SEGURANÇA DA INFORMAÇÃO

Prof. Luis Gonzaga de Paulo

TEMA 1 – INTRODUÇÃO À CRIPTOGRAFIA

Já estamos conscientes de que a segurança da informação, suportada pelos ativos da informação e da comunicação das organizações, é de fundamental importância para os negócios em um mundo interconectado e com negócios globalizados. E a necessidade de se manter a confidencialidade, a integridade e a disponibilidade, além do não repúdio, entre outras características da informação, no que se refere à segurança, é atendida em parte pela criptografia.

Mas, o que é a criptografia? Segundo a literatura, a criptografia é a ciência de transformar a informação para torná-la restrita, de forma que possa ser armazenada e transportada de maneira segura e, assim, torne-se imune a modificações e acesso indevido. A criptografia é, como já dissemos, uma das principais ferramentas de proteção e defesa da informação. Forouzan (2008, p. 929) acrescenta que “a criptografia também pode ser usada para autenticação do emissor e do receptor da mensagem entre si”, ou seja, quando emissores e receptores precisam de um reconhecimento mútuo.

A criptografia é uma ciência do domínio da matemática, destinada ao estudo de técnicas e princípios de transformação da informação de sua forma original para outra, ininteligível, de forma que possa ser conhecida e utilizada apenas quando autorizado. Esse processo de transformação da informação em seu estado original, chamado de *texto plano* (*plain text*), para um formato protegido pela ocultação de seu significado, chamado de *texto cifrado* ou *codificado*, é denominado *cifragem* (ou também *criptografia*, *encriptação*). O processo oposto é denominado *decifragem* (ou *descriptografia*, *descriptação*). Quando é feito à revelia dos interessados ou proprietários da informação – de forma maliciosa ou não – é chamado de *quebra da criptografia* ou *do código*.

Considere um usuário de um sistema que requeira acesso às funcionalidades de um dado sistema: para tanto, o usuário precisará identificar-se com um ID específico e de seu uso pessoal e fornecer uma senha de acesso, em um processo de autenticação e autorização de acesso. Esse processo certamente fará uso dos recursos da criptografia. A Figura 1 mostra os elementos envolvidos em uma troca de mensagens por meio de um processo criptográfico.

Figura 1 – Elementos do processo criptográfico

1.1 Terminologia

Para prosseguirmos em nossos estudos é necessário relacionarmos alguns termos utilizados na literatura e nos documentos. Já vimos o que é **criptografia**. A palavra vem do grego, cujo significado é *escrita secreta*. A criptografia também emprega os termos *texto claro* (ou *texto plano*), que se refere à mensagem original, não modificada pelo processo criptográfico. Já o **texto cifrado** é a mensagem submetida a um **algoritmo criptográfico**, isto é, a um código ou programa de computador que transforma o texto plano em texto cifrado. Esse algoritmo criptográfico é também chamado de *cifra* e geralmente faz uso de uma **chave**, um valor numérico que será aplicado à mensagem para produzir uma modificação controlada e reversível. Uma chave pode ser usada para **criptografar** – ou cifrar (texto claro → texto cifrado) ou para **descriptografar** – ou decifrar (texto cifrado → texto plano).

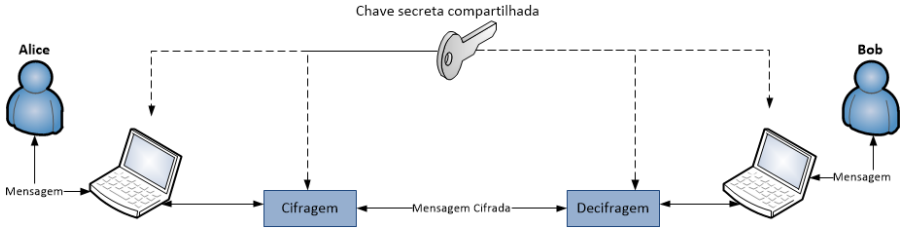
Além desses termos, é comum encontrarmos, nos exemplos da literatura, a utilização de três pessoas envolvidas no processo de comunicação criptografada: **Alice**, **Bob** e **Eve**. **Alice** é quem precisa enviar uma mensagem ou dados de forma segura, enquanto **Bob** é o destinatário dessa comunicação, que deve recebê-la de forma segura, com suas características de confidencialidade, integridade e disponibilidade preservadas, além de, eventualmente, confirmar a recepção e o acesso à informação. Já **Eve** é quem procura, de qualquer forma possível, ter acesso às informações e até alterá-las sem o conhecimento e o consentimento de Alice e Bob. Eve pode também gerar e enviar suas próprias mensagens, com propósitos escusos.

