandes companheiros na jornada da vida.

Ao meu orientador, Luís Carlos Zancanella, por ter me acolhido tão bem desde o primeiro contato, contribuindo enormemente para que a idéia de fazer mestrado na Federal de Santa Catarina deixasse de ser apenas uma possibilidade e passasse a ser um objetivo. Sua orientação, incentivo e amizade foram fundamentais.

Aos professores Ricardo Felipe Custódio e Daniel Santana de Freitas, grandes mestres que encontrei ao longo desta caminhada.

Aos colegas de mestrado e a toda a equipe do LabSEC, que conviveram comigo não apenas na realização de atividades acadêmicas, mas também passaram a integrar meu dia a dia. Em especial, gostaria de agradecer à Adriana Notoya, cuja amizade e incentivo jamais serão esquecidos.

Aos amigos de São Luís, que mesmo à distância continuam fazendo parte da minha vida e comigo dividem mais esta vitória. Em especial, gostaria de agradecer à Andréa Garreto Ramos Pereira, pelo carinho, apoio e presença mais do que constantes.

Aos amigos de Florianópolis, que muito contribuíram para que surgisse em mim o desejo de permanecer morando nesta ilha maravilhosa. Em especial, gostaria de agradecer ao Sr. José Mário, a Neta, Carolina e André, que sempre foram minha família em Florianópolis.

Aos colegas da Directa Automação, por todo o incentivo que me foi dado na etapa final deste mestrado. Em especial, a Alexandre de Carlos Back, Miriam Inês Pauli De Rolt e Carlos Roberto De Rolt que acreditaram no meu trabalho e inicialmente me permitiram trabalhar em horário especial. Também gostaria de agradecer à Saraí Lusia Molin Lisowski, grande amiga e incentivadora.

Por fim, gostaria de agradecer a todos que, embora não tenham sido citados, contribuíram de alguma forma para a realização desta dissertação.

Sumário

Lista de Figuras

Resumo

Este trabalho apresenta uma proposta de protocolo criptográfico seguro para loteria digital, no qual redes de computadores como a Internet são usadas como infraestrutura para a realização rápida e eficiente de apostas. Este protocolo baseia-se na emissão de comprovantes de apostas digitais verificáveis, que asseguram ao apostador o direito de receber a premiação. Como base para esta proposta, são apresentados os principais requisitos funcionais e de segurança que precisam ser contemplados por uma loteria digital a fim de manter compatibilidade com o processo lotérico tradicional, cujas características e funcionamento básico são apresentados de modo sucinto. As principais alternativas tecnológicas para o desenvolvimento de aplicações seguras para Internet, bem como a fundamentação teórica em criptografia necessária para sua compreensão, também são descritas brevemente.

Palavras-chave: loteria digital, protocolos criptográficos, criptografia aplicada.

Abstract

This work presents a proposal of a secure cryptographic protocol for digital lottery, in which computer networks such as the Internet are used to provide the infrastructure for a fast and efficient betting process. This protocol is based on verifiable digital lottery tickets, which grant to the winner player the right to receive its prize. As base for this proposal, the functional and security requirements that should be fulfilled by a digital lottery in order to keep the compatibility with the traditional lottery process are presented. The technological alternatives for the development of secure Internet applications, as well as the cryptography theory necessary for its understanding, are also briefly described.

Keywords: digital lottery, cryptographic protocols, applied cryptography.

Capítulo 1

Introdução

A expansão da Internet revolucionou as telecomunicações tornando possível o acesso a pessoas, produtos, informações e serviços tanto em escala local quanto mundial. Como conseqüência, novas possibilidades de interações sociais e econômicas foram introduzidas em nossa sociedade.

Para o setor empresarial, a Internet propicia a integração de mercados em escala global, bem como facilita a comunicação com parceiros e clientes. Para instituições governamentais, pode representar um meio para melhorar a interação com a população, contribuindo para uma democratização ainda maior das decisões públicas. Para instituições de ensino, pode ser usada como instrumento para o fornecimento de educação à distância.

Sob o ponto de vista individual, a Internet se faz presente não apenas através das novas formas de relacionamento interpessoal, mas principalmente através do papel que vem assumindo na vida das pessoas: o de intermediadora e facilitadora de atividades comuns do dia a dia. Assim, torna-se cada vez mais freqüente a utilização de computadores pessoais para reservar passagens aéreas, fazer compras de supermercado, realizar transações bancárias, pesquisar e trocar informações, adquirir produtos e como forma de entretenimento.

Tomando como motivação este crescente mercado digital, muitas são as iniciativas para o desenvolvimento de aplicações que permitam implementar no ambiente da Internet uma série de serviços hoje fornecidos primordialmente através de métodos tradicionais, que não se beneficiam da mobilidade e independência proporcionados aos usuários da rede mundial de computadores. Uma dessas possíveis aplicações é a loteria.

Uma loteria é uma espécie de jogo, no qual participantes fazem apostas e vencedores são escolhidos através de alguma forma de sorteio. O termo digital é aplicado, neste trabalho, às loterias que utilizam a infraestrutura da Internet, ou de qualquer outra rede de computadores, para captar apostas de participantes geograficamente espalhados, estabelecendo, assim, um novo canal de acesso a este tipo de entretenimento.

Utilizando tecnologias Web, as loterias podem oferecer rapidez, eficiência e comodidade aos apostadores que não desejam se deslocar até uma casa lotérica, nem enfrentar eventuais filas. Além disso, o alcance das loterias é teoricamente maximizado, pois, uma vez implantada, a loteria digital pode ser acessada a partir de qualquer lugar. Por fim, o mundo digital oferece, ainda, facilidade para a introdução de novas modalidades de apostas, sendo possível, inclusive, gerenciar a interação entre apostadores para a elaboração de apostas conjuntas.

Assim, os benefícios trazidos pelas loterias digitais, aliados ao crescimento dos serviços Web e ao fascínio que o homem tem por jogos, tornam de grande interesse o estudo desta forma de prover loteria, incentivando o desenvolvimento deste projeto pelo Laboratório de Segurança em Computação – LabSEC, da Universidade Federal de Santa Catarina.

1.1 Justificativa

Paralelamente à tendência de expansão de serviços para o ambiente da Internet, verifica-se um crescimento na preocupação com a segurança das informações que trafegam na rede e, conseqüentemente, das entidades a quem estas informações pertencem. Segundo estatísticas do CERT (*Computer Emergency Response Team*), o número de ataques reportados nos três primeiros trimestres de 2001 foi 59% maior do que o número total no ano de 2000 [CER01], fato que aumenta o risco não apenas sobre a integridade e a confidencialidade da informação, mas também sobre a imagem das instituições que prestam serviços on-line sem priorizar a proteção de seus usuários.

No caso das loterias, mesmo das tradicionais, a segurança é um requisito fundamental em função de sua suscetibilidade a fraudes. Portanto, é necessário que a

solução adotada para loteria digital contenha mecanismos capazes de garantir a confiabilidade do processo de apostas, mesmo em caso de tentativa de corrupção da loteria por alguma das entidades participantes.

É essencial garantir ao apostador, dentre outras coisas, que:

- As apostas efetuadas junto à loteria digital sejam corretamente registradas, não sendo possível sua alteração ou invalidação;
- Uma aposta vencedora possa ser comprovada por aquele que a efetuou, assegurando ao mesmo o direito de recebimento do prêmio;
- Não seja possível forjar uma aposta vencedora, impedindo fraudes no processo lotérico;
- O pagamento de uma aposta seja realizado de forma segura, sem que informações confidenciais usadas neste procedimento, como números de cartões de créditos, possam ser obtidas por terceiros.

Desta forma, surge a necessidade de se definir um modelo para loteria digital capaz de minimizar ou eliminar problemas relacionados a segurança, garantindo sua credibilidade. A pesquisa tema desta dissertação vem de encontro a esta necessidade.

1.2 Objetivos

1.2.1 Objetivo Geral

Especificar um protocolo criptográfico para loteria digital capaz de prover segurança ao processo de apostas, resguardando os interesses e direitos tanto dos apostadores quanto da própria loteria.

1.2.2 Objetivos específicos

- Conhecer a problemática relacionada ao funcionamento das loterias tradicionais, utilizando as informações obtidas como base para a proposição de uma loteria digital segura e compatível com a tradicional;

- Levantar as soluções existentes para a implementação de loterias digitais e analisar o nível de segurança por elas provido;

- Levantar os requisitos de segurança essenciais ao correto funcionamento de uma loteria digital, de modo que possa, no mínimo, fornecer adequadamente a mesma funcionalidade de uma loteria tradicional;

- Apresentar um protocolo que satisfaça aos requisitos levantados, tornado segura cada uma das etapas do processo lotérico;

- Discutir o protocolo proposto, tentando mostrar que o mesmo trata de maneira satisfatória os problemas que podem surgir em função de tentativas de corrupção da loteria ou de falhas de comunicação entre o apostador e a loteria digital;

- Especificar o protocolo proposto usando a notação ASN.1.

1.3 Materiais e Métodos

Esta dissertação constitui-se em um trabalho teórico de especificação de um protocolo criptográfico para loteria digital. O seu desenvolvimento foi feito em cinco fases distintas:

(i) Inicialmente, foi realizada uma coleta de artigos, tutoriais e leis referentes às loterias tradicionais. Com base neste material, procurou-se conhecer o funcionamento destas loterias, identificando as etapas que compõem o processo lotérico e a maneira como as entidades participantes interagem em cada uma dessas etapas.

(ii) Como segundo passo, foram catalogadas e estudadas as soluções adotadas por alguns países para operacionalizar suas loterias digitais oficiais. Neste levantamento, o ponto de partida foi o site da *World Lottery Association*[1], entidade que congrega 139 loterias federais oficialmente licenciadas

[1] http://www.world-lotteries.org/

(tradicionais e digitais), espalhadas em 72 países dos cinco continentes. Além disso, também foram pesquisados e estudados artigos científicos, dissertações e teses que tratam de loterias digitais.

(iii) A etapa seguinte consistiu em definir os requisitos de segurança essenciais a uma loteria digital, de modo que possa oferecer, pelo menos, o mesmo nível de confiabilidade de uma loteria tradicional. Estes requisitos compreendem tanto propriedades genéricas que conferem segurança ao tráfego de informações entre a loteria e o apostador, quanto propriedades específicas de uma loteria, definidas com o objetivo de impedir fraudes durante o processo de apostas.

(iv) Como próximo passo, tomando por base as etapas anteriores, elaborou-se o protocolo apresentado nesta dissertação. Ao longo deste processo, foram observadas as técnicas criptográficas que poderiam ser utilizadas para atender individualmente aos requisitos definidos na etapa (iii). A seguir, o Lottuseg foi obtido a partir de combinações destas técnicas.

(v) Por fim, realizou-se a etapa de discussão do protocolo proposto em (iv) tomando por base os requisitos definidos em (iii).

Ao longo de todas as fases deste trabalho, foram utilizados recursos computacionais do LabSEC, bem como recursos bibliográficos disponíveis nesta universidade.

1.4 Trabalhos Correlacionados

Países como França, Inglaterra e Austrália possuem loterias oficiais disponíveis através da Internet. Estas loterias adotam um modelo genérico semelhante, no qual cada aposta efetuada é registrada no banco de dados da loteria em nome de um certo apostador. Não há emissão de comprovantes de apostas e técnicas de criptografia são utilizadas para garantir a segurança das informações que trafegam entre o apostador e a loteria, não sendo, contudo, adotados protocolos específicos para loteria digital.

Um protocolo criptográfico para loteria esportiva foi proposto por [KOB00]. Este protocolo, entretanto, também não permite a emissão de comprovantes de apostas digitais, fazendo com que o apostador dependa totalmente das informações contidas no banco de dados da loteria para poder comprovar sua aposta.

Desta forma, dentre os materiais pesquisados, não foram encontradas soluções para loteria digital semelhantes às aplicações tradicionais brasileiras, nas quais acontece a emissão de comprovantes de apostas verificáveis e não duplicáveis, capazes de garantir o anonimato dos apostadores e seu direito à recepção do prêmio.

1.5 Organização do texto

O restante deste trabalho encontra-se assim estruturado: no capítulo 2, o funcionamento das loterias tradicionais é apresentado em termos gerais, considerando-se seus principais elementos constitutivos e entidades que interagem durante o processo de aposta. O capítulo 3 descreve, de forma breve, fundamentos teóricos em criptografia e estende este assunto falando de protocolos criptográficos. O capítulo 4 introduz a problemática da loteria digital, estabelecendo requisitos para a operação de loterias digitais semelhantes às tradicionais, bem como apresenta algumas abordagens utilizadas para implementar loterias através da Internet. O capítulo 5 apresenta o Lottuseg, o protocolo criptográfico proposto nesta dissertação para solucionar o problema da loteria digital. Uma discussão do protocolo é apresentada no capítulo 6. Por fim, o capítulo 7 apresenta as considerações finais da dissertação e sugestões para trabalhos futuros.

Capítulo 2

As Loterias Tradicionais

A operacionalização de loterias pela Internet envolve o desenvolvimento de um modelo computacional capaz de acomodar os requisitos legais e funcionais vigentes para o processo tradicionalmente executado, pois as loterias digitais se apresentam como um meio alternativo para prover este tipo de serviço. Desta forma, a correta definição de tal modelo depende da compreensão da problemática relacionada à execução do processo lotérico tradicional. Tais questões serão discutidas ao longo deste capítulo com enfoque especial para as questões funcionais. A legislação referente ao tema também será citada, não havendo, contudo, um aprofundamento neste assunto, pois o mesmo está fora do escopo deste trabalho.

2.1 Definições Básicas

O conceito de loteria não é algo recente e encontra-se tão difundido que já foi intuitivamente incorporado ao senso comum. Tal noção, contudo, pode ser definida de modo simples, porém um pouco mais formalmente, como um procedimento para acumulação de dinheiro e distribuição de prêmios entre um grupo de pessoas através de alguma forma de sorteio.

O processo de acumulação das loterias modernas geralmente acontece de duas formas distintas:

- Os apostadores pagam por bilhetes de loteria numerados, já contendo um resultado possível para a loteria;

- Os apostadores escolhem os prognósticos que comporão suas apostas e os registram perante o promotor da loteria, pagando por este registro.

O período de tempo no qual a fase de acumulação acontece é chamado de fase de apostas. Cada uma das modalidades de aposta que uma loteria oferece é denominada jogo. Como exemplos de jogos brasileiros, pode-se citar a Mega-Sena e a Lotomania.

Após o encerramento da fase de apostas, ocorre o sorteio da loteria. Este sorteio, também denominado extração, irá determinar o resultado da loteria. Se houver mais de um vencedor, o prêmio é dividido entre eles. Caso não haja vencedores, o prêmio fica acumulado, devendo ser somado ao prêmio da próxima extração.

A Figura 2.1 mostra a linha temporal para um processo lotérico genérico. Nesta linha, os instantes de tempo T0 e T1 delimitam a fase de apostas. O instante T2 marca a realização do sorteio da loteria. Após o sorteio, os vencedores da loteria terão um período de tempo predeterminado para requisitar o pagamento do prêmio. Se o prêmio não for solicitado dentro deste período, o apostador perde o direito de recebê-lo. O instante de tempo T3 encerra este período no qual o prêmio pode ser requisitado.

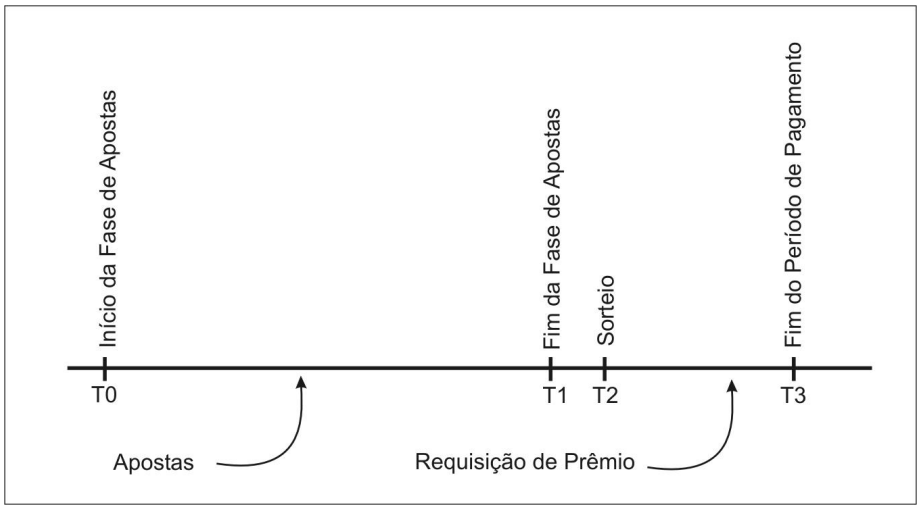

Figura 2.1 – Linha temporal do processo lotérico.

Segundo [KOB00], quatro entidades participam do processo lotérico:

- **Apostadores,** que adquirem o direito de concorrer a prêmios em função dos bilhetes adquiridos ou prognósticos registrados**;**

- **Postos de Venda,** que comercializam bilhetes de loteria numerados e/ou recebem prognósticos e pagamentos dos apostadores, emitindo comprovantes após o registro das apostas. Além disso, prestam contas ao promotor da loteria enviando o dinheiro coletado e informações sobre bilhetes vendidos e/ou prognósticos registrados**;**

- **Promotor da loteria,** que detém toda a responsabilidade pela operação da loteria. É sua função enviar o dinheiro acumulado durante a fase de apostas para a entidade financeira que o administrará, bem como conceder licenças aos postos de venda para comercialização de bilhetes e/ou recebimento de prognósticos. Além disso, é o promotor da loteria quem gera e mantém o banco de dados da loteria, também realizando as extrações e publicando os resultados.

- **Entidade financeira,** que gerencia o dinheiro acumulado, distribui as cotas de participação e paga os prêmios à medida que os mesmos são reclamados pelos vencedores.

No caso de loterias onde os apostadores escolhem seus prognósticos, pagando pelo seu registro, a interação entre estas entidades geralmente acontece conforme esquematizado na Figura 2.2, explicada a seguir.

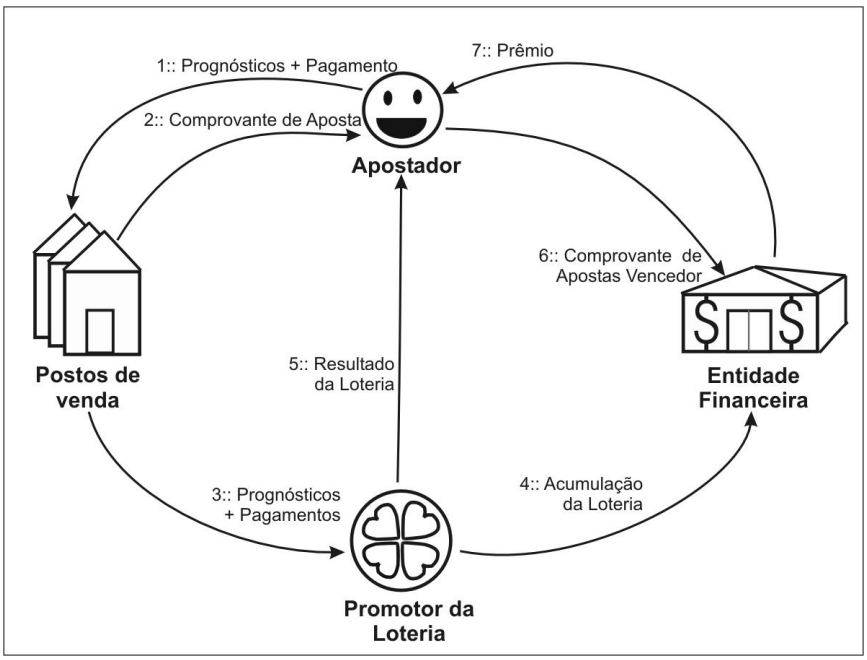

Figura 2.2 – Interação entre os participantes de uma loteria baseada na escolha de prognósticos.

Inicialmente, os apostadores selecionam os prognósticos que comporão sua aposta e os enviam para um posto de vendas junto com o pagamento correspondente (passo 1). Este posto de venda registra os prognósticos recebidos e emite um comprovante de apostas que é entregue ao apostador (passo 2). Ao final da fase de apostas, cada posto de venda envia para o promotor da loteria os pagamentos recebidos e as apostas registradas (passo 3). Por sua vez, o promotor da loteria entrega o dinheiro acumulado para a entidade financeira que o administrará (passo 4) e realiza a extração da loteria, divulgando para os apostadores o resultado (passo 5). Caso um apostador constate ser o vencedor, deve usar o seu comprovante de apostas para requisitar a premiação junto à entidade financeira que administra a acumulação (passos 6 e 7).

No caso de uma loteria baseada em bilhetes, a interação entre estas entidades é um pouco diferente, conforme ilustrado na Figura 2.3. Inicialmente, os postos de venda devem obter junto ao promotor de loteria lotes de bilhetes já impressos (passo 1), que serão vendidos aos apostadores (passos 2 e 3). Após o fim da fase de apostas, os postos de venda enviam para o promotor da loteria os pagamentos recebidos, assim como as informações sobre os bilhetes comercializados (passo 4). O restante do processo é igual ao caso anterior, uma vez que o bilhete de loteria equivale a um comprovante de apostas e é utilizado para requisitar um prêmio caso o apostador vença a loteria.