1.2 Categorias

O processo de criptografia pode ser realizado por meio de dois tipos básicos de cifragem/decifragem ou categorias: a **criptografia simétrica**, de

chave única ou de **chave secreta**; e a **criptografia assimétrica** ou de **chave pública**. Na criptografia simétrica, a mesma chave é utilizada para a cifragem e a decifragem da mensagem, e o algoritmo de cifragem e decifragem é o mesmo. A Figura 2 apresenta o processo de criptografia simétrica.

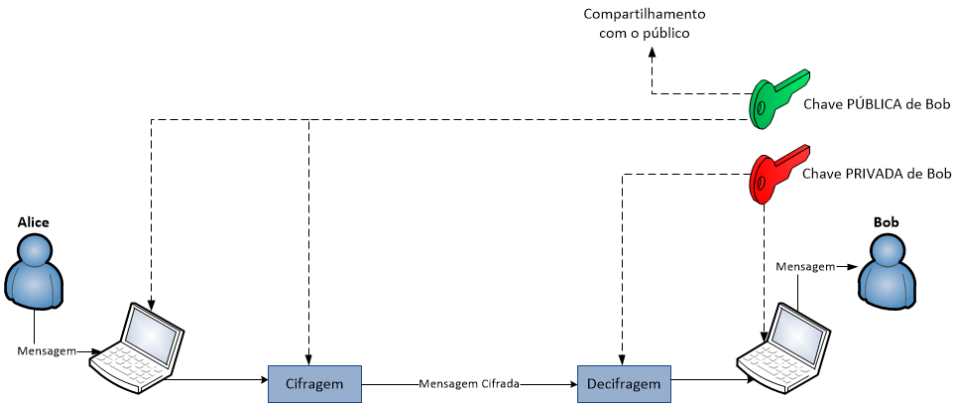
Figura 2 – A criptografia simétrica



Fonte: Adaptado de Forouzan, 2008.

Na criptografia de chave assimétrica, são utilizadas duas chaves no processo de cifragem/decifragem: a **chave pública** e a **chave privada**. A chave pública, usada para cifrar a mensagem, é compartilhada com os possíveis emissores de mensagem para o receptor, que guarda consigo a chave privada para decifrar a mensagem recebida. Essas chaves são diferentes entre si. A Figura 3 mostra o processo de criptografia assimétrica.

Figura 3 – O processo de criptografia assimétrica



Fonte: Adaptado de Forouzan, 2008.

TEMA 2 – CRIPTOGRAFIA SIMÉTRICA

A criptografia de chave única ou simétrica utiliza apenas uma chave para criptografar e descriptografar a mensagem. Portanto, essa chave precisa ser muito bem guardada e seu envio, por um meio de comunicação, representa um risco. Os algoritmos utilizados para a criptografia simétrica apresentam

desempenho muito superior, razão pela qual são preferidos em processos de criptografia de bloco e de fluxo.

São exemplos desse tipo de algoritmo o ***data encryption standard* (DES)**, criado pela IBM em 1974, evoluindo depois para o **3-DES** ou **triple DES**. O algoritmo **RC4**, desenvolvido por Ronald Rivest, é utilizado no SSL e é um dos mais empregados na criptografia de fluxo de dados. Já o **RC5**, do mesmo autor, é empregado para cifragem de blocos e de extrema facilidade. Ambos têm a chave de tamanho fixo.

O ***blowfish*** é um algoritmo de criptografia de blocos com chave de tamanho variável, desenvolvido em 1993 por Bruce Schneier, e seu código-fonte é aberto e pode ser obtido na internet. Já o ***international data encryption algorithm* (Idea)** foi criado em 1991 por James Massey e Xuejia Lai. É também um algoritmo de bloco semelhante ao DES e de fácil implementação. O algoritmo ***advanced encryption standard* (AES)** ou **padrão de criptografia avançada** é um algoritmo de criptografia de bloco padronizado pelo Instituto Nacional de Padrões e Tecnologia (Nist) em 2001 e usado pelo governo dos Estados Unidos em substituição ao DES/3-DES, sendo um dos mais populares algoritmos da atualidade, por combinar as características de segurança, desempenho, facilidade de implementação e flexibilidade.

Na criptografia simétrica, se Bob quer compartilhar informações com Alice:

1. Bob gera uma chave criptográfica e encaminha para Alice;
2. Bob cifra a mensagem com a chave gerada e a envia para Alice;
3. Alice decifra a mensagem com a chave recebida;
4. Se Alice quiser responder a Bob, usa a mesma chave para cifrar a resposta e a enviar para Bob;
5. A chave deve ser protegida tanto por quem a usa quanto no processo de comunicação.

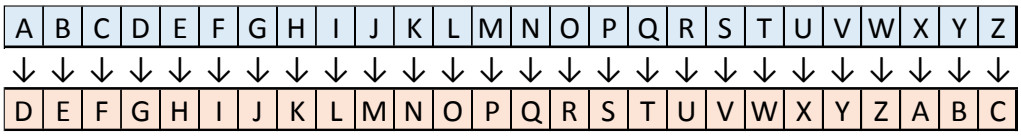
2.1 Cifras simétricas tradicionais

As cifras simétricas são utilizadas desde os primórdios da história, quando a humanidade passou a utilizar a comunicação escrita, e são muito utilizadas na atualidade. Essas cifras compreendem as **cifras de substituição** e as **cifras de transposição**, sendo que as cifras de substituição podem ser **monolfabéticas** ou **polialfabéticas**.

2.1.1 Cifras de substituição

Nas cifras de substituição, um símbolo da mensagem – uma letra, um sinal ou um número – é substituído por um outro símbolo. Na **cifragem monoalfabética** essa troca é constante, ou seja, em qualquer posição da mensagem acontece a mesma troca. A chave criptográfica, nesse caso, contempla uma simples tabela de equivalência, a qual é usada em ambos os processos – cifragem e decifragem. A cifra de substituição monoalfabética mais conhecida é a cifra de César, que consiste em usar como chave um deslocamento de três posições nas letras do alfabeto, como mostrado na Figura 4. Esse tipo de cifra também é conhecido como *cifra de deslocamento*. Outra cifra dessa categoria que já foi bastante utilizada é a ROT13.

Figura 4 – A cifra de César

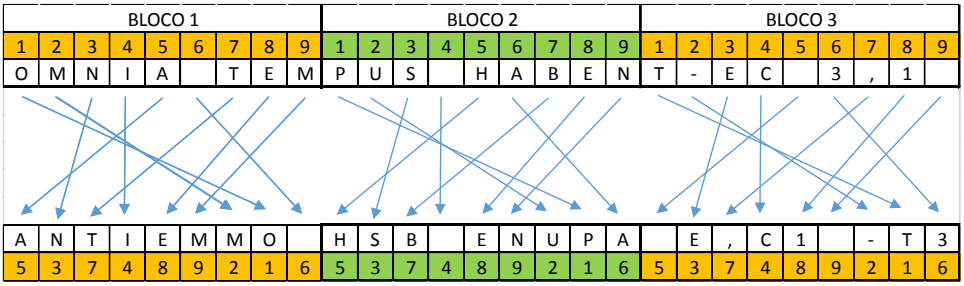


Já em uma cifra polialfabética, a substituição de símbolos é variável, sendo um mesmo símbolo substituído por vários outros, no decorrer da cifragem, configurando uma relação de um para muitos. Nesse caso, a chave e o processo de cifragem devem tratar das possibilidades de substituição. Uma forma de fazer isso é a divisão do texto em blocos de tamanho fixo, com a repetição da chave para completar o tamanho desses blocos.

2.1.2 Cifras de transposição

No processo de transposição a chave é uma relação entre as posições dos símbolos no texto plano e no texto cifrado. A Figura 5 apresenta essa cifragem, usando chaves 123456789 ↔ 537489216 e blocos de nove símbolos.

Figura 5 – Uma cifragem de transposição



A cifragem então consiste em uma transposição com base em uma tabela de-para, na qual a chave numérica representa as posições dos símbolos e a sequência na qual serão transpostos. O resultado é que o texto plano original, “OMINIA TEMPUS HABENT-EC 3,1” é transformado em “ANTIEMMO HSB ENUPA E, C1 -T3”.

2.2 Cifras modernas simples

As cifras que apresentamos até aqui foram criadas quando ainda não havia o computador e, por isso, trabalham com símbolos, com caracteres. Com o uso do computador digital, passamos a utilizar cifras que tratam dos bits, que podem ser aplicadas para além das informações em formato texto, como por exemplo valores, imagens, sons e vídeos, com a vantagem de que essas informações podem ser processadas em fluxo – como em uma ligação telefônica ou em um filme ou um vídeo ao vivo. As cifras modernas simples são adaptações daquelas cifras simples, porém ajustadas ao uso da aritmética e da lógica binária por intermédio da computação digital, realizando operações bit a bit.