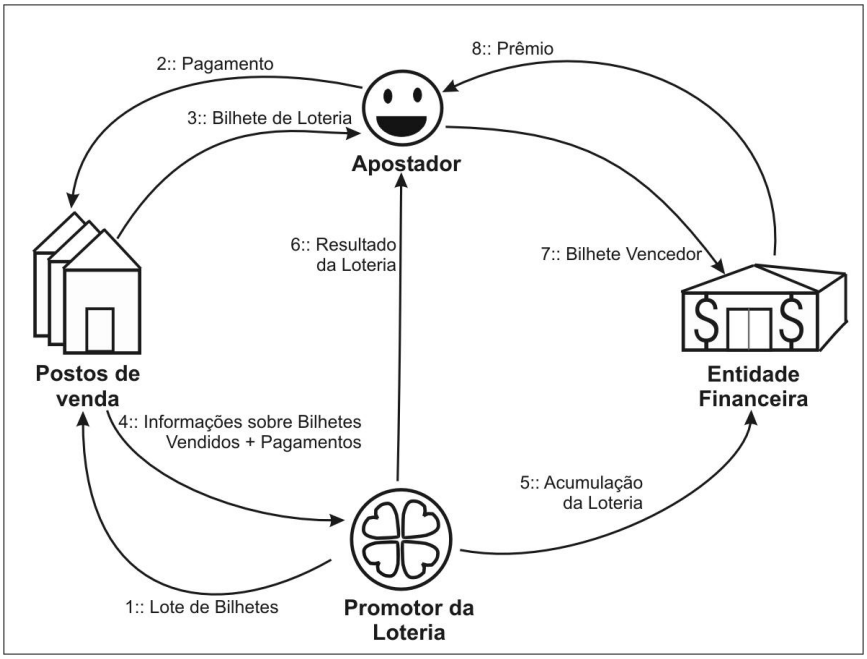

Figura 2.3 – Interação entre os participantes de uma loteria baseada em bilhetes.

Nas loterias federais do Brasil, os papéis de promotor da loteria e de entidade financeira são desempenhados pela Caixa Econômica Federal. Os postos de venda são representados pelas casas lotéricas credenciadas.

2.2 Elementos característicos de uma loteria

Existem várias configurações possíveis para uma loteria, tanto referentes ao tipo de aposta que pode ser feito, quanto ao método para se obter o resultado da loteria. Na maioria dos casos, contudo, pode-se observar a presença de quatro elementos característicos [BRIT01]: um conjunto de regras que regulamentam a loteria, um mecanismo para a captação de apostas, um mecanismo que associa cada apostador à(s) sua(s) aposta(s) e um método de determinação do vencedor. Estes elementos serão detalhados a seguir levando em consideração algumas questões de segurança pertinentes.

2.2.1 A regulamentação da atividade lotérica

Por ser uma atividade lucrativa e, ao mesmo tempo, suscetível a fraudes, um dos elementos mais importantes para o funcionamento de uma loteria é a presença de um conjunto de normas que determinem, dentre outras coisas, os responsáveis legais pelas extrações, as regras dos jogos que serão oferecidos, assim como as porcentagens da acumulação a serem destinadas ao pagamento de prêmios, à cobertura de custos organizacionais e, adicionalmente, destinadas ao governo, a alguma obra social ou à entidade organizadora da loteria. Geralmente, estas normas encontram-se sob a forma de leis e em vários países a exploração das loterias só pode ser feita mediante a obtenção de uma concessão do governo local, ou, ainda, o próprio governo é o responsável por sua operação.

No Brasil, a exploração de loterias é regulamentada pelo **Decreto-Lei nº 6.259, de 10 de fevereiro de 1944** [BRAa], que oficializa a execução dos serviços de loterias, federal e estadual, em todo território nacional. Segundo este Decreto-Lei, a loteria constitui serviço público exclusivo da União não suscetível de concessão, cuja renda líquida obtida será obrigatoriamente destinada a aplicações de caráter social e de assistência médica, em empreendimentos de interesse público. Sua exploração a nível federal, segundo o **Decreto nº 759, de 12 de agosto de 1969** [BRAb], foi cedida em caráter de exclusividade à Caixa

Econômica Federal. A legislação complementar, que estabelece e regula as várias modalidades de loteria que podem ser realizadas no país, é apresentada abaixo de modo sucinto:

- **Decreto-Lei nº 204, de 27 de fevereiro de 1967**: institui e regula a modalidade de Loteria Federal [BRAc]. Neste tipo de jogo, emite-se uma quantidade determinada de bilhetes numerados e os apostadores que os adquirem concorrem a prêmios mediante sorteio.

- **Decreto nº 594, de 27 de maio de 1969:** institui a modalidade de Loteria de Prognósticos Esportivos [BRAd]. Dois tipos de apostas são possíveis: a Esportiva, onde os prognósticos são feitos sobre o resultado de uma série de treze jogos de futebol realizados em datas pré-fixadas, e o Bolão Federal, onde o apostador concorre a prêmios pela indicação da quantidade de gols marcados pelos times de futebol programados no concurso.

- **Lei nº 6.717, de 12 de novembro de 1979:** institui a modalidade de Loteria de Números [BRAe]. Nesta modalidade, estão incluídas a Lotomania, a Super-Sena Dupla Chance, a Mega-Sena e a Quina. Nestes jogos, o apostador deve escolher uma quantidade determinada de prognósticos dentre o total disponível de dezenas. São considerados ganhadores os apostadores que acertarem um mínimo dentre os números sorteados.

- **Decreto nº 99.268, de 31 de maio de 1990:** institui a modalidade de Loteria Instantânea [BRAf]. Neste caso, os apostadores adquirem bilhetes e conhecem o resultado ao rasparem campos encobertos onde estão gravadas as combinações de números, de símbolos ou de caracteres determinantes dos prêmios.

Vale comentar que a legislação vigente no Brasil não prevê nenhum dispositivo legal que regule a implementação das loterias oficiais através da Internet. Além disso, também não havia, até o momento em que esta dissertação foi escrita, nenhum projeto de lei para o estabelecimento de normas específicas que contemplassem este novo paradigma relacionado à loteria. Deste modo, considerar-se-á neste trabalho que a Internet constitui-se

apenas em uma forma alternativa para a captação de apostas e que, portanto, a regulamentação existente deverá ser aplicada para todas as situações.

2.2.2 Mecanismos de captação de apostas

As tarefas de captar as apostas, coletar e contabilizar o dinheiro apostado são muito importantes. Um dos motivos para esta importância é a necessidade de se garantir que apostas e pagamentos sejam corretamente registrados, impedindo que o resultado da loteria seja manipulado, o que pode levar ao surgimento de falsos vencedores. Além disso, também se deve coibir a emissão, pelos próprios responsáveis pela loteria, de comprovantes de apostas válidos para os quais não foram efetuados pagamentos.

Em geral, tais problemas são contornados através do uso de uma hierarquia de agentes rigorosamente selecionados para a venda de bilhetes e recebimento de prognósticos, que repassam o dinheiro arrecadado para a entidade responsável pela loteria. Nas loterias federais brasileiras, as casas lotéricas desempenham este papel, sendo responsáveis pela venda de bilhetes de loteria numerados. Esta venda também é efetuada por vendedores ambulantes cadastrados. No caso dos jogos que envolvem prognósticos, apenas as casas lotéricas têm permissão para receber apostas. Com este objetivo, utilizam terminais on-line para sua captação, emitem comprovantes de apostas verificáveis pelos próprios terminais e registram em um banco de dados as apostas realizadas, bem como a movimentação financeira decorrente da loteria em todo o território nacional.

2.2.3 Mecanismo de associação de um indivíduo à sua aposta

A fim de garantir que o apostador seja capaz de requisitar o prêmio caso vença a loteria, deve-se adotar um mecanismo capaz de associar um indivíduo à sua aposta.

Algumas vezes, esta associação é direta e o promotor da loteria registra a identidade do apostador juntamente com sua aposta. Deste modo, logo após a divulgação do resultado da extração, os apostadores contemplados podem ser contatados. Neste tipo de loteria, a identidade do vencedor é conhecida e pode ser divulgada. Como ponto negativo desta abordagem pode-se citar a ausência de privacidade. Por outro lado, a personificação

do vencedor é dificultada, pois sua identidade precisa ser comprovada para que o prêmio seja pago.

Em outras loterias, não é estabelecida uma vinculação direta entre a aposta e o apostador. Neste caso, a loteria registra apenas as apostas em si e cada apostador recebe um comprovante de apostas que o associa indiretamente à sua aposta, de modo que sua identidade não seja conhecida pela loteria. A responsabilidade de reclamar o prêmio, que será pago ao portador do comprovante premiado, cabe ao apostador.

Um ponto negativo desta configuração é a possibilidade de perda do comprovante e recebimento indevido do prêmio. Adicionalmente, outro problema desta abordagem é a possibilidade de uso de comprovantes falsificados para reclamar prêmios, pois, como o comprovante é o único elemento que identifica o vencedor, pode ser possível gerar comprovantes com o resultado desejado caso não sejam utilizados mecanismos para sua correta validação. Assim, um comprovante de aposta deve conter informações suficientes para identificá-lo como verdadeiro e para tornar sua replicação muito difícil. Além disso, quase sempre é impresso em um papel especial, que pode ser facilmente identificado.

Nas loterias oficiais brasileiras, a privacidade do apostador é preservada através da emissão de comprovantes de aposta ao portador. A confiabilidade destes comprovantes é assegurada através das informações nele codificadas, validáveis pelos terminais de captação, bem como pelo papel utilizado, que contém uma numeração especial.

2.2.4 Método para determinação do vencedor

Um outro aspecto muito importante no processo lotérico é a seleção do procedimento que determinará a(s) aposta(s) vencedora(s). Tal procedimento pode ter a forma de sorteio, como nas loterias oficiais brasileiras, no qual urnas ou globos são usados para armazenar os números a serem escolhidos ou as parcelas que combinadas formarão estes números. Neste caso, o conteúdo da urna ou globo é misturado mecanicamente para conferir caráter aleatório ao processo, ocorrendo, em seguida, o sorteio. Em geral, a fim de se evitar

fraudes nesta etapa da loteria, as entidades promotoras normalmente deixam a auditoria a cargo de uma outra entidade confiável, sendo comumente realizada em eventos públicos.

Outro meio para selecionar o vencedor é a utilização de sistemas computacionais. Atualmente, existem inúmeros trabalhos nesta área, como os que fazem uso de técnicas de comprometimento de bits [SYV98] ou funções de retardo [GOL98] para a escolha justa dos vencedores. Nesta situação, a idéia é gerar o resultado da extração tomando por base informações internas à loteria, como números dos bilhetes emitidos ou valores apostados. Contudo, a fim de garantir a ausência de fraudes na extração, deve-se assegurar que o resultado só possa ser gerado após o encerramento do período de apostas. Além disso, deve-se permitir que qualquer indivíduo possa verificá-lo através da repetição do processo que levou à seleção dos vencedores.

2.3 Conclusão

Por existirem há um longo período de tempo, as loterias tradicionais operam baseadas em modelos consolidados e amplamente utilizados, dotados de mecanismos que garantem sua segurança. No caso das loterias digitais, ainda há muito espaço para pesquisa, principalmente porque os mecanismos físicos usados nas loterias tradicionais para prover segurança não estão disponíveis. Estas questões referentes à segurança de aplicações serão tratadas a partir do próximo capítulo, culminando com a definição de um modelo seguro para loterias digitais baseadas em prognósticos.

Não serão tratadas neste trabalho loterias digitais baseadas na venda de bilhetes numerados. Vale ressaltar que a implementação destas duas formas de loteria requer mecanismos distintos. Nas loterias de bilhetes, é necessário um procedimento para a geração e distribuição aleatória de bilhetes entre os apostadores pagantes. Nas loterias de prognósticos, é necessário um procedimento para a recepção anônima de prognósticos e emissão de comprovantes de apostas.

Capítulo 3

Fundamentos de Criptografia

O capítulo 2 introduziu a problemática relacionada às loterias tradicionais, servindo de parâmetro para a definição de um modelo para loteria digital. Contudo, a proposição de uma solução segura para loterias digitais depende não apenas do conhecimento acerca das loterias tradicionais, mas principalmente do entendimento das técnicas criptográficas usadas para prover segurança a aplicações. Desta forma, este capítulo tem por objetivo dar uma visão geral dos fundamentos de criptografia.

A definição de criptografia e sua idéia básica são apresentadas na seção 3.1. Em 3.2 e 3.3 são apresentados dois esquemas criptográficos amplamente utilizados: o simétrico e o assimétrico. A seção 3.4 trata das funções de resumo, componentes básicos das assinaturas digitais, abordadas em 3.5. A seção 3.6 apresenta o certificado digital, que tem por função identificar o signatário de uma assinatura digital. Por fim, protocolos criptográficos e suas aplicações são tratados em 3.7.

3.1 Criptografia

Criptografia pode ser definida como a ciência de escrever em códigos. Seu objetivo primordial é garantir que duas entidades, um emissor e um receptor, possam trocar mensagens privadas em um canal de comunicação inseguro, de modo que nenhuma outra entidade possa compreender o que está sendo comunicado [STI95]. Este sigilo ou privacidade da informação é denominado confidencialidade.

Para atingir esse propósito, a mensagem gerada pelo emissor, chamada de texto aberto, deve passar por uma operação de cifragem, tornando seu conteúdo incompreensível a todos que não estão autorizados a acessá-la. A mensagem cifrada, chamada de texto oculto, é o que circula pelo canal de comunicação inseguro. A operação que reverte a cifragem e obtém o texto aberto a partir do texto oculto é denominada decifragem. A Figura 3.1 ilustra estas operações.

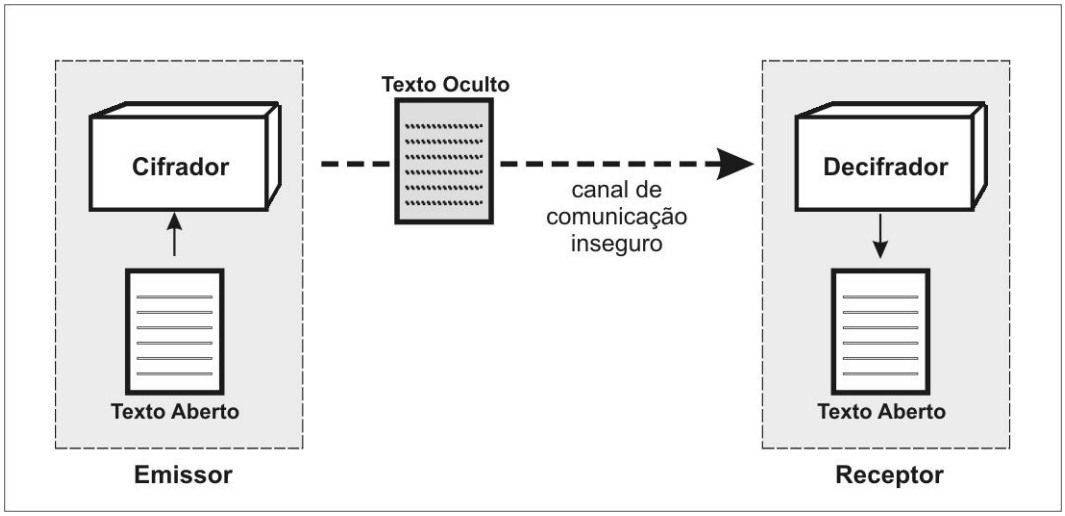

Figura 3.1 – Comunicação segura: as operações de cifragem e decifragem.

Além da confidencialidade, a criptografia também pode prover serviços de [SCH96]:

- **Autenticação:** garante que o emissor de um documento eletrônico esteja corretamente identificado, havendo certeza de que esta identidade é autêntica.

- **Integridade:** assegura que uma informação não pode ser indevidamente modificada sem que este fato seja detectado. Esta modificação pode ocorrer tanto no conteúdo de um documento, quanto na seqüência de informações trocadas entre duas entidades, além de poder incluir o retardo ou reenvio de mensagens.

- **Irretratabilidade:** garante que, uma vez realizada uma determinada operação, sua ocorrência não poderá ser negada por nenhuma das entidades participantes.

A função utilizada para cifrar ou decifrar uma mensagem é chamada de algoritmo criptográfico ou cifra.

Se a segurança deste algoritmo criptográfico baseia-se no sigilo do próprio algoritmo, ele é dito restrito [SCH96]. Os primeiros esquemas criptográficos, como o cifrador de César [STA99], funcionavam desta forma. O conhecimento do algoritmo permitia decifrar qualquer mensagem com ele cifrada.

Nas cifras modernas, segue-se o princípio de Kerckhoff, que determina que a segurança de uma cifra deve estar baseada no sigilo de chaves, e não no sigilo do algoritmo em si [STI95].

Uma chave é uma seqüência aleatória de bits que serve de parâmetro para o algoritmo criptográfico. Para cada chave possível, o algoritmo criptográfico produz uma transformação diferente sobre o texto aberto, gerando um texto oculto diferente. O conjunto de todas as chaves que podem ser usadas em uma cifra é chamado de espaço de chaves.

Segundo [STI95], um sistema criptográfico baseado em chaves pode ser definido como uma cinco-tupla *(P,C,K,E,D)*, que satisfaz as seguintes condições:

1. *P* é o conjunto finito dos possíveis textos abertos;
2. *C* é o conjunto finito dos possíveis textos ocultos;
3. *K*, o espaço de chaves, é o conjunto finito das possíveis chaves;
4. Para cada $k \in K$, existe uma regra de cifragem $e_k \in E$ e uma regra de decifragem correspondente $d_k \in D$. Cada $e_k : P \to C$ e $d_k : C \to P$ são funções tais que $d_k(e_k(x)) = x$ para cada texto aberto $x \in P$.

De acordo com a relação entre as chaves usadas para cifragem e decifragem, pode-se classificar um sistema criptográfico em simétrico ou assimétrico. Estas duas categorias de criptografia serão explicadas a seguir.

3.2 Criptografia Simétrica

Um sistema criptográfico é dito simétrico, ou convencional, quando a mesma chave é utilizada para cifrar um texto aberto e decifrar o texto oculto correspondente. Esta chave única é comumente chamada de chave secreta e referenciada por *k*.

Neste tipo de sistema, para que duas entidades possam trocar informações em sigilo, é necessário que compartilhem uma chave secreta k. Esta chave deve ser escolhida antes que o processo de comunicação tenha início e deve ser conhecida apenas pelas entidades comunicantes, devendo ser definida através de um canal de comunicação seguro, conforme ilustrado na Figura 3.2. Depois que esta operação for concluída, a chave k selecionada pode ser usada para cifrar e decifrar dados.

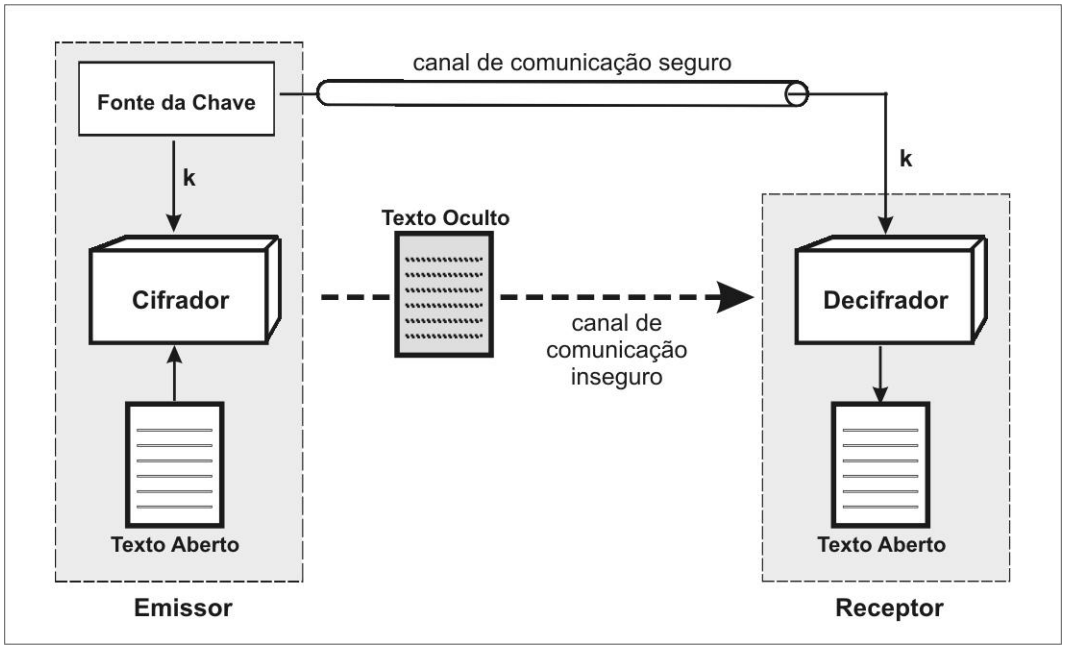

Figura 3.2 – Criptografia simétrica: uma chave única e secreta é usada para cifrar e decifrar dados.

Uma vez que a confidencialidade da informação transmitida depende do sigilo da chave utilizada, um dos principais problemas relacionados à criptografia simétrica é a distribuição segura de chaves, pois nem sempre é fácil obter um canal seguro para esta operação. Além disso, o gerenciamento de chaves também pode ser complexo, pois deve haver uma chave para cada par de usuários que deseja se comunicar. Desta forma, em uma rede com *n* usuários, seriam necessárias *n(n-1)/2* chaves para que todos possam trocar informações de forma sigilosa entre si.

Como exemplos de cifradores simétricos, pode-se citar os algoritmos DES, IDEA, Blowfish, RC5 [STA99] e o AES [NIS01]. Todos estes algoritmos baseiam-se na aplicação de operações de substituição e permutação para cifrar e decifrar dados, conforme indicado pelos conceitos de teoria da informação introduzidos por Claude Shannon [STI95, SHA49].

3.3 Criptografia Assimétrica

Um sistema criptográfico é dito assimétrico, ou de chave pública, quando são utilizadas duas chaves distintas: uma para cifrar o texto aberto e outra para decifrar o texto oculto correspondente.

Toda entidade que deseja fazer uso de um sistema deste tipo deve possuir um par de chaves próprio. Estas chaves, apesar de estarem intimamente relacionadas, guardam a propriedade de que é computacionalmente inviável determinar a chave de decifragem conhecendo-se apenas a chave de cifragem e o algoritmo criptográfico usado [MEN97].

Desta forma, a chave de cifragem, denominada de chave pública (*KU*), pode ser amplamente divulgada, eliminando a necessidade de distribuir chaves através de um canal de comunicação sigiloso. A outra chave, usada na decifragem, é chamada de chave privada (*KR*) e deve ser mantida em segredo.

Para que duas entidades possam se comunicar confidencialmente, a chave pública *KU* do receptor deve ser obtida pelo emissor e usada para cifrar o texto aberto a ser transmitido. Ao receber o texto oculto, o receptor deve usar sua chave privada *KR* para decifrá-lo, obtendo, assim, o texto aberto original. Por este modelo, nenhum outro indivíduo, nem o próprio emissor, é capaz de decifrar a mensagem, pois apenas o receptor conhece a chave privada *KR* [DIF76]. O processo descrito acima se encontra ilustrado na Figura 3.3.

Como exemplos de cifras assimétricas, pode-se citar os algoritmos RSA, ElGamal e as Curvas Elípticas [STI95]. O RSA será tratado a seguir.

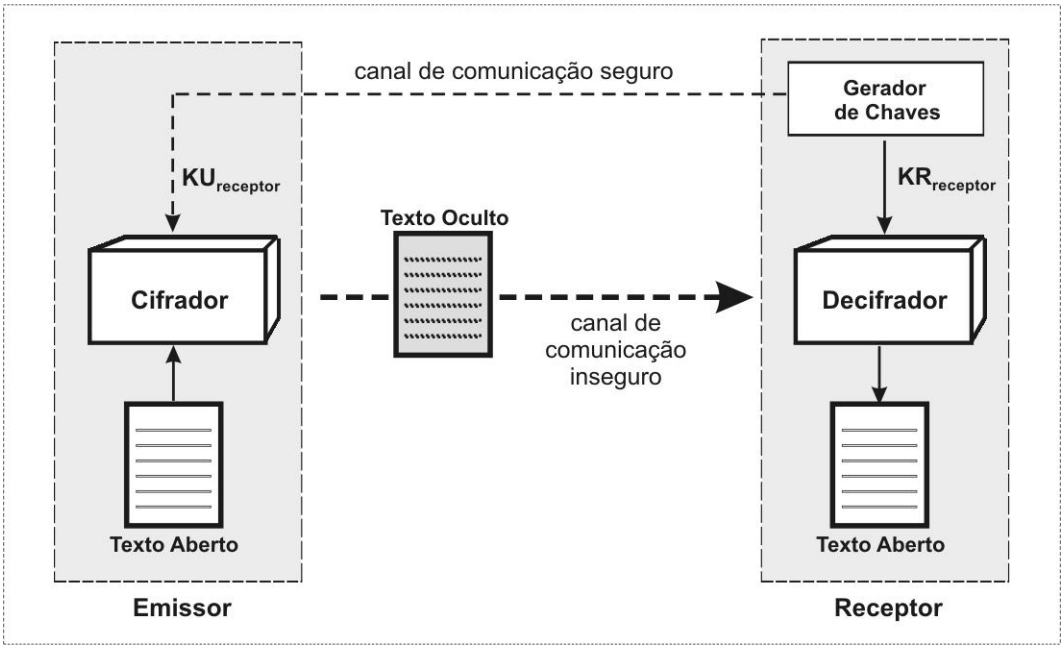

Figura 3.3 – Criptografia assimétrica: as chaves para cifrar e decifrar dados são distintas.

3.3.1 RSA

O RSA é um dos algoritmos de criptografia assimétrica mais populares, tendo sido criado em 1978 por Ron Rivest, Adi Shamir e Leonard Adleman [RIV78]. Seu funcionamento é baseado em operações de exponenciação e o texto aberto é cifrado em blocos, cada um dos quais correspondendo a um inteiro positivo menor que um certo número *n*.

Para a geração de um par de chaves no RSA, as seguintes operações devem ser executadas [STA99]:

- Escolher dois números primos grandes, *p* e *q;*
- Calcular $n = p \times q$;
- Calcular[2] $\phi(n) = (p-1)(q-1)$;

[2] A função $\phi(n)$ é denominada totiente de Euler e representa o número de inteiros positivos menores que *n* relativamente primos a *n*. Dois números são relativamente primos se o número 1 é o único divisor de ambos.

- Escolher um número aleatório *e* tal que[3] $mdc(\phi(n),e) = 1$ e $1 < e < \phi(n)$;
- Calcular *d* tal que $d = e^{-1} \bmod \phi(n)$;

A chave pública *KU* será igual à dupla {*e*,*n*}, devendo ser publicada. A chave privada *KR*, igual à dupla {*d*,*n*}, deve ser armazenada em lugar seguro.

Tendo sido geradas a chave pública e a privada, uma entidade estará apta a receber mensagens seguras de qualquer outra entidade que conheça sua chave pública.

Considerando o texto aberto *x* e o texto oculto *y*, ambos pertencentes à Z_n, onde $n = p \times q$, as funções de cifragem e decifragem podem ser definidas, respectivamente, por:

$$e_K(x) = x^e \bmod n$$

$$d_K(y) = y^d \bmod n$$

A segurança do RSA baseia-se na dificuldade de fatorar números grandes. Se for possível fatorar *n* em *p* e *q*, será fácil obter a chave privada {*d*,*n*} a partir da chave pública {*e*,*n*}, bastando apenas seguir o mesmo procedimento usado na fase de geração das chaves. Desta forma, para tornar computacionalmente inviável um ataque baseado em tentativas de fatoração, deve-se trabalhar com valores de *n* muito grandes.

Além disso, algumas das outras técnicas usadas para dificultar a fatoração de *n* determinam que os valores de *p* e *q* devem ser escolhidos tais que [STA99]:

(i) *p* e *q* difiram em tamanho em apenas alguns dígitos;

(ii) Tanto (*p-1*) quanto (*q-1*) contenham números primos grandes;

(iii) mdc(*p-1*, *q-1*) deva ser pequeno.

[3] A função *mdc(a,b)* representa o máximo divisor comum dos números *a* e *b*.

3.4 Funções de Resumo (Hash)

Uma função de resumo, ou função hash, é uma transformação *H(M)* que, aplicada sobre mensagens *M* de tamanho variável, produz sempre uma cadeia de bits *h* de tamanho fixo [SCH96]. *h* é chamado de valor de hash ou resumo.

$h = H(M)$, onde h tem o tamanho fixo m.

Seu objetivo básico é produzir uma representação concisa, porém única, da mensagem ou documento sobre o qual é aplicada. Esta representação pode ser considerada a impressão digital do elemento que a originou.

Para que uma função *H* possa ser considerada um hash, deve apresentar as seguintes propriedades [STA99]:

- $h = H(M)$ é relativamente fácil de calcular para qualquer *M* dado;
- Dada uma função de hash *H* e um valor de hash *h* produzido através da aplicação de *H* sobre *M*, qualquer modificação realizada em *M*, mesmo que de um bit, deve implicar na produção de um resumo *h* diferente;
- Conhecido um valor de hash *h*, deve ser computacionalmente inviável deduzir a mensagem *M* que o originou. Desta forma, como a função hash não deve ser invertida, é chamada de função de sentido único;
- Dada uma mensagem *M*, deve ser computacionalmente impossível encontrar uma outra mensagem qualquer $M' \neq M$ tal que $H(M) = H(M')$, garantindo-se assim que não se pode criar uma mensagem que tenha uma certa "impressão digital". Uma função hash que obedece a esta propriedade é chamada de fracamente livre de colisões.
- Para que uma função de resumo seja fortemente livre de colisões, é necessário que seja computacionalmente inviável encontrar, dentro do universo possível de mensagens, duas mensagens diferentes quaisquer *M* e *M'* tais que $H(M) = H(M')$.

Como exemplos de funções hash, pode-se citar os algoritmos MD2, MD5 e SHA1 [STA99].

3.5 Assinaturas Digitais

O problema de provar a autoria de um documento ou a concordância com as cláusulas de um contrato, ambos em papel, pode ser resolvido através da utilização de assinaturas manuscritas. Em um meio digital como a Internet, um problema como este também pode ser resolvido através da aplicação de assinaturas, contudo, de natureza digital.

Segundo [SCH96], um algoritmo de assinaturas digitais deve produzir assinaturas que tenham como propriedades:

- *Autenticidade:* a assinatura identifica unicamente o signatário do documento;
- *Não-falsificação*: dado um certo signatário, ninguém, além dele mesmo, deve ser capaz de gerar uma assinatura em seu nome;
- *Não-reutilização*: a assinatura deve fazer parte do documento, não podendo ser removida e utilizada para validar outro documento;
- *Integridade*: dado um documento assinado, não deverá ser possível alterar o corpo do documento mantendo válida a assinatura;
- *Irretratabilidade*: uma vez que uma assinatura tenha sido gerada, seu signatário não deve ser capaz de negar sua autoria.

Assinaturas digitais podem ser criadas através da aplicação de criptografia assimétrica e de funções de resumo. Para tanto, deve-se tomar o documento *M* a ser assinado e, aplicando uma função hash, obter seu resumo *h*. A seguir, este resumo, que identifica univocamente o documento a partir do qual foi obtido, deverá ser cifrado com a chave privada *Kr* do signatário. A assinatura digital será o resultado desta cifragem e poderá ser distribuída junto com o documento ao qual se refere.

De posse de um documento assinado, a autenticidade da assinatura pode ser verificada decifrando-a com a chave pública *Ku* do signatário e comparando o valor obtido

com a aplicação da função hash sobre o documento *M*. Caso os dois valores sejam iguais, a autenticidade fica provada. A Figura 3.4 ilustra a geração e verificação de assinaturas. O símbolo || representa concatenação.

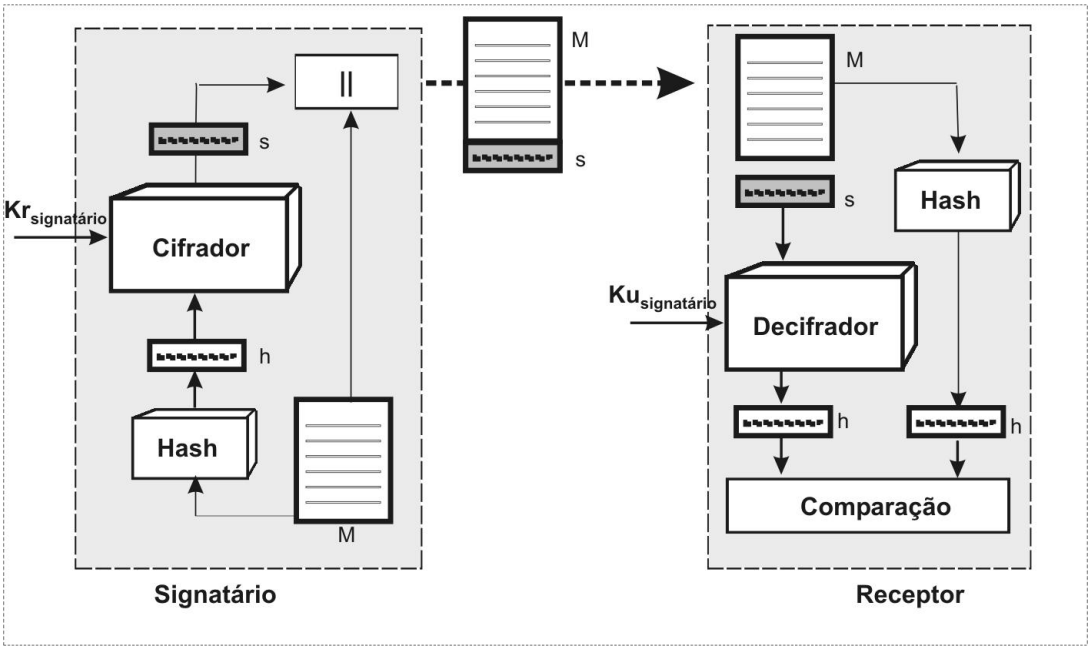

Figura 3.4 – Processo de geração e verificação de uma assinatura digital.

Aplicando este procedimento, verifica-se que as cinco propriedades sugeridas por [SCH96] são garantidas:

- *Autenticidade, Não-falsificação e Irretratabilidade*: como a assinatura é verificada utilizando a chave pública do signatário, este processo é capaz de identificar se a mesma foi produzida com a chave privada de um certo usuário. Em caso afirmativo, este usuário não poderá repudiar este fato. Caso a chave privada não tenha sido corrompida e seja conhecida apenas por seu proprietário, esta assinatura poderá ser considerada autêntica;

- *Não-reutilização e Integridade*: uma vez que a assinatura é gerada sobre o resumo do documento e este resumo será modificado caso o documento o seja, o processo de verificação de assinatura não será bem sucedido caso o documento tenha perdido a integridade. Por outro lado, esta mesma propriedade garante que a assinatura de um documento não poderá ser reutilizada para validar um outro documento.

Como exemplo de algoritmo de assinatura digital, pode-se citar o DSA [STA99].

3.6 Certificados Digitais

Uma vez que a criptografia assimétrica é usada tanto para cifrar mensagens, quanto para a gerar assinaturas digitais, torna-se essencial poder determinar se a chave pública de uma certa entidade é autêntica. Caso não seja possível provar esta autenticidade, o processo de verificação de assinatura ou decifragem de mensagens poderá ser mal sucedido pelo uso da chave incorreta.

A maneira mais usual de garantir a autenticidade de uma chave pública é utilizar um certificado digital. Um certificado digital é uma seqüência de bits digitalmente assinada contendo informações que associam uma chave pública ao detentor da chave privada correspondente [HOU01]. A entidade responsável por emitir e assinar estes certificados digitais é denominada Autoridade Certificadora (AC) .

Para que se possa considerar um certificado digital confiável, é necessário que se tenha confiança na Autoridade Certificadora que o emitiu. Desta forma, fazendo uma analogia com os documentos em papel, um certificado digital pode ser comparado a uma cédula de identidade, que só tem validade caso seja emitida por um órgão confiável, como a Secretaria de Segurança Pública do estado emissor.

Para que um certificado seja gerado, as informações que associam a chave pública à entidade devem ser assinadas pela Autoridade Certificadora, de modo que as seguintes propriedades sejam válidas [STA99]:

- Qualquer usuário com acesso à chave pública de uma Autoridade Certificadora poderá verificar a validade da assinatura de um certificado digital por ela emitido;

- Nenhuma entidade além da Autoridade Certificadora poderá ser capaz de modificar o conteúdo de um certificado sem que este fato seja detectado.

Desta forma, como certificados não podem ser forjados caso a chave privada da Autoridade Certificadora não esteja corrompida, os mesmos podem ser publicados em diretórios públicos ou distribuídos livremente sem a necessidade de esforços especiais para sua proteção.

O padrão mais reconhecido para certificados digitais é o X.509 (ISO/IEC/ITU-T) [ITU00]. Este padrão encontra-se ilustrado na Figura 3.5 e as informações nele contidas são explicadas a seguir.

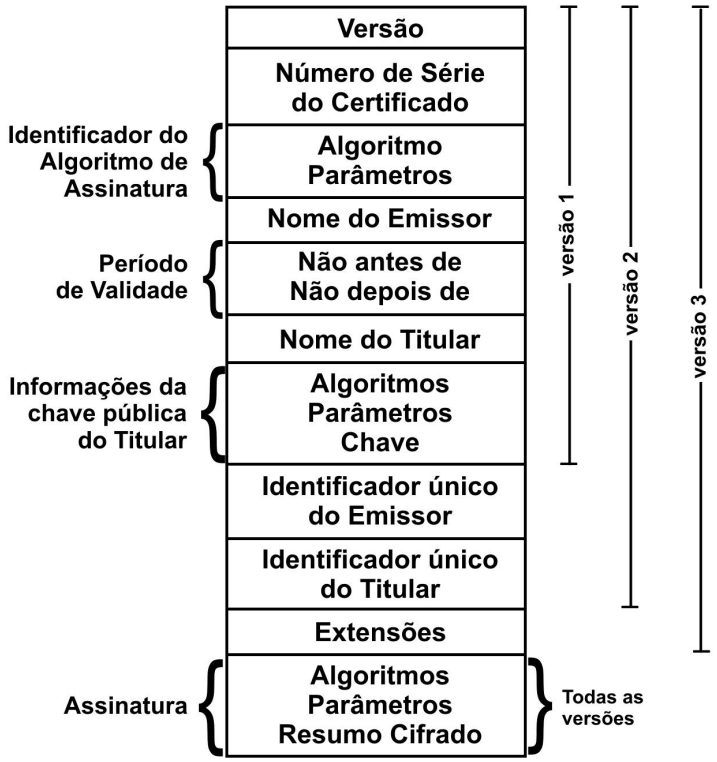

Figura 3.5 – O padrão de certificado X.509.

- *Versão*: especifica a versão do referido certificado, podendo variar de um a três.

- *Número de série*: valor inteiro que identifica o certificado, único dentro da autoridade certificadora que o emitiu;

- *Identificador do algoritmo de assinatura*: informações referentes ao algoritmo usado para assinar o certificado e parâmetros associados;

- *Nome do emissor*: nome no padrão X.500 da autoridade certificadora que criou e assinou o certificado;
- *Período de validade*: datas que delimitam a partir de quando e até quando o certificado será válido;
- *Nome do titular do certificado*: nome do usuário para o qual o certificado foi emitido;
- *Informações da chave pública do titular do certificado*: compreende a chave pública do titular, o identificador do algoritmo com a qual a chave deve ser usada e os parâmetros necessários;
- *Identificador único do emissor*: string de bits opcional usada para identificar unicamente a autoridade emissora do certificado caso o nome no padrão X.500 tenha sido usado por mais de uma entidade;
- *Identificador único do titular do certificado*: string de bits opcional usada para identificar unicamente o titular do certificado caso o nome no padrão X.500 tenha sido usado por mais de uma entidade;
- *Extensões*: conjunto de um ou mais campos de extensão;
- *Assinatura*: valor do resumo (hash) de todos os outros campos do certificado cifrado com a chave privada da autoridade certificadora. Este campo também inclui um identificador do algoritmo de assinatura.

3.7 Protocolos Criptográficos

Um protocolo é um conjunto de passos, executados em uma seqüência pré-definida, que envolve dois ou mais participantes e tem por objetivo a realização de alguma tarefa [SCH96]. Para o seu funcionamento adequado, todas as partes envolvidas devem conhecer o protocolo com antecedência e concordar com os procedimentos estabelecidos.

De modo mais específico, um protocolo criptográfico é um protocolo que utiliza criptografia simétrica/assimétrica, funções de resumo e/ou assinaturas digitais para atingir seus objetivos, garantindo, ainda, que nenhum dos participantes consiga saber mais ou fazer mais do que está definido no protocolo.

Dentre os objetivos de um protocolo criptográfico, podem estar tanto os serviços básicos de confidencialidade, integridade, autenticação e irretratabilidade, quanto requisitos de segurança específicos da aplicação.

No caso de aplicações que apresentam múltiplos requisitos de segurança, é possível modularizar o processo de elaboração do protocolo pretendido, utilizando protocolos criptográficos genéricos como blocos para sua construção. Alguns exemplos de protocolos muito utilizados para o desenvolvimento de outros protocolos são [SCH96]: anonimato, autenticação, assinaturas cegas e geração aleatória de bits.

O protocolo proposto neste trabalho, o Lottuseg, segue esta idéia de modularização, utilizando como base dois protocolos: comprometimento de bits e redes de misturadores. Estes dois protocolos serão apresentados a seguir. Vale observar, contudo, que a forma como são utilizados para a obtenção de um protocolo seguro para loteria digital será discutida apenas no capítulo 6, no qual o Lottuseg será apresentado.

3.7.1 Comprometimento de Bits

Este protocolo permite que uma entidade *A* se comprometa à existência de uma informação *I* perante uma entidade *B*, sem ter que revelar esta informação para *B* [SCH96]. Com este objetivo, *A* deve fornecer a *B* evidências relacionadas a *I*, de modo que, posteriormente, quando *I* for revelada, *B* possa verificar se esta é a informação com a qual *A* se comprometeu originalmente.

Estas evidências são chamadas de comprometimento de bits e devem ser geradas de forma que não seja possível utilizá-las para descobrir a informação secreta. O processo através do qual a entidade *A* revela a informação com a qual se comprometeu é chamado de abertura do comprometimento de bits. Neste processo, o comprometimento de bits deverá ser utilizado para detectar qualquer tentativa de trapaça.

A Figura 3.6 ilustra a idéia geral do protocolo. No instante 1, a entidade *A* gera o comprometimento de bits *C* relacionado a uma informação *I*, enviando-o para *B*. No instante 2, a entidade *A* revela a informação *I* para *B*, que, usando o comprometimento *C*, verifica se *I* é a informação original.