2.2.1 XOR

A cifra XOR é um processo que aplica a operação aritmética lógica ou-exclusivo (XOR), comparando os bits do texto plano com os da chave para gerar o texto cifrado. Além da elevada velocidade, por tratar-se de uma operação muito simples, essa cifra tem a vantagem de que o processo de cifragem e decifragem é exatamente o mesmo, ou seja: **M ⊕ K = C** tanto quanto **C ⊕ K = M**.

2.2.2 Rotação

Na cifra de rotação, os bits de um símbolo ou bloco são deslocados para a esquerda ou para a direita. Esse processo pode ser fixo, com o número de posições do deslocamento sendo constante; ou variável, em função do valor da chave. Uma característica interessante desse processo é que, se aplicarmos um deslocamento idêntico ao número de bits do fluxo de entrada (N), o resultado é inócuo. Portanto, o número de deslocamentos deve ficar entre 1 e N-1. Para a decifragem é necessária a chave, se houver, e realizar a operação de deslocamento no sentido contrário ao da cifragem.

2.2.3 Substituição S-box

Esse processo – *substitution box* ou caixa de substituição – é semelhante à cifra de substituição de símbolos ou caracteres, porém realizado com bits. Não são utilizadas chaves e o processo geralmente é utilizado como um estágio intermediário de outros tipos de cifragens mais complexas.

2.2.4 Transposição P-box

A caixa de permutação – *permutation box* – é a correspondente, para bits, da cifra de transposição. Geralmente implementado por *hardware*, por ser mais ágil, esse processo não requer chave e realiza a permutação **direta**, **por expansão** ou **por compressão**.

2.3 Cifras modernas cíclicas

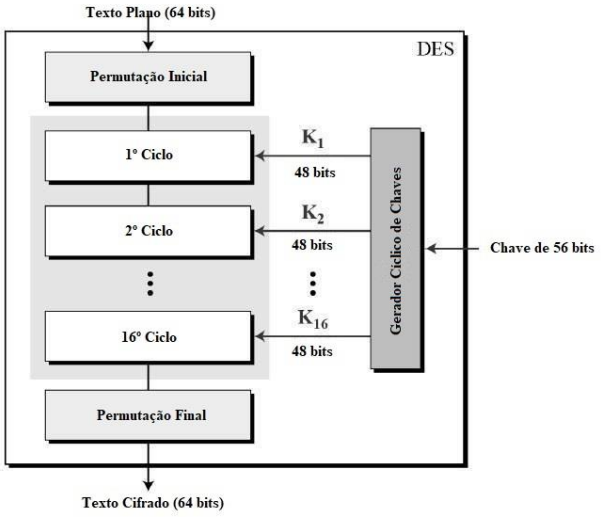
O uso da computação na aplicação de cifragem possibilitou o surgimento de cifras complexas, nas quais o processo de cifragem simples é repetido inúmeras vezes, usando toda a chave, partes ou variações dela de forma cíclica até se produzir o resultado cifrado, dando origem ao que denominamos *cifragem moderna cíclica*. Os processos mais conhecidos desse modelo são o DES, o 3DES e o AES.

2.3.1 DES

O DES é uma cifra de bloco de chave simétrica publicada pelo Nist. O DES é uma implementação de uma cifra Feistel que utiliza 16 ciclos da estrutura de

Feistel. O tamanho do bloco de dados a ser criptografado é de 64 bits. Embora o tamanho da chave seja de 64 bits, o DES usa um comprimento de chave efetivo de 56 bits, pois 8 dos 64 bits da chave não são usados pelo algoritmo de criptografia e funcionam apenas como bits de verificação. A estrutura geral do DES é mostrada na Figura 6.

Figura 6 – Estrutura do DES



Fonte: Adaptado de Forouzan, 2008.

O DES satisfaz ambas as propriedades desejadas da cifra de bloco. Essas duas propriedades tornam a cifra muito forte: o **efeito avalanche** – uma pequena mudança no texto simples resulta na grande mudança no texto cifrado –; e a **completude** – cada bit de texto cifrado depende de muitos bits de texto simples. A criptoanálise já encontrou alguns pontos fracos no DES, especialmente quanto ao tamanho da chave, considerada muito curta.