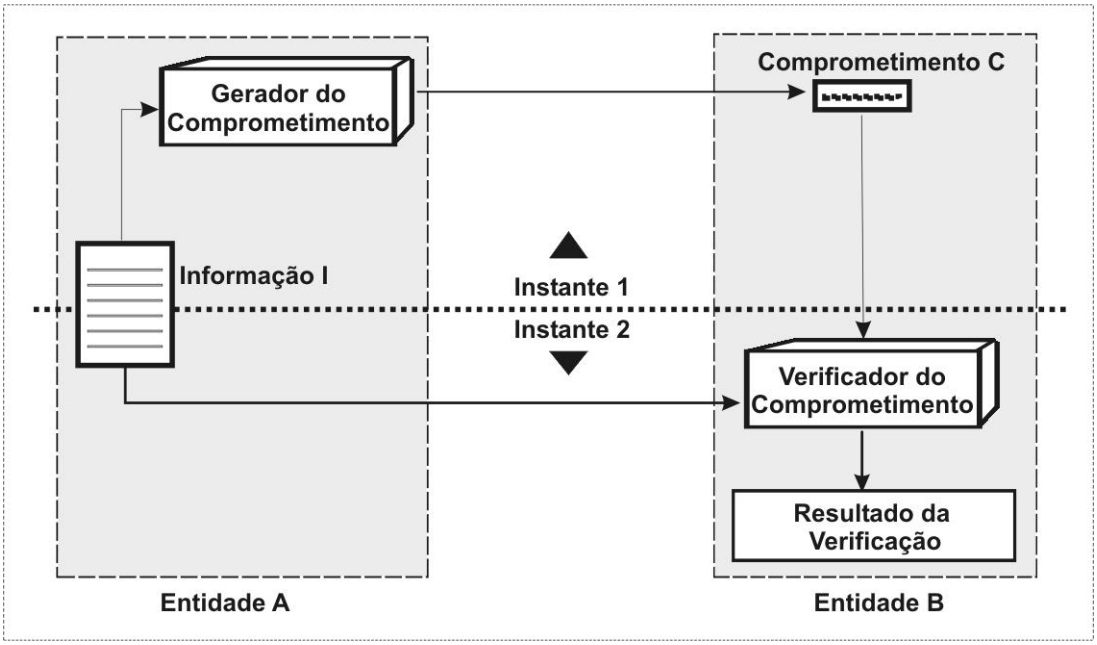

Figura 3.6 – O protocolo de Comprometimento de Bits.

Duas das técnicas que podem ser utilizadas para implementar este protocolo serão apresentadas a seguir [SCH96].

3.7.1.1 Comprometimento de Bits usando Criptografia Simétrica

(1) *B* gera uma string de bits aleatórios, denominada *R*, e a envia para *A*;

(2) *A* cria uma mensagem que consiste da informação *I* com a qual deseja se comprometer e da string *R* enviada por *B*. Esta mensagem é cifrada com uma chave aleatória *K* e o resultado é enviado para *B*;

Concluída a etapa de comprometimento, verifica-se que *B* não pode ter acesso à informação *I*, pois não sabe como decifrar a mensagem. Quando *A* desejar revelar a informação *I*, o protocolo continua da seguinte forma:

(3) *A* envia a chave *K* para *B*;

(4) *B* decifra a mensagem para obter *I*, conferindo a presença da string *R* para confirmar a validade da mensagem.

3.7.1.2 Comprometimento de Bits usando Funções de Sentido Único

(1) *A* gera duas strings de bits aleatórios, denominadas de R_1 e R_2;

(2) *A* cria uma mensagem contendo R_1 e R_2 e a informação *I* com a qual deseja se comprometer (R_1, R_2, *I*);

(3) *A* aplica uma função de hash *H(x)* sobre a mensagem produzida no passo 2 e envia o resultado para *B*, juntamente com uma das strings geradas ($H(R_1, R_2, I)$, R_1);

Como a função *H(x)* é de sentido único, *B* não pode invertê-la para obter *I*. Quando *A* desejar revelar a informação *I*, o protocolo continua da seguinte forma:

(4) *A* envia para *B* a mensagem original (R_1, R_2, *I*)

(5) *B* aplica a função de sentido único sobre a mensagem recebida no passo 4 e a compara com o valor de hash recebido no passo 3. *B* também deve verificar se a string R_1 recebida no passo 3 está contida na mensagem recebida no passo 4. Se estas verificações forem bem sucedidas, o comprometimento é considerado válido e, conseqüentemente, a mensagem verdadeira.

3.7.2 Redes de Misturadores

Algumas aplicações, como eleições digitais e esquemas de pagamento, têm o anonimato como um dos principais requisitos de segurança. Contudo, a obtenção desta propriedade, quando da comunicação através de redes de computadores, requer a aplicação de procedimentos especiais, uma vez que os protocolos de rede incluem os endereços de

origem e destino nos pacotes em circulação. Uma das soluções para contornar este problema é a utilização de uma Rede de Misturadores [CHA81b, JAK98].

Um misturador é uma entidade que, posicionada entre os emissores e os destinatários de mensagens, esconde a relação entre as mensagens postadas pelos emissores e as mensagens recebidas pelos destinatários, tornando-as anônimas. Para atingir este fim, cada emissor *E* deve cifrar a mensagem a ser enviada e a identidade do destinatário *D* com a chave pública do misturador *M*, enviando, então, o resultado desta operação para o misturador. Este processo é ilustrado na Figura 3.7.

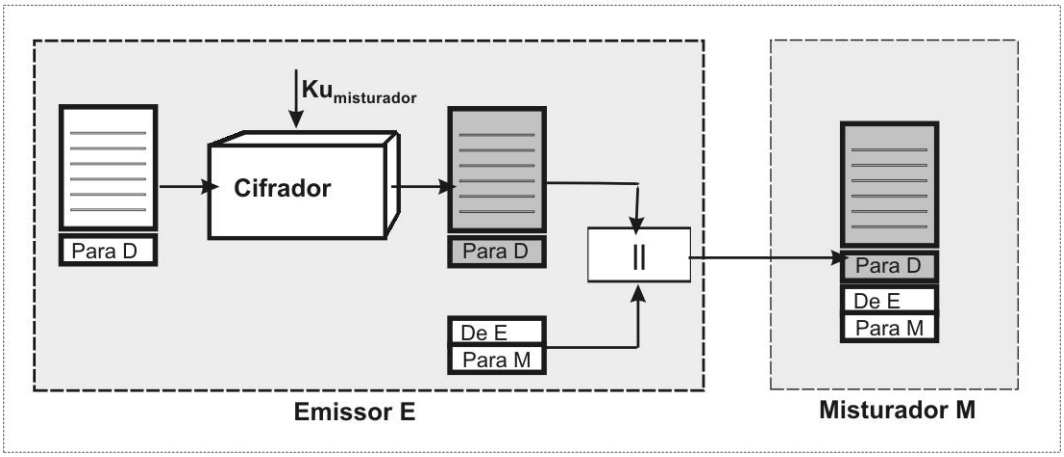

Figura 3.7 – O procedimento para envio de mensagens para o Misturador.

A seguir, o misturador *M* decifra cada mensagem recebida e a envia para o destinatário *D* correspondente, usando o seu próprio endereço como o endereço de origem da mensagem. O envio da mensagem para o destinatário é ilustrado na Figura 3.8.

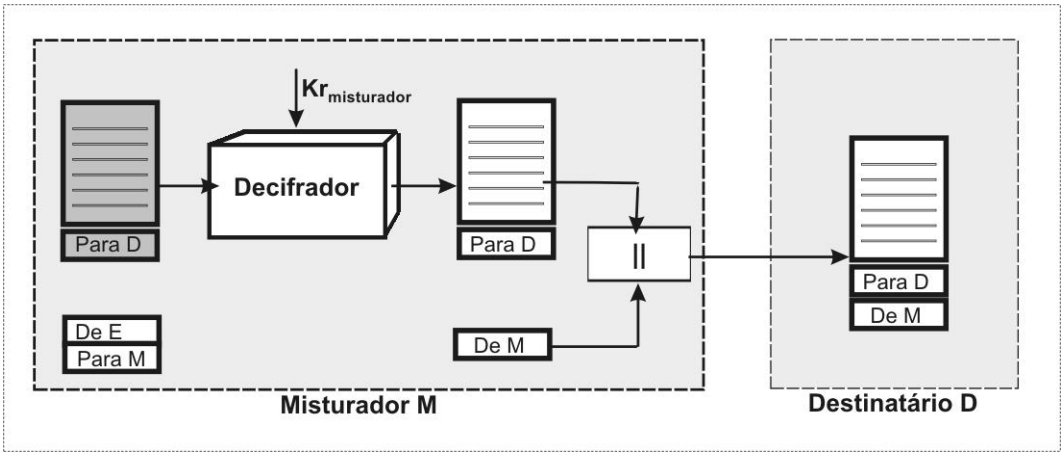

Figura 3.8 – O procedimento de envio de mensagens para o Destinatário.

Além de esconder a origem da mensagem, o misturador também permuta a ordem na qual as mensagens recebidas são enviadas a seus destinos, impedindo que se estabeleça uma relação entre as mensagens de entrada e de saída caso as mesmas tenham um tamanho único.

Quando um conjunto de misturadores é utilizado em seqüência, ligando-se a saída de um à entrada do próximo, obtém-se uma rede de misturadores. Uma rede como esta é usada para impedir que o uso de um único misturador malicioso comprometa o anonimato do sistema. Adicionalmente, observa-se que, mesmo que *n-1* dos *n* misturadores presentes na rede sejam comprometidos, a existência de um único misturador honesto evita que se relacionem as mensagens que entram na rede às mensagens que dela saem.

3.8 Conclusão

Este capítulo apresentou uma revisão dos fundamentos de criptografia necessários à compreensão do protocolo criptográfico proposto, devendo-se destacar assinaturas e certificados digitais. O conceito de protocolo criptográfico também foi apresentado, bem como os protocolos utilizados como base para a elaboração deste trabalho. Algumas formas para prover segurança a aplicações usando criptografia serão apresentadas no próximo capítulo, que contém exemplos de loterias digitais em operação e protocolos criptográficos relacionados à loteria.

Capítulo 4

Introdução à Loteria Digital

Conhecendo-se o funcionamento e os principais elementos característicos de uma loteria tradicional, surge a questão de como implementar uma loteria digital que disponibilize os mesmos serviços com, pelo menos, o mesmo nível de segurança. Neste capítulo, serão introduzidas algumas possíveis abordagens para o projeto de uma aplicação segura, serão apresentados exemplos de loterias oficiais que operam via Web e de protocolos criptográficos para loteria digital. Além disso, serão definidos os principais requisitos de segurança e de implementação para uma Loteria Digital.

4.1 Desenvolvimento de aplicações seguras para Internet

Em uma rede de computadores como a Internet, baseada no protocolo TCP/IP [TAN97], a informação pode trafegar por uma série de máquinas intermediárias antes de atingir o seu destino, o que traz à tona a necessidade de se adotar um conjunto de medidas capazes de deter, prevenir ou, pelo menos, detectar possíveis violações de segurança. Estas violações, comumente chamadas de ataques, podem ser genericamente classificadas, segundo [STA99], em quatro tipos:

- **Interrupção:** tem por objetivo destruir ou tornar inacessíveis recursos computacionais, como computadores, linhas de transmissão e arquivos, que deveriam estar disponíveis aos usuários autorizados assim que fossem requisitados;

- **Interceptação:** é um ataque no qual um usuário não autorizado ganha acesso a informação privada, comprometendo sua confidencialidade. Esta informação

pode ser obtida diretamente através da captura de uma mensagem em circulação ou pode ser obtida de modo indireto através da análise de tráfego na rede;

- **Modificação:** compreende não apenas o acesso não autorizado à informação, mas também a sua modificação. Este ataque compromete a integridade da informação e pode estar baseado na modificação do conteúdo ou seqüência de mensagens trocadas, além do retardo ou reenvio de mensagens;

- **Fabricação:** baseia-se na inserção de mensagens no sistema por usuários não autorizados, que se fazem passar por usuários legítimos. Nesta modalidade de ataque, coloca-se em risco a autenticidade da informação, uma vez que o emissor da mensagem não é aquele que afirma ser.

Existem várias abordagens possíveis para a proteção do tráfego de informações em redes de computadores [STA99]. Estas abordagens, embora possam ser consideradas semelhantes no que diz respeito aos serviços que provêem, diferem quanto ao seu escopo de aplicação e quanto à sua localização ao longo das camadas do protocolo TCP/IP.

Uma destas abordagens é o protocolo IPSec [STA99, CHE98]. Este protocolo atua ao nível da camada IP provendo serviços de confidencialidade e autenticação aos pacotes em circulação entre dois pontos da rede. Esta solução, considerada de propósito geral, tem como vantagem ser transparente ao nível de aplicação, de modo que os softwares executados em máquinas que utilizam o IPSec podem gozar dos serviços de segurança por ele providos, sem necessidade de modificação.

Subindo para o nível da camada de transporte, uma outra alternativa é oferecer segurança tomando por base os serviços orientados a conexão do protocolo TCP. Nesta categoria enquadram-se os protocolos SSL/TLS [APO97, FRI96, WAG99], que têm por objetivo permitir que dois processos possam negociar e estabelecer, através de um mecanismo prático e já estruturado, canais seguros de comunicação providos de confidencialidade, integridade e mútua autenticação entre as partes. Neste nível, existem duas alternativas de implementação [STA99]: (i) fornecer suporte ao SSL/TLS como parte da camada de transporte, sendo, desta forma, transparente para a aplicação; ou (ii) embutir

o SSL/TLS em aplicações específicas, como efetivamente acontece com os navegadores Web Internet Explorer e Netscape.

Uma terceira abordagem refere-se à implementação dos serviços de segurança na camada de aplicação. Uma das vantagens desta abordagem é a possibilidade de adaptar os serviços oferecidos às necessidades e aos requisitos específicos da aplicação em questão, que podem ir além da mera necessidade de confidencialidade e autenticação. Deste modo, protocolos específicos podem e devem ser desenvolvidos neste nível a fim de atender a aplicações mais complexas, como as que envolvem votações digitais, trocas de segredo, loterias e modelos de pagamento, dentre tantos outros possíveis exemplos.

A Figura 4.1 ilustra as camadas do protocolo TCP/IP e a localização ao longo destas camadas das abordagens apresentadas.

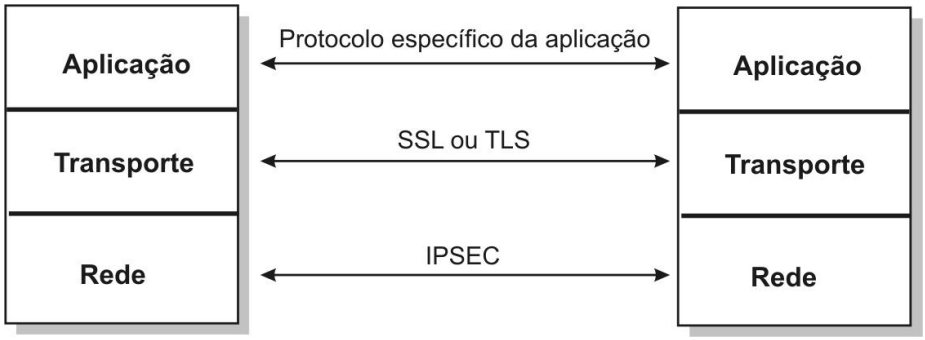

Figura 4.1 – Localização de alguns protocolos de segurança ao longo das camadas do TCP/IP.

4.2 Exemplos de Loterias Digitais Oficiais

Considerando as abordagens apresentadas para prover segurança ao tráfego de informações, serão apresentados três exemplos de sistemas de loteria que operam via Web. Estes três exemplos correspondem a loterias que, durante a fase de pesquisa desta dissertação, contavam com autorização oficial dos governos de seus países de origem para operar via Internet: Inglaterra, França e Austrália. A funcionalidade destas loterias, bem como a forma adotada para garantir segurança de tráfego, será apresentada nesta seção.

No caso da Inglaterra, o primeiro sítio de loteria legalmente autorizado é o Lotter-e, que tem por endereço *http://www.lotter-e.co.uk*. Sua operação está a cargo da

empresa britânica Alladdin Lotteries Limited, autorizada pelo Conselho de Jogos da Grã-Bretanha (Gaming Board for Great Britain) a gerenciar as loterias inglesas na Internet, e tem sua renda revertida em benefício dos clubes membros da Sociedade de Futebol da Grã-Bretanha.

Este sítio oferece uma loteria de números disponível apenas através da Internet, onde o apostador escolhe cinco prognósticos dentre trinta dezenas. Para estar apto a jogar, um apostador deve se registrar através do sítio como membro da Sociedade de Futebol da Grã-Bretanha, devendo ser residente na Grã-Bretanha e maior de dezesseis anos. Uma vez concluído este procedimento, no qual deve ser fornecido um número válido de cartão de crédito, o apostador terá uma conta que lhe permitirá utilizar o sítio. O acesso a esta conta é realizado através de um esquema de autenticação do tipo usuário-senha. Cada apostador dispõe de um nome de usuário e de uma senha, também conhecidos pela loteria, que devem ser corretamente fornecidos sempre que o apostador desejar acessar sua conta.

Nesta loteria, não são emitidos bilhetes ou qualquer tipo de comprovante digital que sirva para reclamar a premiação. Cada aposta está diretamente relacionada a um apostador, ficando registrada em sua conta. Quando os números sorteados são divulgados, os vencedores são individualmente notificados por e-mail. O pagamento das apostas é feito debitando-se o valor apostado no cartão de crédito fornecido na fase de registro.

Segundo informações obtidas através da Internet, a segurança do *sítio* do Lotter-e baseia-se na utilização de um servidor certificado pela Verisign e na adoção do protocolo SSL para garantir confidencialidade e integridade das informações que trafegam pela Internet. Não é mencionada a utilização de protocolos específicos ao nível da camada de aplicação.

Outro exemplo de loteria oficial oferecida pela Internet é o francês, cujo sítio, disponível no endereço *http://www.francaise-des-jeux.fr/*, pertence à empresa La Française des Jeux, organizadora e operadora oficial de jogos de loteria na França. Esta empresa semi-estatal, regulada pelo Estado francês, responsabiliza-se por autorizar os jogos, definir suas regras, preços e calendários, bem como determinar os montantes da arrecadação destinados à premiação e aos outros fins.

Assim como no caso inglês, para que uma pessoa possa apostar em qualquer um dos jogos, oferecidos apenas através da Internet, é necessário realizar um cadastro, comprovando residência em território francês e maioridade. Concluída esta etapa, o apostador terá um nome de usuário e uma senha para fins de autenticação e poderá, através de um cheque enviado à La Française des Jeux ou transferência bancária, adicionar créditos a sua conta. Uma vez que os créditos sejam incluídos, o apostador poderá usá-los para realizar apostas. Esta loteria também não oferece privacidade aos participantes, pois cada aposta é registrada em nome de um apostador específico.

Em se tratando de segurança, a loteria francesa também adota apenas o SSL para transmitir de modo seguro as informações trocadas entre o seu servidor e os clientes, não sendo especificados outros protocolos.

A loteria digital da Austrália está disponível no endereço *http://www.tattersalls.com.au/*. Tattersall's é uma organização privada australiana que detém concessão estatal para operacionalizar loterias na capital da Austrália, no norte do país e nos territórios de Vitória e Tasmânia.

Assim como nos casos francês e inglês, para estar apto a usar a loteria digital, um apostador deve se cadastrar junto a Tattersall's, comprovando, através da submissão de cópias de documentos, residir em um dos locais onde esta loteria pode operar e ter mais de dezoito anos. Concluído o processo de cadastramento, o apostador disporá de uma conta de acesso, que poderá ser acessada através de um esquema de autenticação do tipo usuário-senha. Nesta conta, serão armazenadas informações referentes a todas as apostas realizadas. As formas de pagamento aceitas são cartão de crédito e débito em conta.

A realização de apostas é feita de modo semelhante a operações de comércio eletrônico. Os prognósticos escolhidos são armazenados em um “carrinho de compras” enquanto não são submetidos, podendo-se remover apostas contidas no carrinho ou inserir novas. Para concluir uma aposta, o apostador deverá escolher uma forma de pagamento, fornecer as informações necessárias para sua efetivação e confirmar a operação. Após esta confirmação, o pagamento é processado em tempo real através de um sistema australiano chamado SecuryPay Network, que está interligado ao sistema bancário regional. Caso a disponibilidade financeira do apostador para o pagamento da aposta se confirme, a

transação é efetuada e a loteria registra esta aposta na conta do apostador, confirmando ao mesmo o sucesso da operação.

Com relação à segurança, a loteria australiana não utiliza protocolos específicos para loteria digital. Apenas faz uso do protocolo SSL para garantir confidencialidade e integridade das informações que trafegam pela Internet e utiliza um servidor certificado pela Verisign. Adicionalmente, vale comentar que as informações referentes ao pagamento da aposta, como números de cartão de crédito ou números de conta corrente, não são armazenadas pela loteria. Estas informações são armazenadas pelo SecuryPay, que submete para a loteria apenas a confirmação/recusa do pagamento.

4.3 Protocolos criptográficos para loteria digital

As três loterias digitais apresentadas anteriormente não fazem uso de protocolos específicos para loteria digital. Ao invés disso, estes sítios apenas utilizam o protocolo SSL para obter confidencialidade, integridade e autenticação de tráfego.

Nesta seção, será apresentado um protocolo criptográfico proposto no Japão para loteria esportiva [KOB00]. Este protocolo tem por objetivo permitir que apostadores possam realizar seus jogos através da Internet, efetuar o pagamento correspondente, verificar se suas apostas foram devidamente registradas e permitir a requisição do prêmio em caso de acerto dos prognósticos. Questões de confiabilidade de tráfego não são tratadas pelo protocolo, sendo deixadas a cargo de outros protocolos como SSL e IPSEC, que operam em camadas inferiores do TCP/IP.

Ao longo de sua execução, não são emitidos comprovantes de aposta para a requisição da premiação. A idéia sobre a qual o protocolo se baseia consiste em usar a técnica de comprometimento de bits para associar a aposta à identidade do apostador. Esta associação apenas será revelada caso o apostador precise requisitar o prêmio.

A forma utilizada no protocolo para implementar o comprometimento de bits é a aplicação de uma função de resumo sobre a aposta e a identidade do apostador, de modo que o valor obtido é a evidência do comprometimento. Vale observar que as funções de resumo servem a este propósito, pois, para um certo resumo *r* produzido a partir de um par

aposta-apostador, é computacionalmente inviável encontrar outro par diferente do original que produza o mesmo *r*. Desta forma, o resumo produzido associa univocamente uma aposta a um apostador.

Outro ponto importante a ser observado é que o protocolo pressupõe a existência de vários postos virtuais de venda, responsáveis por receber as apostas e os pagamentos dos participantes e enviá-los ao promotor da loteria. Cada um desses postos possui um identificador único.

As quatro fases definidas no protocolo são:

- ***Compra de apostas***, na qual os apostadores submetem suas apostas e os pagamentos correspondentes a um posto de vendas, responsável por registrá-las perante a loteria.

- ***Verificação da aposta***, através da qual o apostador pode verificar se o posto de vendas registrou sua aposta corretamente.

- ***Fechamento da loteria***, na qual a loteria publica, antes da realização do sorteio que definirá os vencedores, uma lista digitalmente assinada contendo todas as apostas recebidas. Esta lista tem por função assegurar que não possam ser inseridas apostas fraudulentas após a divulgação do resultado.

- ***Requisição de pagamento***, através da qual um apostador solicitará o pagamento de uma premiação caso vença a loteria.

A notação utilizada ao longo de todas as etapas do protocolo encontra-se descrita abaixo. Após a definição da notação, cada uma das fases do protocolo é apresentada em detalhes.

- *AP*: apostador;

- *PV*: posto virtual de venda;

- *L*: entidade promotora da loteria;

- *aposta*: conteúdo da aposta de *AP*;

- *idPV*: identidade do posto virtual de venda;
- *idAP*: identidade do apostador;
- *H()*: função de resumo (hash);
- *h1*: comprometimento de bits entre *aposta* e *idAP;*
- *h2*: comprometimento de bits entre *h1* e idPV*;*
- *h2*:* metade inicial de h2;
- *$D*: informações de pagamento;
- $S_A(X)$*:* informação X assinada com a chave privada da entidade *AP*;
- *X* || *Y*: concatenação de X e Y;
- *Σ(X):* conjunto de todas as ocorrências de X.

4.3.1 Fase de Compra de Apostas

Na fase de compra de apostas, o apostador pode realizar sua aposta acessando um dos postos virtuais de venda e submetendo a ele os prognósticos apostados e o pagamento correspondente. O protocolo de comprometimento de bits é usado para relacionar a identidade do apostador a sua aposta e estes valores serão registrados no banco de dados da loteria. Este procedimento é realizado através dos passos especificados a seguir, ilustrados na Figura 4.2.

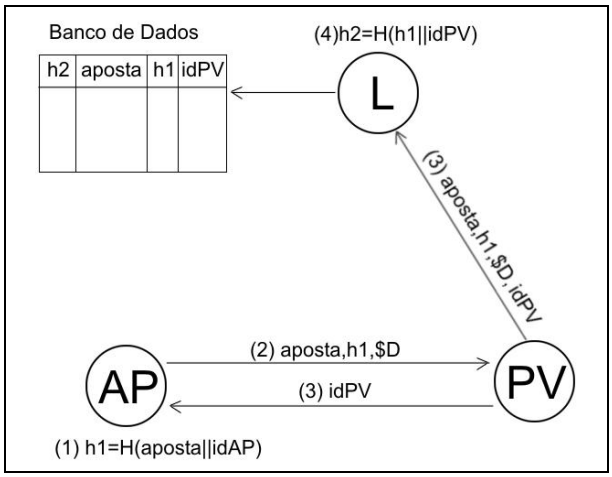

Figura 4.2 – Fase de compra de apostas.

(1) *AP* gera a *aposta* e produz o comprometimento de bits *h1* entre *aposta* e *idAP* através da aplicação da função de resumo *H(x)*;

$$h1 = H(aposta \,||\, idAP)$$

(2) *AP* envia a *aposta*, o resumo *h1* e as informações de pagamento *$D* para *PV*;

(3) *PV*, por sua vez, envia a *aposta, o resumo h1, as informações de pagamento $D* e sua identidade *idPV* para *L* e, depois, envia *idPV* para *AP*;

(4) *L* calcula o comprometimento de bits *h2* entre *h1* e *idPV*, relacionando também a aposta ao posto de venda através do qual foi realizada;

$$h2 = H(h1 \,||\, idPV)$$

(5) *L* armazena *h2*, *aposta*, *h1* e *idPV* em seu banco de dados.

4.3.2 Fase de Verificação da Aposta

Concluída a fase de compra, o cliente pode executar a fase de verificação, que consiste em conferir se sua aposta foi corretamente registrada no banco de dados do promotor da loteria. Esta fase encontra-se ilustrada na Figura 4.3 e os passos que a compõem estão descritos abaixo.

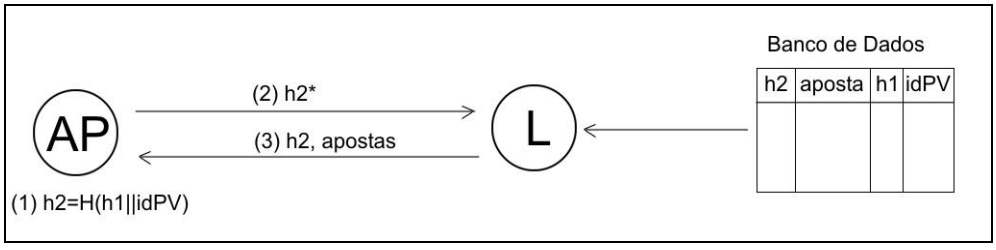

Figura 4.3 – Fase de verificação de aposta

(1) Utilizando *h1* e *idPV* obtidos na fase de compras, *AP* calcula *h2*, que servirá de índice de busca para sua aposta;

$$h2 = H(h1 \,||\, idPV)$$

(2) *AP* envia *h2** para *L* e solicita que lhe sejam devolvidos todos os pares *h2-aposta* cujo valor de *h2* tenham início igual ao fornecido;

(3) *L* devolve os valores que satisfazem a solicitação;

(4) *AP* verifica os valores recebidos. Se um deles for o valor correto do par *h2-aposta*, *AP* considera que fase de compra foi corretamente executada.

4.3.3 Fase de Fechamento da Loteria

Quando for encerrado o período de apostas, deve ser executada a fase de fechamento da loteria, que tem por objetivo impedir futuras modificações nas apostas registradas. Com este objetivo, a loteria deve gerar uma assinatura digital sobre a lista de apostas recebidas, divulgando esta lista assinada. A Figura 4.4 ilustra a fase de fechamento, cujos passos estão descritos a seguir.

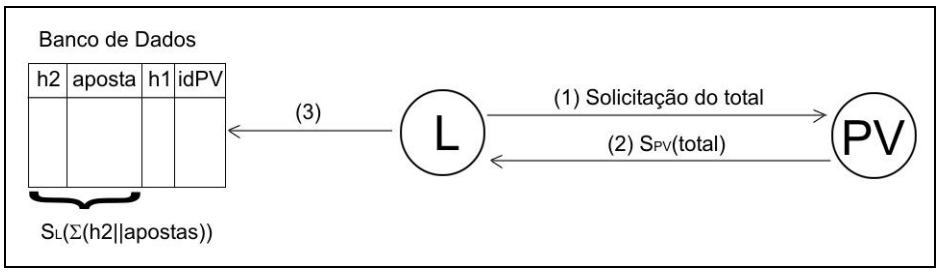

Figura 4.4 – Fase de fechamento.

(1) *L* solicita que cada *PV* informe o número de apostas recebidas;

(2) Cada *PV* envia para *L* uma mensagem assinada contendo o seu total;

$$S_{PV}(total)$$

(3) *L* verifica se os totais armazenados em seu banco de dados conferem com os totais fornecidos por cada *PV*. Em caso afirmativo, *L* gera uma assinatura digital sobre os campos *aposta* e *h2* de todas as entradas armazenadas para aquela extração, assegurando, assim, sua proteção contra tentativas de modificação.

$$S_L(\Sigma(h2||aposta))$$

4.3.4 Fase de Requisição de Pagamento

A fase de requisição de pagamento, mostrada na Figura 4.5, é opcional, só devendo ser executada caso o apostador tenha uma aposta vencedora e precise reclamar seu prêmio. A seguir, os passos componentes desta fase são apresentados.

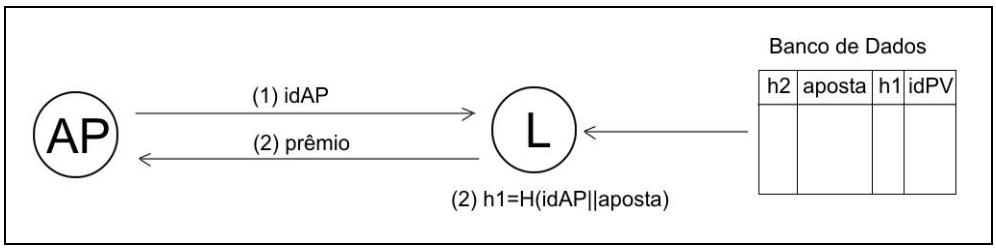

Figura 4.5 – Fase de requisição de pagamento.

(1) *AP* envia sua identidade *idAP* para *L;*

(2) *L* calcula *H(aposta || idAP)* e verifica se este valor corresponde ao *h1* registrado no banco de dados para a *aposta* vencedora. Em caso afirmativo, o prêmio é pago.

4.3.5 Análise do Protocolo

O protocolo apresentado permite a implementação de uma loteria digital no qual se considera *L* uma entidade confiável. A seguir, serão comentados os requisitos de segurança que definiram seu projeto e que foram satisfatoriamente alcançados:

- Apenas o apostador vencedor pode recuperar seu prêmio, pois a aposta está implicitamente relacionada a ele através do comprometimento de bits;
- O apostador pode detectar, através da fase de verificação, se sua aposta foi corretamente registrada no banco de dados da loteria;
- Após a fase de fechamento, não deve ser possível inserir ou modificar apostas no banco de dados da loteria. Este requisito é atingido através da assinatura digital gerada pela loteria sobre as apostas, que pode ser verificada por qualquer apostador, permitindo, assim, que se detecte a existência de irregularidades.

Contudo, embora este protocolo atenda aos requisitos sobre os quais foi definido, algumas outras questões podem ser levantadas:

- *Ausência de tolerância à falhas*: durante a fase de compra, caso a conexão entre o apostador *AP* e o posto de venda *PV* seja perdida entre os passos 2 e 3, o usuário já terá realizado o pagamento e enviado sua aposta, contudo, não terá como saber se o procedimento de aposta foi concluído, cancelado ou simplesmente abandonado. Não é definido no protocolo o que acontecerá com uma operação interrompida. Vale enfatizar que esta situação é crítica, pois pode implicar em perdas financeiras para o apostador e perda de credibilidade da loteria;

- *Um apostador não tem como comprovar sua aposta*: mesmo quando a fase de compras do protocolo é concluída com sucesso, o apostador não recebe um comprovante que sirva para provar de forma não repudiável sua aposta. Ao invés disso, recebe apenas uma confirmação contendo o valor do *idPV* do posto de venda, permitindo, assim, que o apostador execute o procedimento de verificação. Esta abordagem, contudo, não é totalmente satisfatória, pois a execução da verificação permite apenas que se detecte algum problema no procedimento de registro de aposta. Uma vez que o apostador não dispõe de um comprovante, não será possível provar de forma indubitável que uma aposta deixou de ser registrada e exigir a garantia de seus direitos;

- *Impossibilidade de auditoria*: na fase de fechamento, a loteria e os postos virtuais de venda fazem a contagem do número de apostas realizadas. Neste momento, se algum problema for detectado, não há como descobrir qual aposta deixou de ser armazenada ou qual aposta foi incluída indevidamente no banco de dados. Para resolver este problema, cada posto de venda deveria também armazenar todas as apostas que realizou.

Desta forma, observa-se que é possível definir uma lista mais ampla de requisitos de segurança capazes de guiar o desenvolvimento e a análise de um protocolo criptográfico para loteria digital.

4.4 O problema da loteria digital: requisitos necessários

Nesta seção, serão apontados os requisitos sugeridos neste trabalho para um protocolo seguro de loteria digital. Estes requisitos foram subdivididos em dois grupos: requisitos de segurança e requisitos funcionais.

4.4.1 Requisitos de Segurança

Como requisitos de segurança de um protocolo seguro para loteria digital, pode-se citar:

- **Autenticação:** impõe que o ato de apostar deve ser permitido apenas aos apostadores autorizados. Esta propriedade deve ser garantida porque as loterias atuais são consideradas jogos de azar e apresentam regras rígidas que regulam o seu funcionamento. Tais regras, instituídas e mantidas pelo governo, determinam os tipos de loterias que podem ser realizadas em uma determinada localidade e as entidades por elas responsáveis. Desta forma, é fundamental identificar os indivíduos que desejam apostar, liberando esta operação somente àqueles que residem no local onde a loteria digital em questão é autorizada a operar. Além disso, uma outra questão que torna imprescindível a autenticação é a necessidade de garantir que os apostadores tenham, segundo a legislação vigente, idade suficiente para apostar. Não deve ser permitido que menores de idade possam utilizar serviços de loteria, tanto tradicionais quanto digitais;

- **Confidencialidade**: diz respeito à propriedade através da qual o conteúdo de uma aposta só pode ser conhecido pelo apostador que a efetuou. Nem a própria loteria deve ter acesso a esta informação enquanto o período de apostas não for encerrado, impedindo que seja possível obter estatísticas sobre os prognósticos apostados. Desta forma, evita-se que apostas sejam realizadas em funções de outras recebidas previamente. Por outro lado, informações fornecidas pelos apostadores para validação de apostas, como números de cartões de crédito, também devem permanecer em sigilo, não podendo ser obtidas por terceiros enquanto forem válidas;

- **Integridade:** garante que nenhuma informação trocada entre o apostador e a operadora da loteria pode ter seu conteúdo modificado por qualquer outra entidade durante sua transmissão. Além disso, apostas registradas não podem ser alteradas sem que haja detecção. Por fim, não deve ser possível registrar apostas para extrações com resultados já divulgados;

- **Privacidade:** determina que nenhuma aposta deve ser associada diretamente ao indivíduo que a produziu, de modo que, nem a loteria, nem qualquer outra entidade, sejam capazes de identificar o apostador que originou uma aposta;

- **Irretratabilidade:** determina que, depois que uma aposta tenha sido paga, a sua ocorrência não possa ser negada. Desta forma, é introduzido o ônus da prova, devendo ser garantido ao apostador o direito a um comprovante de apostas digital que possa ser usado para requisitar o prêmio caso contemplado pela loteria.

Para que este comprovante possa desempenhar seu papel adequadamente, garantindo tanto o correto funcionamento da loteria, quanto a confiança dos apostadores nos procedimentos adotados, deve apresentar os seguintes requisitos de segurança:

- **Intempestividade:** uma vez que as apostas para uma determinada extração devem ser registradas dentro de um período de tempo pré-definido, os comprovantes de aposta emitidos devem estar corretamente datados para que possam ter validade. Adicionalmente, o processo que executa esta datação deve ser confiável;

- **Verificabilidade:** deve ser possível ao apostador verificar se um comprovante de apostas emitido pela loteria é válido e, conseqüentemente, assegura seu direito de receber o prêmio caso acerte o resultado da loteria. Por outro lado, quando for feita uma requisição de pagamento de prêmio, a loteria também deve ser capaz de validar o comprovante de apostas utilizado nesta operação;

- **Não-falsificação:** deve ser computacionalmente inviável produzir um comprovante de loteria verificável que possa ser usado para solicitar indevidamente o pagamento da premiação da loteria. Cada comprovante de

apostas deve conter evidências que identifiquem a entidade que o emitiu. Além disso, a própria loteria não deve ser capaz de fraudar o processo lotérico emitindo comprovantes de apostas para extrações cujos sorteios já foram realizados;

- **Não-duplicação:** comprovantes de apostas tradicionais, emitidos em papel, apresentam inúmeras características físicas que dificultam eventuais tentativas de duplicação. Um comprovante digital, assim como qualquer outro documento digital, é uma seqüência de bits que pode ser replicada, produzindo uma cópia igual à seqüência original. Desta forma, é necessário garantir que cada comprovante digital contenha informações que o identifiquem unicamente, permitindo detectar tentativas de uso indevido de apostas duplicadas.

4.4.2 Requisitos Funcionais

Além dos requisitos de segurança especificados, um sistema de loteria digital plenamente funcional deve prover necessariamente:

- **Tolerância a falhas:** o procedimento de apostas deve ser projetado de modo a garantir que o apostador e a operadora da loteria não saiam prejudicados caso o protocolo seja interrompido antes do seu final. Assim, deve-se garantir que sempre que uma aposta e seu pagamento sejam registrados pela loteria, o apostador deverá ser capaz de comprovar sua aposta;

- **Mobilidade:** deve ser possível a um apostador submeter suas apostas de qualquer terminal conectado a Internet, contanto que disponha dos mecanismos necessários para completar adequadamente o protocolo, cumprindo, por exemplo, requisitos como autenticação.

Além dos requisitos acima citados, considerados imprescindíveis a uma loteria digital, os seguintes requisitos também são desejáveis:

- **Flexibilidade:** o protocolo de loteria deve ser flexível o suficiente a fim de permitir sua utilização em qualquer tipo de loteria. Também deve ser capaz de aceitar novos tipos de jogos sempre que necessário;

- **Conveniência:** o protocolo de loteria deve se adequar às necessidades de cada apostador, permitindo que o mesmo faça suas apostas e receba seu comprovante digital de modo fácil e rápido, além de permitir que a solicitação da premiação seja realizada on-line. Alternativamente, deve ser permitido ao apostador imprimir seu comprovante de apostas e utilizá-lo para solicitar a premiação pessoalmente;

- **Escalabilidade:** um sistema de loteria digital escalável é aquele no qual pode haver um número indefinido de apostadores, acomodando de maneira satisfatória a demanda a qual pode estar submetido.

4.5 Conclusão

Tendo em vista os requisitos sugeridos para uma loteria, verifica-se a inviabilidade de adoção de uma abordagem de segurança somente em nível da camada de rede ou de transporte. Neste caso, faz-se necessário o desenvolvimento de uma solução ao nível da camada de aplicação a fim de que sejam contemplados todos os requisitos de segurança levantados. O capítulo seguinte apresenta o Lottuseg, o protocolo criptográfico para loteria digital proposto nesta dissertação.

Capítulo 5

Lottuseg

O Lottuseg é, em sua essência, um protocolo que define um procedimento seguro para o recebimento de prognósticos, emissão de comprovantes de apostas digitais e requisição/validação de pagamento de premiação. Além disso, também contempla uma série de outras questões importantes para o pleno funcionamento de uma loteria digital confiável: autenticação dos apostadores, gerenciamento de jogos/extrações e pagamento de apostas. Estas e outras atividades encontram-se distribuídas ao longo das seis fases que constituem o protocolo.

As primeiras três fases correspondem a atividades administrativas, que têm por objetivo viabilizar a operação da loteria:

- **Estabelecimento da Loteria:** compreende atividades voltadas à criação da loteria digital, incluindo a emissão de certificados digitais para a loteria digital e seus administradores;

- **Cadastramento de Apostadores:** consiste na emissão de certificados digitais para identificação e autenticação dos apostadores;

- **Configuração de Jogos e Extrações:** permite definir os jogos válidos e suas regras, bem como os prêmios pagos para cada extração, as datas quando acontecerão os sorteios e o período no qual as apostas estarão sendo recebidas;

Uma vez que a loteria digital esteja pronta para operar, pode ter início a fase de apostas, na qual cada um dos apostadores deve executar as seguintes etapas:

- **Consulta à Loteria:** através da qual o apostador pode obter informações sobre jogos com extrações abertas, preços de apostas, valores dos prêmios e resultados de extrações anteriores;

- **Autenticação do Apostador:** utilizando o certificado digital obtido na fase de cadastramento, o apostador deve se identificar perante a loteria digital, recebendo acesso aos seus serviços;

- **Aquisição de Créditos:** na qual o apostador adquire créditos com o valor correspondente à aposta que deseja efetuar;

- **Validação da Aposta:** permite ao apostador utilizar os créditos previamente adquiridos para efetuar sua aposta, recebendo em troca um comprovante de apostas digital.

Quando o período válido para a realização de apostas terminar, o protocolo prosseguirá com as seguintes fases:

- **Encerramento da Extração:** consiste na apuração dos totais acumulados, realização do sorteio e divulgação do resultado da loteria;

- **Requisição da Premiação:** última fase do protocolo, realizada apenas pelos apostadores vencedores. Estes apostadores devem apresentar à loteria seu comprovante premiado, que passará por um processo de verificação a fim de que o prêmio possa ser pago.

A explicação detalhada de cada uma dessas fases é apresentada ao longo deste capítulo. Inicialmente é definida a notação adotada no protocolo.

5.1 Notação

Para permitir uma perfeita compreensão do protocolo, a seguinte notação é utilizada para descrever entidades envolvidas e ferramentas criptográficas:

- LD: loteria digital; entidade responsável pelos jogos de loteria;
- ADM: administrador, pessoa responsável pela configuração da loteria;
- AP: apostador; aquele que realiza apostas;
- Crédito: documento digital assinado que assegura ao seu beneficiário o direito de fazer uma aposta no valor nele especificado;
- EC: emissor de créditos; entidade responsável por receber o pagamento dos apostadores, emitindo em troca créditos assinados no valor correspondente;
- idAP: identidade do apostador AP;
- idEC: identidade do emissor de créditos EC;
- idCR: identificador do crédito emitido por EC;
- RM: rede de misturadores; entidade responsável por garantir o anonimato das apostas;
- H(x): função de calcula o resumo (hash) da mensagem x;
- $S_K(x)$: função que assina a mensagem x com a chave K;
- $E_K(x)$: função que cifra a mensagem x com a chave K.

5.2 Fase de estabelecimento da loteria

Na primeira fase do protocolo, são realizadas tarefas relacionadas à criação da loteria digital *LD*. Inicialmente, deve ser gerado o par de chaves de *LD*. Em seguida, uma autoridade certificadora *AC* deve emitir um certificado digital padrão x.509 v3 para *LD*. Este certificado deverá ser amplamente divulgado de modo que a chave pública nele contida possa ser usada para verificar assinaturas digitais produzidas por *LD*, bem como para sua autenticação perante os apostadores.

Além do certificado de *LD*, deve-se emitir certificados digitais para os administradores da loteria, responsáveis pelo cadastramento e manutenção das informações sobre jogos, extrações e resultados da loteria. Estes certificados serão usados na autenticação dos administradores perante a loteria digital.

Para obter seu certificado, cada administrador deverá gerar seu par de chaves, gerar uma requisição de certificado e enviá-la à autoridade certificadora *AC* responsável por emitir certificados digitais para *LD*. A requisição será verificada por *AC* e, caso seja aprovada, será emitido um certificado digital contendo a extensão crítica `idadministrador`. Esta extensão contém um identificador único do administrador e também é usada para reconhecer certificados de administradores. `idadministrador` é definido em ASN.1 conforme mostrado abaixo:

```
idadministrador ATTRIBUTE ::= {
    WITH SYNTAX identificador
    ID oid-administrador }

identificador VisibleString (FROM (“0”…“9”|“/.-”))

oid-administrador OBJECT-IDENTIFIER ::= {iso(1) org(3)
    dod(6) internet (1) private(4) enterprise(1)
    ufsc/labsec(7687) lottuseg(12) idadministrador(1)}
```

5.3 Fase de cadastramento de apostadores

Conforme definido pelo requisito de autenticação, é necessário garantir que apenas apostadores autorizados possam apostar na loteria digital. A forma proposta para autorizar estes apostadores é emitir certificados digitais para sua identificação e autenticação.

Desta forma, cada apostador *AP* deverá gerar seu par de chaves, gerar uma requisição de certificado digital e enviá-la para uma autoridade certificadora *AC* na qual a loteria digital *LD* confie. *AC* se responsabilizará por verificar as informações providas por *AP* e, caso a requisição seja aprovada, deverá emitir um certificado digital para *AP*.

A fim de garantir que o certificado possa identificar inequivocamente o apostador ao qual se relaciona, este trabalho propõe que nele seja incluída a extensão não crítica `idapostador`. Esta extensão contém o número de um documento de identificação do apostador em seu país de origem e tem por função complementar as informações contidas no "Distinguished Names" do certificado digital. `idapostador` é definido em ASN.1 conforme mostrado abaixo:

```
idapostador ATTRIBUTE ::= {
    WITH SYNTAX identificador
    ID oid-apostador }

identificador VisibleString (FROM ("0"…"9"|"/.-"))

oid-apostador OBJECT-IDENTIFIER ::= {iso(1) org(3) dod(6)
    internet (1) private(4) enterprise(1)
    ufsc/labsec(7687) lottuseg(12) idapostador(2)}
```

Vale observar que esta extensão não é obrigatória e sua função pode ser desempenhada por outras extensões. No caso do Brasil, a legislação que regulamenta a Infraestrutura de Chave Pública [BRAg] define um conjunto de extensões válidas para certificados utilizados em aplicações como confirmação de identidade na Web, correio eletrônico, transações on-line, redes privadas virtuais, transações eletrônicas e assinatura de documentos eletrônicos com verificação da integridade de suas informações. Uma dessas extensões é a "Subject Alternative Name", obrigatória e não crítica, formada por um único campo otherName composto por:

- OID = 2.16.76.1.3.1
- Conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato *ddmmaaaa*; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subseqüentes, o número de inscrição do titular no PIS/PASEP; nas 11 (onze) posições subseqüentes, o número do Registro Geral (RG) do titular; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva unidade da federação.

5.4 Fase de Configuração de Jogos e Extrações

Para que os apostadores façam suas apostas é necessário que a loteria disponha de pelo menos um jogo com regras definidas, que especifiquem, por exemplo, as dezenas que podem compor uma aposta, o número de dezenas a serem sorteadas e o preço de uma aposta. Além disso, também deve ter extrações definidas, que indiquem, dentre outras coisas, a data do sorteio do jogo ao qual se refere e o período de tempo válido no qual se pode apostar para concorrer a um determinado prêmio. No Lottuseg, o cadastramento destas informações é responsabilidade do administrador *ADM*.

Para a realização destas tarefas, propõe-se que a troca de informações entre *ADM* e *LD* seja feita através do protocolo SSL, capaz de prover confidencialidade, integridade e identificação ao processo de comunicação. Segundo esta abordagem, *ADM* e *LD* devem realizar uma autenticação mútua usando os certificados digitais obtidos durante a fase de estabelecimento da loteria.

Feita a autenticação, as informações que compõem um jogo ou uma extração podem ser enviadas para a loteria, devendo, para tanto, ser digitalmente assinadas por *ADM*. A seguir, *LD* verifica esta assinatura e, caso seja válida, toma as informações recebidas e as assina, reconhecendo que vieram de uma fonte confiável.

As informações assinadas e validadas pela loteria devem ser armazenadas em uma base de dados disponibilizada para consultas dos apostadores. Esta base será o repositório de jogos e regras vigentes, bem como extrações válidas. A cópia original das informações sobre jogos e extrações, assinada pelo administrador, deve ser armazenada em uma base de dados de auditoria, garantindo que todo o histórico de modificações sobre jogos e extrações fique registrado.

A Figura 5.1, explicada a seguir, ilustra o processo de configuração de jogos.

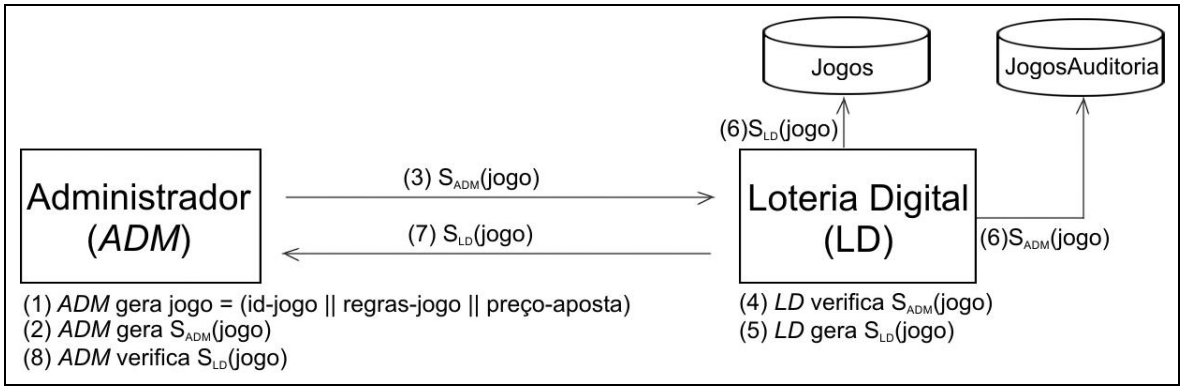

Figura 5.1 – Configuração de um jogo.

(1) *ADM* gera um jogo composto por: (a) o identificador do jogo; (b) regras do jogo e (c) o preço da aposta;

(2) *ADM* assina o jogo produzindo S_{ADM}(jogo);

(3) *ADM* envia S_{ADM}(jogo) para *LD*;

(4) *LD* verifica a assinatura de S_{ADM}(jogo). Se a assinatura não for válida, aborta a configuração do jogo;

(5) *LD* assina o jogo recebido produzindo S_{LD}(jogo);

(6) *LD* insere S_{LD}(jogo) na base de dados de jogos. Se o jogo já tiver sido cadastrado previamente, armazena as alterações. Além disso, insere um registro contendo S_{ADM}(jogo) na base de dados de auditoria;

(7) *LD* envia S_{LD}(jogo) para *ADM* confirmando a operação;

(8) *ADM* verifica assinatura de S_{LD}(jogo). Se a assinatura for válida, considera que a operação foi concluída com sucesso.

Um processo semelhante ao descrito acima é realizado para a configuração de extrações. Este processo é ilustrado na Figura 5.2, explicada a seguir.

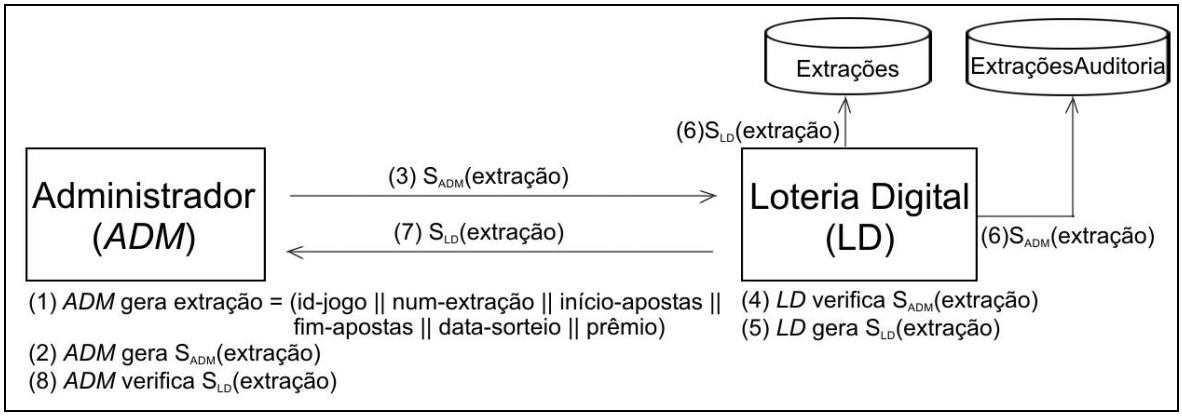

Figura 5.2 – Configuração de uma extração.

(1) *ADM* gera uma extração composta por: (a) o identificador do jogo; (b) número da extração; (c) a data de início do período de apostas; (d) a data final do período de apostas; (e) a data do sorteio e (f) o valor do prêmio;

(2) *ADM* assina a extração produzindo S_{ADM}(extração);

(3) *ADM* envia S_{ADM}(extração) para *LD*;

(4) *LD* verifica a assinatura de S_{ADM}(extração). Se a assinatura não for válida, aborta a configuração da extração. Caso o jogo identificado por id-jogo não exista na base de dados de jogos, a configuração da extração também é abortada;

(5) *LD* assina a extração recebida produzindo S_{LD}(extração);

(6) *LD* insere S_{LD}(extração) na base de dados de extrações. Se a extração já tiver sido cadastrada previamente, armazena as alterações. Além disso, insere um registro contendo S_{ADM}(extração) na base de dados de auditoria;

(7) *LD* envia S_{LD}(extração) para *ADM* confirmando a operação;

(8) *ADM* verifica assinatura de S_{LD}(extração). Se a assinatura for válida, considera que a operação foi concluída com sucesso.

5.5 Fase de Apostas

Esta é a fase central do Lottuseg, através da qual um apostador submete uma aposta e o pagamento correspondente à loteria, recebendo em troca um comprovante de apostas digital. Para tornar mais simples a compreensão deste processo, a fase de apostas foi subdividida em etapas: consulta à loteria, autenticação do apostador, aquisição de créditos e validação da aposta. Estas etapas são explicadas a seguir.

5.5.1 Etapa de consulta à loteria

Através desta etapa, o apostador *AP* pode obter informações sobre os jogos com extrações abertas, sendo capaz de decidir em que jogo apostar. Considera-se que uma extração está aberta quando a data corrente for maior que a data de início e menor que a data de fim do período de apostas.

Para realizar a consulta, *AP* deve enviar uma requisição a *LD*, que recupera em seu repositório os dados sobre os jogos com extrações abertas e os devolve para *AP*. Esta seqüência de passos é ilustrada na Figura 5.3 e explicada em detalhes a seguir.

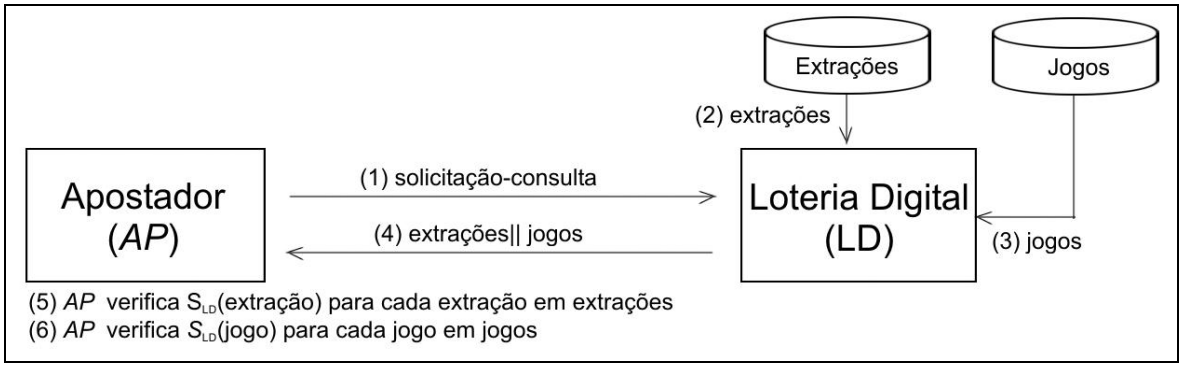

Figura 5.3 – Etapa de consulta à loteria.

(1) *AP* envia a *LD* uma solicitação de consulta às informações da loteria;

(2) A partir de seu repositório de dados, *LD* obtém extrações, que corresponde ao conjunto de todas as extrações que satisfazem à condição de que a data corrente esteja entre a data de início e a data de fim do período de apostas daquela extração. Todas as extrações encontram-se assinadas e apresentam a

seguinte estrutura: S_{LD}(id-jogo || num-extração || início-apostas || fim-apostas || data-sorteio || prêmio);

(3) A partir de seu repositório de dados, *LD* obtém jogos, que corresponde ao conjunto de todos os jogos que se relacionam às extrações contidas em extrações. Todos os jogos encontram-se assinados e apresentam a seguinte estrutura: S_{LD}(id-jogo || regras-jogo || preço-aposta);

(4) *LD* envia extrações e jogos para *AP*;

(5) *AP* verifica as assinaturas de todas as extrações contidas em extrações;

(6) *AP* verifica as assinaturas de todos os jogos contidos em jogos.

Os jogos e extrações que tiverem assinaturas válidas são considerados válidos e constituem opções de aposta. É importante observar que as informações serão usadas nas fases subseqüentes para que o apostador conheça: (a) os preços das apostas e valores dos prêmios, podendo adquirir créditos no valor correto para a aposta que pretende realizar; (b) as regras que regem o jogo no qual pretende apostar, incluindo quantidade de prognósticos e seus valores possíveis, de modo que possa gerar sua aposta corretamente.

5.5.2 Etapa de Autenticação do Apostador

Uma vez que o apostador *AP* disponha de um certificado digital que permita sua identificação, poderá se autenticar perante a loteria digital *LD* e fazer uso dos serviços por ela providos. Por outro lado, *LD* também deverá se autenticar perante *AP*, de modo que *AP* tenha certeza de que estará realizando suas apostas com a loteria digital pretendida. Para atender a esta necessidade de autenticação mútua, propõe-se a adoção do protocolo SSL, tal qual utilizado entre *LD* e *ADM*. Com isso, *AP* e *LD* disporão de um canal de comunicação provido de confidencialidade e integridade.

5.5.3 Etapa de Aquisição de Créditos

A fim de oferecer flexibilidade à loteria digital, propõe-se a separação entre os procedimentos de pagamento e aposta, permitindo-se que várias formas de pagamento (cartão de crédito, débito em conta, dinheiro digital, etc) possam ser utilizadas pelo apostador sem que o mecanismo de apostas seja alterado. Esta separação baseia-se na idéia de utilizar créditos como moeda da loteria. Assim, antes de apostar, o apostador *AP* deverá adquirir o valor em créditos correspondente à sua aposta em um emissor de créditos *EC*. A própria loteria digital pode desempenhar o papel de emissor de créditos, ou pode delegá-lo a entidades como bancos.

Os passos que compõem a etapa de emissão de créditos estão ilustrados na Figura 5.4 e serão explicados a seguir.

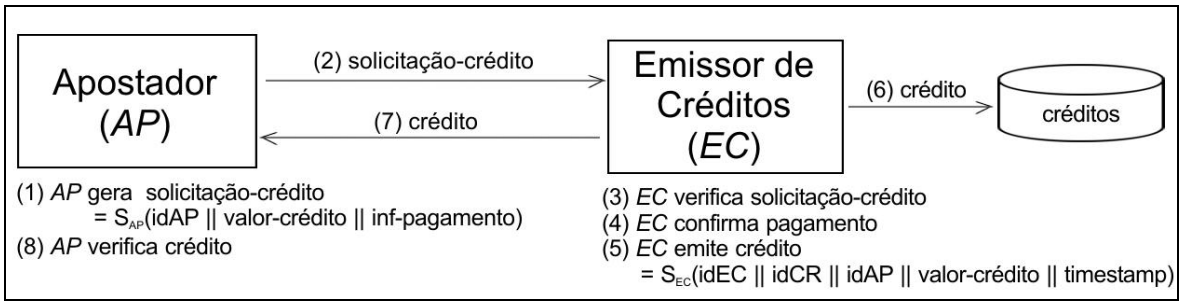

Figura 5.4 – Etapa de aquisição de créditos.

(1) *AP* gera uma solicitação de crédito assinada. Esta solicitação é composta por: (a) o identificador de *AP*; (b) o valor em créditos que deseja adquirir e (c) as informações necessárias para o pagamento do crédito. O identificador de *AP* pode ser o número de um documento que o identifica ou o seu certificado digital. As informações de pagamento podem incluir números de cartão de crédito, contas correntes, etc;

(2) *AP* envia a solicitação de crédito produzida para *EC*;

(3) *EC* verifica a assinatura da solicitação de crédito. Caso a verificação seja mal sucedida, aborta a emissão do crédito;

(4) *EC* confirma a disponibilidade financeira de *AP* para o pagamento do crédito de acordo com a forma de pagamento escolhida. Caso a disponibilidade não seja confirmada, aborta a emissão do crédito;

(5) *EC* emite um crédito assinado em benefício de *AP*. Este crédito é composto por: (a) identificador de *EC*, (b) identificador do crédito, (c) identificador de *AP*, (c) valor do crédito e (d) data e hora de emissão do crédito. O identificador de *EC* pode ser o número de um documento que identifique a entidade emissora de créditos ou o seu certificado digital. O identificador do crédito é um número que identifica unicamente aquele crédito dentro da entidade que o emitiu;

(6) *EC* armazena o crédito emitido;

(7) *EC* envia o crédito gerado para *AP*;

(8) *AP* verifica a assinatura do crédito e, caso a verificação seja bem sucedida, armazena-o.

É importante observar que os créditos emitidos nesta etapa são nominais a um determinado apostador. Optou-se por esta abordagem porque oferece maior segurança aos apostadores, uma vez que se pode impor no protocolo que um crédito apenas poderá ser gasto se estiver assinado por seu beneficiário. Desta forma, evita-se que um crédito seja roubado e utilizado indevidamente.

Um outro aspecto importante a ser ressaltado é que o protocolo Lottuseg considera que a entidade emissora de créditos deve ser confiável. Este é um requisito primordial, uma vez que *EC* terá acesso a informações como números de cartão de crédito.

5.5.4 Etapa de validação da aposta

Nesta etapa, o apostador enviará sua aposta para a loteria digital, efetuará o pagamento usando um crédito e, em troca, receberá um comprovante que lhe permitirá reclamar a premiação caso seja vencedor.

Em um sistema convencional de loteria, no qual as apostas são realizadas pessoalmente, o apostador preenche uma aposta com os prognósticos escolhidos e a entrega, junto com seu pagamento, em um posto de vendas da loteria. Por sua vez, o posto de vendas verifica a aposta e o pagamento e, caso estejam corretos, registra-os e emite um comprovante de apostas para o apostador.

Em uma loteria digital, entretanto, este processo não pode acontecer exatamente desta forma, pois o protocolo não seria resistente a falhas. Caso o apostador envie o pagamento e a aposta para a loteria digital, poderia jamais receber um comprovante de apostas se acontecesse algum problema de comunicação com a loteria ou se esta loteria fosse maliciosa. Por outro lado, se a loteria emitisse um comprovante de apostas e o enviasse ao apostador antes de receber o pagamento, também poderia ter prejuízos.

Além disso, se o modelo tradicional fosse usado em loterias digitais, o requisito da privacidade do apostador também não seria atendido. Em uma loteria digital, a fim de garantir que apenas apostadores autorizados possam jogar na loteria, os canais de comunicação devem ser identificados. Desta forma, se um usuário submetesse sua aposta diretamente para a loteria digital, a mesma poderia associá-lo à sua aposta.

Assim, a fim de solucionar estas questões, propõe-se que:

- Seja criada uma associação entre a aposta e o crédito usado em seu pagamento, de modo que todo crédito recebido pela loteria esteja diretamente relacionado a uma aposta. Com isso, para a loteria negar o recebimento de uma aposta, terá que negar o recebimento de seu pagamento. Esta associação, contudo, deverá ser secreta e o segredo capaz de revelar este relacionamento deve ser conhecido apenas pelo apostador, de modo a assegurar sua privacidade. Uma forma de conseguir este relacionamento implícito consiste em usar o protocolo de comprometimento de bits;

- Os prognósticos de um apostador sejam enviados para a loteria de forma anônima usando uma rede de misturadores.

O procedimento completo para etapa de validação de apostas encontra-se ilustrado na Figura 5.5 e é explicado em detalhes a seguir. Considera-se que as

informações referentes a jogos e extrações, incluindo seus identificadores, quantidade de prognósticos que devem compor uma aposta e valores válidos para os prognósticos, bem como os créditos necessários para a efetivação da aposta, foram obtidos ao longo das etapas anteriores do protocolo.

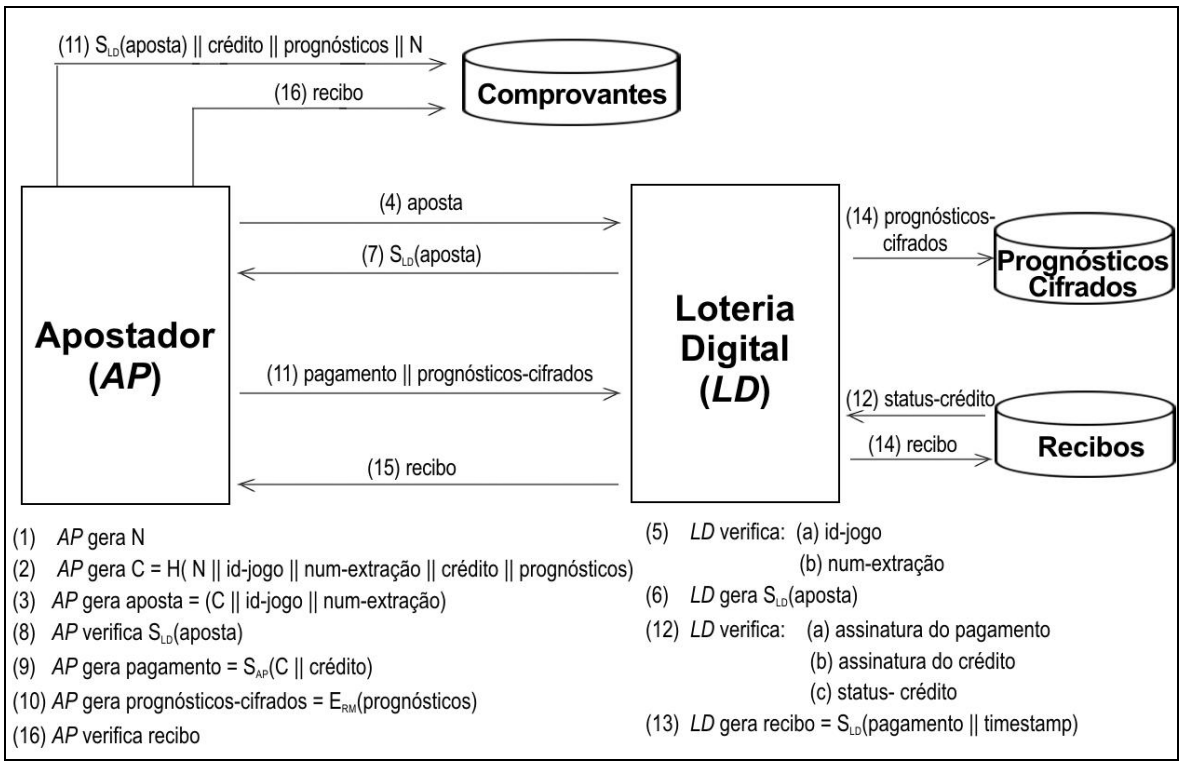

Figura 5.5– Etapa de Validação de Apostas.

(1) *AP* gera um número aleatório N;

(2) *AP* gera o comprometimento de bits C, obtido pela aplicação de uma função resumo H sobre: (a) N; (b) o identificador do jogo; (c) o número da extração; (d) o crédito a ser usado para pagamento e (e) os prognósticos escolhidos. Através deste comprometimento, o apostador associa os prognósticos que deseja apostar à sua identidade, contida no crédito;

(3) *AP* gera sua aposta, composta por: (a) o comprometimento C; (b) o identificador do jogo e (c) o número da extração. É importante observar que os prognósticos não compõem diretamente a aposta, mas estão implicitamente representados através do comprometimento C;

(4) *AP* envia a aposta para *LD* a fim de que seja assinada;

(5) *LD* verifica se o identificador do jogo e o número da extração que compõem a aposta são válidos. Se não forem, o protocolo é encerrado;

(6) *LD* assina a aposta recebida;

(7) *LD* envia a aposta assinada para *AP*;

(8) *AP* verifica a assinatura da aposta. Se a assinatura não for válida, o protocolo é encerrado;

(9) *AP* gera o pagamento da aposta, formado por: (a) um crédito e (b) o comprometimento C que relaciona o crédito à aposta, gerado no passo 2. O pagamento é assinado pelo apostador e esta assinatura é requisito para que o valor do crédito possa ser recebido junto ao emissor de créditos. Assim, como esta assinatura também é gerada sobre o comprometimento C, cada crédito gasto guarda informações que permitem relacioná-lo a uma aposta;

(10) *AP* cifra com a chave pública de *RM* os prognósticos por ele escolhidos;

(11) *AP* envia para *LD* a mensagem de pagamento e os prognósticos cifrados. Além disso, armazena a aposta assinada, os prognósticos escolhidos, o crédito usado para pagamento e N;

(12) *LD* verifica: (a) a validade da assinatura de *AP* na mensagem de pagamento; (b) a validade da assinatura de *EC* no crédito contido na mensagem de pagamento e (c) se o crédito já foi gasto anteriormente (usando idCR). Se alguma das verificações falhar, o protocolo é encerrado;

(13) *LD* gera e assina um recibo de pagamento. Este recibo é composto pela mensagem de pagamento recebida no passo (11) e pela data e hora de emissão do recibo. Esta datação tem por função registrar o instante de validação da aposta, que deve estar contido dentro do período válido de apostas;

(14) *LD* armazena o recibo emitido no passo (13) e a aposta cifrada recebida no passo (11). A operação de armazenagem destes dois itens deve ser uma

transação indivisível, de modo a garantir que prognósticos e recibo correspondentes sejam corretamente armazenados;

(15) *LD* envia o recibo de pagamento para *AP*;

(16) *AP* verifica a assinatura do recibo e, se a mesma for válida, armazena o recibo, completando o comprovante de apostas. Este comprovante é composto por: (a) a aposta assinada; (b) o recibo de pagamento e (c) N.

Uma vez que a aposta assinada é igual a S_{LD}(C || id-jogo || num-extração) e seu recibo corresponde a S_{LD}(C || crédito || timestamp), verifica-se que estes dois elementos estão diretamente associados pelo comprometimento C. Contudo, apenas conhecendo-se N é possível recalcular C = H(N || id-jogo || num-extração || crédito || prognósticos) e provar que a aposta foi feita sobre um certo conjunto de prognósticos. Desta forma, o comprovante de apostas precisa ter esta tripla composição.

Por fim, com o objetivo de assegurar a tolerância a falhas, foi definido um procedimento de recuperação para os casos em que *AP*, por exemplo, perca a conexão com *LD* antes que tenha recebido o recibo. A Figura 5.6 ilustra este procedimento, que é explicado a seguir.

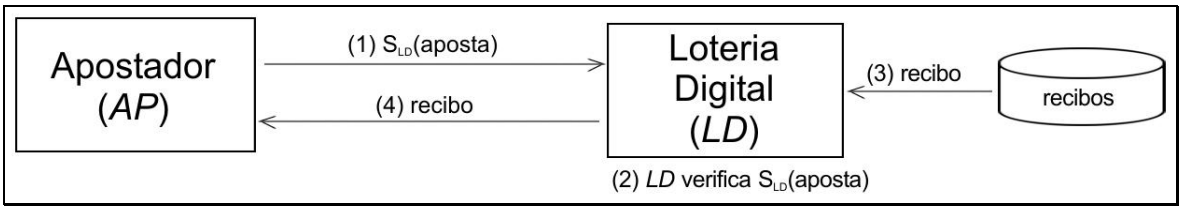

Figura 5.6– Procedimento de recuperação.

(1) *AP* envia para *LD* sua aposta, formada pelo comprometimento C, o identificador do jogo e o número da extração;

(2) Após receber a aposta, *LD* verifica sua assinatura. Caso não seja válida, o procedimento é encerrado;

(3) *LD* pesquisa em seu repositório de recibos se existe, para aquele jogo e extração, algum crédito relacionado a C. Se não houver, o procedimento é encerrado;

(4) *LD* envia o recibo validado para *AP*.

5.6 Fase de Encerramento da Extração

5.6.1 Etapa de Apuração

Após o encerramento do período de apostas, *LD* deve apurar o total acumulado verificando o valor total dos créditos recebidos como pagamento. Finalizada esta apuração, *LD* deve publicar uma lista assinada contendo os identificadores dos créditos recebidos e os comprometimentos a eles relacionados. O cabeçalho desta lista deve conter o identificador do jogo, número da extração e o total acumulado.

Através da emissão desta lista de apuração, garante-se a honestidade do processo lotérico, uma vez que não será possível, depois do sorteio da loteria, gerar uma aposta vencedora, pois o crédito a ela relacionado não constará na lista. Para dar maior segurança a este processo, propõe-se que a lista de apuração seja datada por uma protocoladora digital de documentos [PAS02].

Para concluir a etapa de apuração, *LD* deve enviar para a rede de misturadores *RM* todos os prognósticos cifrados recebidos na etapa de validação de apostas. *RM* se encarregará de decifrá-los e misturá-los, devolvendo-os então para *LD*. Desta forma, *LD* terá acesso aos prognósticos apostados, podendo, após o sorteio, determinar se houve vencedores na extração.

5.6.2 Etapa de cadastramento de resultados

Uma vez que tenha sido realizado o sorteio, um administrador *ADM* deve cadastrar no sistema o resultado da extração e verificar se houve vencedores. Estas tarefas, ilustradas na Figura 5.7, são executas conforme o conjunto de passos descritos a seguir.

(1) *ADM* gera o resultado a ser registrado na loteria, composto por: (a) o identificador do jogo; (b) o número da extração e (c) os prognósticos sorteados;

(2) *ADM* assina o resultado produzindo S_{ADM}(resultado);

(3) *ADM* envia S_{ADM}(resultado) para *LD*;

(4) *LD* verifica a assinatura de S_{ADM}(resultado). Se a assinatura não for válida, aborta o cadastramento de resultados;

(5) *LD* assina o resultado recebido produzindo S_{LD}(resultado), confirmando que foi recebido de uma fonte válida;

(6) *LD* insere S_{LD}(resultado) no repositório de resultados. Além disso, insere S_{ADM}(resultado) no repositório de auditoria;

(7) *LD* verifica no repositório de prognósticos quantas apostas vencedoras foram realizadas para o jogo e extração em questão;

(8) *LD* gera uma mensagem assinada confirmando o cadastramento de resultados. Esta mensagem é composta por: (a) o identificador do jogo; (b) o número da extração e (c) o número de vencedores;

(9) *LD* envia a confirmação para *ADM*;

(10) *ADM* verifica assinatura da mensagem de confirmação. Se a assinatura for válida, considera que a operação foi concluída com sucesso.

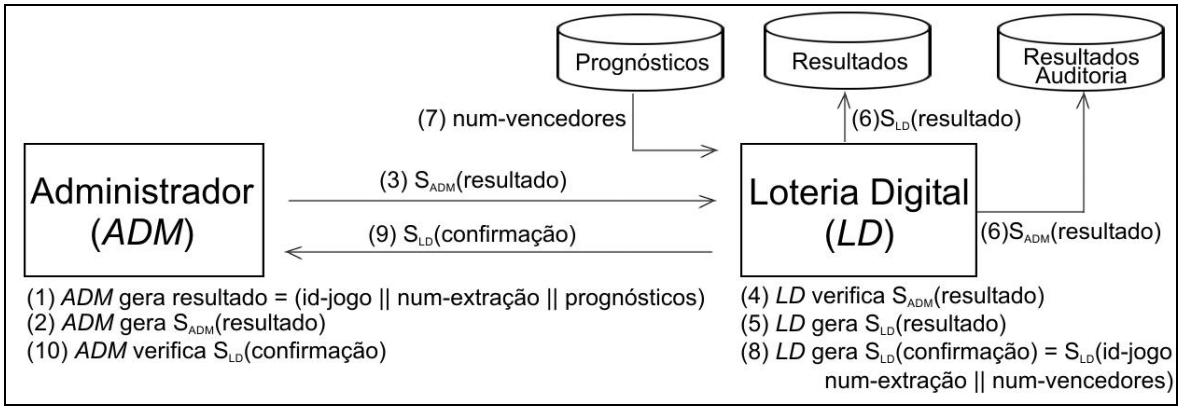

Figura 5.7– Cadastramento de Resultados.

5.7 Fase de Requisição da Premiação

A última fase do protocolo é opcional e só deve ser executada quando um apostador constatar ser portador de uma aposta premiada. Nesta situação, *AP* deve apresentar à *LD* o seu comprovante digital, que lhe permitirá receber a premiação. Este comprovante é composto por três elementos: (a) uma aposta assinada por *LD*; (b) um recibo também assinado por *LD* e (c) o número aleatório N que prova o relacionamento entre o jogo e extração contidos na aposta, o crédito contido no recibo e os prognósticos vencedores.

Desta forma, esta fase consiste dos seguintes passos, ilustrados pela Figura 5.8.

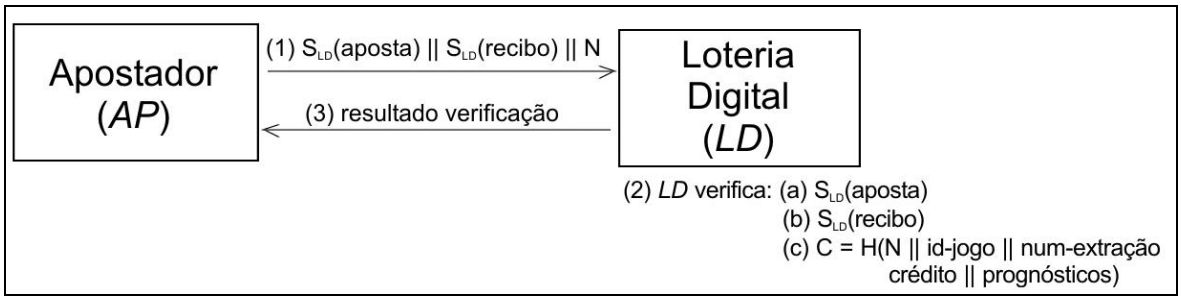

Figura 5.8– Requisição da premiação.

(1) *AP* envia para *LD* o seu comprovante de apostas;

(2) *LD* verifica: (a) se a assinatura da aposta e do recibo são válidas; (b) se o crédito e comprometimento contidos no recibo estão na lista produzida ao final da etapa de apuração da acumulação e (c) se o número aleatório N contido no comprovante prova o comprometimento entre a aposta S_{LD}(C || id-jogo || num-extração) e o crédito contido no recibo S_{LD}(C || crédito || timestamp). Para tanto, deve-se recalcular o valor do resumo C = H(N || id-jogo || num-extração || crédito || prognósticos) tomando por base os prognósticos vencedores e os valores contidos na aposta e no recibo. Caso todos as verificações sejam realizadas com sucesso, o comprovante fornecido é considerado premiado;

(3) *LD* reporta o resultados das verificações à *AP*. Caso o resultado seja positivo, *LD* e *AP* entram em negociação para determinar como o pagamento do prêmio será realizado. Poderão ser adotadas várias soluções, como o depósito

do prêmio em uma conta do apostador ou emissão de uma ordem de pagamento digital em benefício do apostador.

5.8 Conclusão

Este capítulo apresentou o Lottuseg, um protocolo seguro para loteria digital que contempla todas as etapas do processo lotérico, incluindo desde procedimentos iniciais para a criação da loteria, até procedimentos para a validação de apostas e requisição de premiação. Como cerne deste protocolo está a idéia de fornecer comprovantes de apostas digitais verificáveis e não falsificáveis ao apostador, capazes de provar a realização de uma aposta. A segurança e a funcionalidade do protocolo apresentado serão avaliadas no capítulo seguinte.

Capítulo 6

Discussão do Lottuseg

Este capítulo trata da discussão do protocolo Lottuseg, tomando por base os requisitos funcionais e de segurança sugeridos para um protocolo de loteria digital. Nesta discussão, maior enfoque será dado às questões de segurança, uma vez que o principal objetivo deste trabalho é estabelecer um modelo confiável para loteria digital. Antes do tratamento destes requisitos, contudo, serão definidos os pressupostos para o correto funcionamento do protocolo.

6.1 Definições

A utilização do protocolo Lottuseg para oferecer serviços seguros de loteria considera como válidas as seguintes hipóteses:

- **Honestidade da Rede de Misturadores:** a fim de assegurar que a loteria só terá acesso aos prognósticos depois do encerramento da fase de apostas, a rede deve ser honesta. Por definição, uma rede de misturadores é honesta se pelo menos um dos misturadores que compõem a rede for honesto;

- **Confiabilidade no processo de protocolação digital da lista de apuração:** a lista de apuração gerada após o encerramento do período de apostas contém informações sobre todos os créditos gastos em uma extração. A sua protocolação assegura que a loteria não poderá modificá-la depois da realização do sorteio. A necessidade da confiabilidade nesta protocolação relaciona-se aos

requisitos de irretratabilidade e não-falsificação e será melhor compreendia ao longo do restante deste capítulo.

6.2 Discussão dos Requisitos de Segurança

6.2.1 Autenticação

No Lottuseg, obtém-se autenticação através do uso do protocolo SSL, que deve ser configurado para requerer que os apostadores se identifiquem utilizando certificados digitais emitidos durante a fase de cadastramento de apostadores. Considera-se que a posse de um certificado digital confiável e sua chave privada correspondente é suficiente para provar a elegibilidade de um apostador. A confiabilidade do certificado depende da confiabilidade que a Loteria Digital deposita na Autoridade Certificadora que o emitiu. É esta autoridade que detém a responsabilidade de verificar se um apostador tem idade mínima para apostar e se reside em uma área na qual a loteria é autorizada a operar.

6.2.2 Confidencialidade

Através da utilização da rede de misturadores, os prognósticos que compõem as apostas apenas são conhecidos pela loteria digital ao final do período de apostas. Desta forma, não é possível obter estatísticas sobre os valores apostados enquanto for possível realizar apostas. Por outro lado, a utilização do protocolo SSL para a comunicação entre loteria digital e apostador permite o estabelecimento de um canal de comunicação sigiloso, no qual informações como números de cartão de crédito podem trafegar de modo seguro.

6.2.3 Integridade

Também em função da utilização do protocolo SSL, pode-se garantir a integridade das informações que trafegam entre a loteria digital e o apostador. Depois da efetivação de uma aposta, a integridade tanto do comprovante entregue ao apostador quanto do recibo armazenado pela loteria é garantida através das assinaturas digitais geradas pela loteria

sobre estas informações. Qualquer tentativa de modificação indevida do conteúdo de um recibo ou aposta pode ser identificada através da verificação da assinatura.

6.2.4 Privacidade

Como os prognósticos de cada apostador são enviados à loteria digital através de uma rede de misturadores, a loteria não é capaz de associar diretamente uma aposta ao indivíduo que a produziu. Contudo, em função da necessidade de autenticação, a loteria terá conhecimento dos apostadores que participaram de uma certa extração, bem como dos montantes por eles apostados.

6.2.5 Irretratabilidade

No Lottuseg, uma aposta passa a ser considerada válida quando seu pagamento for efetuado. Para isso, o apostador deverá gerar uma mensagem de pagamento, constituída por um crédito comprometido implicitamente aos prognósticos apostados. Ao receber este pagamento, a loteria deverá enviar para o apostador um recibo assinado. Além disso, ao final do período de apostas, a loteria deverá publicar na lista de apuração contendo informações sobre os créditos recebidos. Como esta lista também é assinada, a loteria estará duplamente comprometida e não poderá negar o recebimento de um crédito e, conseqüentemente, a realização da aposta ao qual ele se relaciona.

6.2.6 Intempestividade

A fim de garantir que as apostas apenas sejam recebidas dentro do período válido, os recibos digitais emitidos pela loteria são datados. Além disso, a lista de apuração é protocolada através de um procedimento confiável, o que impede inclusive a loteria digital de inserir apostas em um período de tempo indevido.

6.2.7 Verificabilidade

Durante o processo de apostas, é possível que o apostador se certifique da validade da aposta e de seu recibo através da verificação das assinaturas geradas pela loteria digital. Estas assinaturas também são usadas no momento da requisição da premiação para que a loteria digital possa verificar a validade do comprovante de apostas. Além disso, a loteria digital também é capaz de verificar a validade do relacionamento entre o crédito contido no comprovante e um conjunto de prognósticos. Como conseqüência direta desta propriedade, é possível que a loteria verifique a autoria de uma aposta, uma vez que os créditos são nominais aos apostadores.

6.2.8 Não-falsificação

Tomando como princípio o sigilo da chave privada da loteria digital, não é possível a uma entidade diferente da loteria emitir comprovantes de apostas verificáveis, pois sua assinatura digital não poderá ser corretamente gerada. Para impedir tentativas de fraude por parte da própria loteria digital, é publicada uma lista de apuração digitalmente assinada, contendo a relação de todos os créditos recebidos em uma extração. Em função desta lista, a loteria não poderá forjar comprovantes de apostas para extrações realizadas, pois créditos de pagamento e comprometimentos com apostas não poderão ser inseridos em uma lista já publicada e protocolada.

6.2.9 Não-duplicação

Cada comprovante digital está diretamente relacionado a um crédito de pagamento. Como este crédito é único e é nominal a um apostador, não é possível duplicar um comprovante de apostas sem que haja detecção.

6.3 Discussão dos Requisitos Funcionais

6.3.1 Tolerância a falhas

O Lottuseg é reversível até o instante em que o pagamento é efetuado, pois o apostador não dispõe de um comprovante de apostas. A partir deste momento, o apostador poderá usar o recibo emitido para completar o seu comprovante de apostas, passando a estar apto a requisitar a premiação caso seja necessário. Caso o apostador envie o pagamento para a loteria e não obtenha o recibo, poderá solicitá-lo através do procedimento de recuperação especificado no protocolo, confirmando assim que o pagamento de sua aposta foi registrado corretamente. Caso verifique que o pagamento não foi registrado, poderá reiniciar o protocolo.

6.3.2 Mobilidade

Um apostador pode utilizar o Lottuseg para submeter suas apostas a partir de qualquer terminal conectado à Internet. A única restrição existente é a disponibilidade de um certificado digital para o processo de autenticação, bem como de sua chave privada correspondente para a geração de assinaturas digitais.

6.3.3 Flexibilidade

Uma vez que o conjunto de prognósticos de uma aposta pode corresponder a qualquer tipo de informação, o protocolo especificado pode ser utilizado em vários tipos de loteria. Por exemplo, em loterias esportivas os prognósticos podem ser compostos por resultados de jogos, enquanto que em loterias de números podem ser compostos por um conjunto de dezenas.

6.3.4 Conveniência

O protocolo proposto permite que um comprovante de apostas possa ser usado para fazer uma requisição on-line de premiação. Além disso, se for conveniente ao apostador, também é possível fazer sua impressão e solicitar a premiação pessoalmente. Esta segunda alternativa é viável porque assinaturas e certificados digitais são conjuntos de bits, podendo ser diretamente impressos. Alternativamente, também é possível adotar algum padrão, como um formato de código de barra, para sua impressão.

6.3.5 Escalabilidade

A escalabilidade de um sistema está diretamente relacionada às alternativas utilizadas para sua implementação. Como questões de implementação estão fora do escopo deste trabalho, este requisito não será analisado.

6.4 Conclusão

Ao longo desta discussão, procurou-se mostrar que o protocolo Lottuseg é confiável tomando como parâmetros os requisitos de segurança definidos neste trabalho. Além disso, foi apresentado que em termos de funcionalidade este protocolo também se adequa ao que foi estabelecido.

Capítulo 7

Considerações Finais

Este trabalho apresentou uma proposta de protocolo criptográfico para realização segura de apostas de loteria através de redes de computadores como a Internet, constituindo o resultado final de uma pesquisa de mestrado na área de criptografia e segurança de computadores.

O processo para definição deste protocolo envolveu várias fases. Inicialmente, foi realizado um estudo sobre as etapas constituintes do processo lotérico tradicional, bem como das entidades que interagem durante sua execução. Foram também observados alguns mecanismos utilizados pelas loterias tradicionais para garantir sua segurança e a legislação vigente no Brasil para a regulamentação de loterias.

Uma evolução natural deste estudo levou ao levantamento de soluções disponíveis para a implementação de loterias digitais, culminando com uma análise das loterias digitais federais da França, Inglaterra e Austrália, bem como de trabalhos científicos que tratam deste tema. Como conseqüência, pôde-se definir um conjunto de requisitos funcionais e de segurança necessários ao estabelecimento de uma loteria digital, que guiaram a elaboração do Lottuseg.

Um aspecto importante a ser observado é o fato de o Lottuseg não se constituir apenas em um protocolo para o registro de apostas digitais, mas sim em um conjunto de protocolos que modela o processo lotérico como um todo. Questões como configuração de jogos e extrações, apuração de acumulação e cadastramento de resultados também são tratadas no Lottuseg, tendo sido propostos mecanismos para garantir tanto a segurança quanto a auditoria destas operações.

Para a efetivação de apostas digitais, procurou-se definir um modelo que se assemelhasse ao tradicional, havendo a emissão de comprovantes de apostas. O comprovante proposto tem como característica primordial a verificabilidade, sendo baseado em técnicas criptográficas como assinaturas digitais, redes de misturadores e comprometimento de bits. Desta forma, assim como no caso tradicional, é possível aferir se um comprovante é válido com base em informações nele contidas.

Contudo, além desta propriedade geral, o comprovante digital apresenta algumas peculiaridades. Uma delas relaciona-se ao fato de um comprovante de apostas digital estar diretamente relacionado ao apostador que realizou a aposta, não sendo possível a sua apropriação indevida. No caso da Internet, esta é uma propriedade muito importante, pois oferece ao apostador a segurança de que, mesmo que seu comprovante seja roubado, o prêmio não seja reclamado sem que a identidade do verdadeiro apostador seja conhecida.

Um outro ponto a ser destacado é a tolerância à falhas. Uma vez que problemas de comunicação são comuns em conexões à Internet via telefone, procurou-se encadear o protocolo de modo que a loteria digital não pudesse receber o pagamento de uma aposta sem que o apostador tivesse como comprová-la. Para atingir este fim, o comprovante de apostas é constituído por informações obtidas em diferentes pontos do protocolo, estando completo após o momento de entrega do pagamento.

Por fim, também se deve ressaltar a preocupação em modelar uma loteria digital que contenha mecanismos capazes de lidar com as restrições legais que envolvem a operação de uma loteria digital. Neste sentido, viabilizou-se a autenticação dos usuários através de certificados digitais, permitindo assim o controle daqueles que efetivamente terão acesso aos serviços da loteria digital.

7.1 Trabalhos Futuros

Com o objetivo de aprimorar o modelo proposto para uma loteria digital segura, são apresentadas as seguintes sugestões de trabalhos futuros:

- Formalização e validação do protocolo Lottuseg utilizando alguma técnica de especificação formal, como, por exemplo, Redes de Petri;

- Estudo de mecanismos de pagamento eletrônico, fazendo-se um aprofundamento nas opções que podem ser utilizados para a aquisição de créditos para apostar na loteria;

- Estudo de opções para o gerenciamento de créditos e comprovantes de apostas nas máquinas dos apostadores, culminando com a definição de uma sistemática para armazenar, recuperar e verificar de forma simples e ordenada estes documentos digitais. Com isso, pretende-se simplificar o procedimento de aposta digital, facilitando sua utilização por usuários com pouca experiência em informática;

- Definição de um padrão para impressão dos comprovantes de apostas digitais, propondo-se também uma infraestrutura para o reconhecimento e validação de comprovantes impressos, oferecendo maior flexibilidade à loteria. Neste caso, uma das opções seria a utilização de códigos de barras.

Referências Bibliográficas

[APO97] APOSTOLOPOULOS, G.; PERIS, V.; SAHA D.; Transport Layer Security: How much does it really cost. In: Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. *Proceedings*. Nova York, 1999. p 717-725.

[BRAa] BRASIL. Decreto-Lei n. 6259, de 10 de fevereiro de 1944. *Dispõe sobre o serviço de loterias e dá outras providências.* Publicado no Diário Oficial da União, de 18 de fevereiro de 1944.

[BRAb] BRASIL. Decreto-Lei n. 759, de 12 de agosto de 1969. *Autoriza o Poder Executivo a constituir a empresa pública Caixa Econômica Federal e dá outras providências.*

[BRAc] BRASIL. Decreto-Lei n. 204, de 27 de fevereiro de 1967. *Dispõe sobre a exploração de loterias e dá outras providências.*

[BRAd] BRASIL. Decreto-Lei n. 594, de 27 de maio de 1969. *Institui a Loteria Esportiva Federal e dá outras providências.*

[BRAe] BRASIL. Lei n. 6717, de 12 de novembro de 1979. *Autoriza modalidade de concurso de prognósticos da Loteria Federal regida pelo Decreto-lei nº 204, de 27 de fevereiro de 1967, e dá outras providências.*

[BRAf] BRASIL. Decreto n. 99268, de 31 de maio de 1990. *Cria a Loteria Federal sob a modalidade instantânea e dá outras providências.*

[BRAg] BRASIL. Resolução n. 11, de 14 de fevereiro de 2002. *Altera os requisitos mínimos para as políticas de certificado na ICP-Brasil, a declaração de*

práticas de certificação da AC Raiz da ICP-Brasil, delega atribuições para a AC Raiz e dá outras providências.

[BRI01] ENCYCLOPÆDIA BRITANNICA. *Lottery*. On-line. Capturado em 06 de Agosto de 2001. Disponível na Internet em http://www.britannica.com.

[CER01] CERT. *CERT/CC Statistics 1988-2001*. On-line. Capturado em 24 de Outubro de 2001. Disponível na Internet em http://www.cert.org/stats/cert_stats.html.

[CHE98] CHENG, C.; GARAY, J.; HERZBERG A.; et al. A security architecture for the Internet Protocol. *IBM Systems Journal*. v.37, n. 1, p42-60, 1998.

[DEV01] DEVEGILI, Augusto. *Farnel: Uma Proposta de Protocolo Criptográfico para Votação Digital*. Florianópolis, 2001. 68f. Dissertação (Mestrado em Ciência da Computação) – Centro Tecnológico, Universidade Federal de Santa Catarina.

[DIF76] DIFFIE, W.; HELLMAN, M. New directions in Cryptography. *IEEE Transactions on Information Theory*, v.22, n.6, p.644–654, 1976.

[DUB00] DUBUISSON, O. *ASN.1 - Communication between heterogeneous systems*. San Diego: Morgan Kaufmann Publishers, 2000.

[FRI96] FRIER, A.; KARLTON, P.; KOCHER, P. *The SSL 3.0 Protocol*. On-line. Capturado em 15 de setembro de 2001. Disponível na Internet em http://home.netscape.com/eng/ssl3/draft302.txt

[GOL98] GOLDSCHLAG, D.; STUBBLEBINE, S. Publicly verifiable lotteries: applications of delaying functions. In: Financial Cryptography. *Proceedings*. British West Indies, 1998, p.214-226.

[HOU01] HOUSLEY R.; POLK T. *Planning for PKI*. Nova York: John Wiley & Sons, 2001.

[ITU00] ITU-T. *Recommendation X.509 (03/00) – Information Technology – Open Systems Interconnection – the Directory: Authentication Framework*, 2000.

[KOB00] KOBAYASHI, K.; MORITA, H.; HAKUTA, M.; et al. An electronic soccer lottery system that uses bit commitment. *IEICE Transactions on Information and Systems*. v.E83-D, n.5, p. 980-987, 2000.

[MEN97] MENEZES, A.; OORSCHOT, P.; VANSTONE, S. *Handbook of Applied Cryptography*. Boca Raton: CRC Press, 1997.

[NIS01] NIST. *Advanced encryption standard (AES)*. National Institute of Standards and Technology, 2001. Technical report.

[PAS02] PASQUAL, E. S. *IDDE – Uma infraestrutura para a datação de documentos Eletrônicos*. Florianópolis, 2002. 95f. Dissertação (Mestrado em Ciência da Computação) – Centro Tecnológico, Universidade Federal de Santa Catarina.

[RIV78] RIVEST, R.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. v.21, n.2, p. 120-126, 1978.

[SCH96] SCHNEIER, B. *Applied Cryptography*. 2. ed. New York: John Wiley & Sons, 1996.

[SHA49] SHANNON, C. Communication theory of secrecy systems. *Bell Systems Technical Journal*, v.28, p.656-715, 1949.

[STA99] STALLINGS, W. *Cryptography and Network Security*. 2.ed. Upper Saddle River: Prentice-Hall, 1999.

[STI95] STINSON, D. *Cryptography – Theory and Practice*. Boca Raton: CRC Press, 1995.

[SYV98] SYVERSON, P. Weakly Secret Bit Commitment: Applications to lotteries and fair exchange. In: IEEE Computer Security Foundations Workshop. *Proceedings*. Rockport, 1998.

[TAN97] TANENBAUM, S. *Redes de Computadores*. 5 ed. Rio de Janeiro: Editora Campus, 1997.

[WAG99] WAGNER, D.; SCHNEIER, B. Analysis of the SSL 3.0 protocol. In: Second USENIX Workshop on Electronic Commerce. *Proceedings*. Berkeley, 1996, p.29-40.

Apêndice A

Codificação do Lottuseg em ASN.1

Este apêndice apresenta a codificação em ASN.1 do protocolo Lottuseg. Nesta codificação, foi definido um módulo chamado '`Estruturas-loteria`' contendo todas as estruturas de dados usadas ao longo das diversas fases do protocolo. Assim, este módulo contém a codificação de estruturas como jogo, extração, aposta, pagamento e recibo.

Tomando por base o módulo de estruturas, foram codificados os protocolos para várias fases do Lottuseg: (a) configuração de jogos; (b) configuração de extrações; (c) consulta à loteria; (d) aquisição de créditos; (e) validação de apostas; (f) recuperação de erros; (g) cadastramento de resultados; (h) requisição da premiação.

A seguir é apresentada a codificação realizada.

```
Estruturas-loteria DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

   Jogo :: = SEQUENCE {
      id-jogo                  PrintableString(SIZE(1..10)),
      regras-jogo              PrintableString(SIZE(1..2000)),
      preco-aposta             Real
   }


   Jogo-ass-adm :: = SEQUENCE {
      jogo                     Jogo,
      ass-jogo                 Assinatura
   }


   Assinatura :: = PrintableString(SIZE(500))


   Jogo-ass-loteria :: = SEQUENCE {
      jogo                     Jogo,
      ass-loteria              Assinatura
   }
```

```
Jogos :: = SEQUENCE OF {
   jogo-ass                  Jogo-ass-loteria
}


Extracao :: = SEQUENCE {
   id-jogo                   PrintableString(SIZE(1..10)),
   num-extracao              PrintableString(SIZE(1..10)),
   inicio-apostas            Timestamp,
   fim-apostas               Timestamp,
   data-sorteio              Timestamp,
   premio                    Real
}


Timestamp :: = NumericString (SIZE(15) -- DDMMYYYY HHMISS -- )


Extracao-ass-adm :: = SEQUENCE {
   extracao                  Extracao,
   ass-extracao              Assinatura
}


Extracao-ass-loteria :: = SEQUENCE {
   extracao                  Extracao,
   ass-extracao              Assinatura
}


Extracoes :: = SEQUENCE OF {
   extracoes-ass             Extracoes-ass-loteria
}


Solicitacao-consulta :: = Boolean


Solicitacao-credito :: = SEQUENCE {
   idAP                      Identidade,
   valor-credito             Real,
   inf-pagamento             Pagamento,
   ass-solicitacao-credito   Assinatura
}


Identidade :: = CHOICE {
    num-documento            PrintableString(SIZE(1..30)),
    certificado              PrintableString(SIZE(1..2000))
}


Pagamento :: = CHOICE {
    cartao-credito           Cartao-credito,
    debito-conta             Debito-conta
}
```

```
Cartao-credito :: = SEQUENCE {
    tipo                    Tipo-cartao,
    numero                  NumericString(SIZE(30)),
    data-expira             NumericString(SIZE(6) -- MMYYYY --)
}


Tipo-cartao :: = ENUMERATED {visa(0), master(1),
                             american(2), diners(3)}


Debito-conta :: = SEQUENCE {
    banco                   Banco,
    agencia                 NumericString(SIZE(10)),
    conta                   NumericString(SIZE(15))
}


Banco :: = ENUMERATED {brasil(0), bradesco(1), itau(2),
                       caixa(3), real(4)}


Credito :: = SEQUENCE {
    idEC                    Identidade,
    idCR                    Identidade,
    idAP                    Identidade,
    valor-credito           Real,
    timestamp               Timestamp,
    ass-credito             Assinatura
}


Aposta :: = SEQUENCE {
    c                       PrintableString(SIZE(160)),
    id-jogo                 PrintableString(SIZE(1..10)),
    num-extracao            PrintableString(SIZE(1..10))
}


Aposta-assinada :: = SEQUENCE {
    aposta                  Aposta,
    ass-aposta              Assinatura
}


Pagamento :: = SEQUENCE {
     C                      PrintableString(SIZE(160)),
     credito                Credito,
     ass-pagamento          Assinatura
}


Prognosticos-cifrados :: = PrintableString(SIZE(1..2000))


Recibo :: = SEQUENCE {
     pagamento              Pagamento,
     timestamp              Timestamp
}
```

```
   Recibo-assinado :: = SEQUENCE {
        recibo                  Recibo,
        ass-recibo              Assinatura
   }


   Resultado :: = SEQUENCE {
        id-jogo                 PrintableString(SIZE(1..10)),
        num-extracao            PrintableString(SIZE(1..10)),
        prognosticos            PrintableString(SIZE(1..2000))
   }


   Resultado-assinado :: = SEQUENCE {
        resultado               Resultado,
        ass-resultado           Assinatura
   }


   Confirmacao :: = SEQUENCE {
        id-jogo                 PrintableString(SIZE(1..10)),
        num-extracao            PrintableString(SIZE(1..10)),
        num-vencedores          NumericString(SIZE(3))
   }


   Confirmacao-assinada :: = SEQUENCE {
        confirmacao             Confirmacao,
        ass-confirmacao         Assinatura
   }


   N :: = PrintableString(SIZE(120))


   Resultado-Verificacao :: = Boolean

END



Config-jogo-protocolo DEFINITIONS AUTOMATIC TAGS :: =
BEGIN
IMPORTS Jogo-ass-adm, Jogo-ass-loteria from Estruturas-loteria;

    Mensagem :: = CHOICE { pergunta Jogo-ass-adm,
                           resposta Jogo-ass-adm
                         }
END


Config-extracao-protocolo DEFINITIONS AUTOMATIC TAGS :: =
BEGIN
IMPORTS Extracao-ass-adm, Extracao-ass-loteria from Estruturas-loteria;

    Mensagem :: = CHOICE { pergunta Extracao-ass-adm,
                           resposta Extracao-ass-adm
                         }
END
```

```
Consulta-loteria-protocolo DEFINITIONS AUTOMATIC TAGS :: =
BEGIN
IMPORTS Solicitacao-consulta, Jogos, Extracoes from Estruturas-loteria;

    Mensagem :: = CHOICE { pergunta Solicitacao-consulta,
                           resposta SEQUENCE {jogos      Jogos,
                                              extracoes  Extracoes}
                         }
END



Aquisicao-creditos-protocolo DEFINITIONS AUTOMATIC TAGS :: =
BEGIN
IMPORTS Solicitacao-credito, credito from Estruturas-loteria;

    Mensagem :: = CHOICE { pergunta Solicitacao-credito,
                           resposta Credito
                         }
END



Validacao-apostas-protocolo DEFINITIONS AUTOMATIC TAGS :: =
BEGIN
IMPORTS Aposta, Aposta-assinada, Pagamento, Prognosticos-cifrados,
        Recibo from Estruturas-loteria;

    Mensagem :: = CHOICE { pergunta CHOICE {
                              aposta                  Aposta,
                              pagamento-prognosticos  SEQUENCE {
                                  pagamento           Pagamento,
                                  prognosticos        Prognosticos
                                                      -cifrados }
                              },

                           resposta CHOICE {
                               aposta-ass             Aposta-assinada,
                               recibo                 Recibo
                              }
                         }
END



Recuperacao-protocolo DEFINITIONS AUTOMATIC TAGS :: =
BEGIN
IMPORTS Aposta-assinada, Recibo from Estruturas-loteria;

    Mensagem :: = CHOICE { pergunta Aposta-assinada,
                           resposta Recibo
                         }
END
```

```
Cadastramento-resultado-protocolo DEFINITIONS AUTOMATIC TAGS :: =
BEGIN
IMPORTS Resultado-assinado, Confirmacao-assinada from Estruturas-loteria;

    Mensagem :: = CHOICE { pergunta Resultado-assinado,
                           resposta Confirmacao-assinada}
                         }
END



Requisicao-premio-protocolo DEFINITIONS AUTOMATIC TAGS :: =
BEGIN
IMPORTS Aposta-assinada, Recibo-assinado, N,
        Resultado-verificacao from Estruturas-loteria;

    Mensagem :: = CHOICE { pergunta SEQUENCE {
                               aposta-ass          Aposta-assinada,
                               recibo-ass          Recibo-ass,
                               n                   N }
                               },
                           resposta Resultado-verificacao
                         }
END
```