2.3.2 3DES (triple DES)

A partir de 1990, várias tentativas de quebra do DES começaram a ser empreendidas, algumas com sucesso, gerando desconfiança entre os usuários de DES. Porém, os usuários não quiseram substituir o DES, em parte devido ao tempo e aos gastos para alterar o algoritmo, então amplamente adotados e incorporados em várias arquiteturas de segurança. A abordagem pragmática foi não abandonar completamente o DES, mas mudar a maneira como ele é usado. Isso levou aos esquemas modificados do triple DES (conhecido como 3DES). A propósito, existem duas variantes do triple DES conhecidas como 3-chave triple

DES (3TDES) e 2-chave triple DES (2TDES).

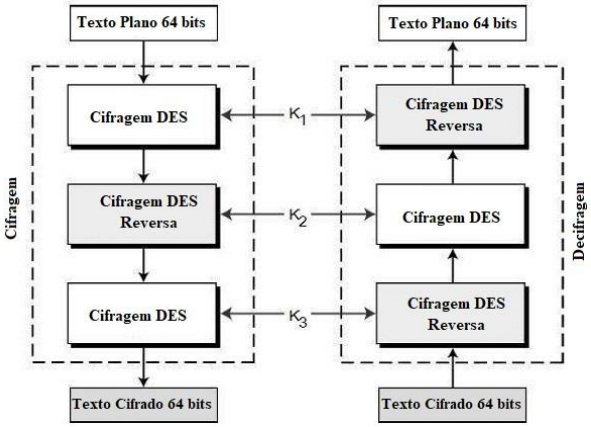
Para usar o 3TDES, o usuário primeiro gera e distribui uma chave 3TDES K, que consiste em três diferentes chaves DES, denominadas *K1*, *K2* e *K3*. Isso significa que a chave 3TDES atual tem comprimento de 3 × 56 = 168 bits. O esquema de criptografia é mostrado na Figura 7. O processo de criptografia-descriptografia é o seguinte:

1. criptografam-se os blocos de texto sem formatação usando DES único com chave K1;
2. descriptografa-se a saída do passo 1 usando DES único com a chave K2;
3. criptografa-se a saída da etapa 2 usando DES único com a chave K3.

A saída do passo 3 é o texto cifrado. A descriptografia de um texto cifrado é um processo inverso. Primeiro se descriptografa o texto cifrado usando a chave K3, depois criptografa-se com a chave K2 e, finalmente, descriptografa-se com a chave K1. Devido a esse *design* do triple DES como um processo de criptografar/descriptografar/criptografar, é possível usar uma implementação do 3-DES (mesmo em *hardware*) para DES único definindo-se K1, K2 e K3 como sendo um mesmo valor. Isso fornece compatibilidade com versões anteriores do DES.

A segunda variante do triple DES (2TDES) é idêntica a 3TDES, exceto que K3 é substituído por K1. Em outras palavras, o usuário criptografa blocos de texto simples com a chave K1, depois descriptografa com a chave K2 e finalmente criptografa com K1 novamente. Portanto, o 2TDES tem um comprimento de chave de 112 bits. As cifras triple DES são significativamente mais seguras que o DES, porém resultam em um processo muito mais lento que o da criptografia DES.

Figura 7 – Estrutura do 3-DES



Fonte: Adaptado de Forouzan, 2008.

2.3.3 AES

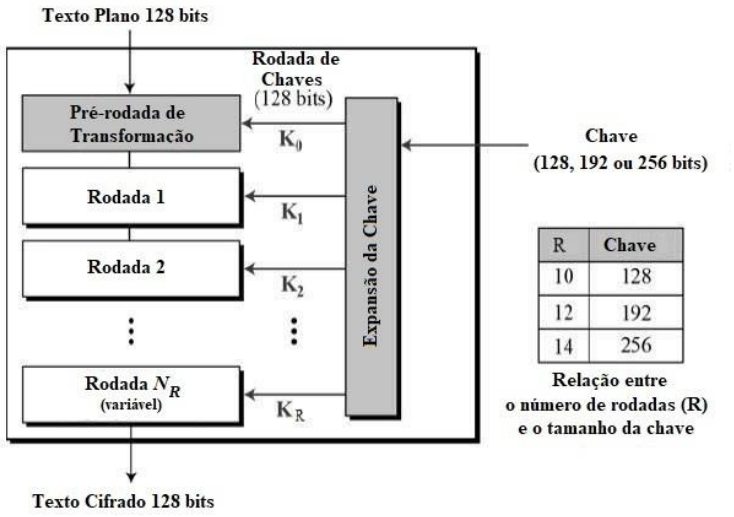
O algoritmo de criptografia simétrica mais popular e mais adotado atualmente é o AES, cujo desempenho é cerca de seis vezes mais rápido que o do 3-DES. Com o aumento do poder de computação, um substituto para o DES tornou-se necessário, pois o tamanho da chave do DES era muito pequeno, o que o tornava vulnerável a ataques de busca de chave exaustivos. O 3-DES foi projetado para superar essa desvantagem, mas foi considerado lento. Então, após uma solicitação do governo americano, foi desenvolvido o AES, cujas características principais são as seguintes:

- chave simétrica de bloco simétrico;
- dados de 128 bits, chaves de 128/192/256 bits;
- mais forte e mais rápido que o 3-DES;
- fornece detalhes completos de especificação e *design*;
- *software* implementável em C e Java.

O algoritmo AES é uma cifra iterativa que, ao invés de em Feistel, baseia-se na **rede de substituição-permutação**. É composto por uma série de operações vinculadas, algumas das quais envolvem a substituição de entradas por saídas específicas (substituições) e outras envolvem a divisão aleatória de bits (permutações). Porém, o AES executa todos os seus cálculos em bytes, em vez de bits. O AES trata os 128 bits de um bloco de texto simples como 16 bytes. Esses 16 bytes são organizados em quatro colunas e quatro linhas para processamento como uma matriz.

Ao contrário do DES, o número de rodadas no AES é variável e depende do tamanho da chave. O AES usa 10 rodadas para chaves de 128 bits, 12 rodadas para chaves de 192 bits e 14 rodadas para chaves de 256 bits. Cada uma dessas rodadas usa uma chave redonda de 128 bits diferente, que é calculada com base na chave AES original. O esquema da estrutura AES é mostrado na Figura 8.

Figura 8 – Estrutura do AES



Fonte: Adaptado de Forouzan, 2008.

2.4 Cifras de bloco

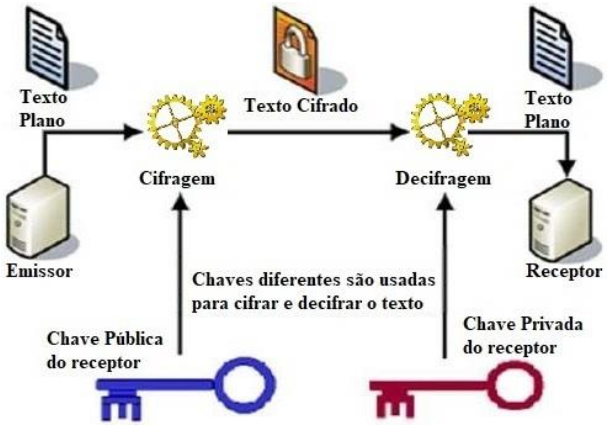
Uma cifra de bloco processa os blocos de dados de tamanho fixo. Geralmente, o tamanho de uma mensagem é maior que o tamanho do bloco. Portanto, a mensagem longa é dividida em uma série de blocos de mensagens sequenciais e a cifra opera nesses blocos, em um de cada vez. As principais cifras de bloco são as seguintes:

- livro de código eletrônico (ECB, de *electronic code book*);
- encadeamento de blocos de cifras (CBC, de *cipher block chaining*);
- codificação com *feedback* (CFB, de *cipher feedback*);
- *feedback* de saída (OFB, de *output feedback*);
- contador (CTR, de *counter*).

TEMA 3 – CRIPTOGRAFIA ASSIMÉTRICA

A criptografia assimétrica – ou de chave pública – é um conceito relativamente novo. Com a disseminação de redes de computadores abertas nas últimas décadas, aumentou a necessidade de se usar a criptografia em larga escala. A chave simétrica provou-se ineficaz, devido aos desafios enfrentados pelo gerenciamento de chaves. Isso levou à criptografia de chave pública, cujo processo de criptografia e descriptografia é descrito na Figura 9.

Figura 9 – Criptografia assimétrica



Fonte: Adaptado de Forouzan, 2008.

As principais características da criptografia de chave pública são:

- Chaves diferentes são usadas para criptografia e descriptografia. Essa é uma propriedade que a diferencia da criptografia simétrica.
- Cada receptor possui uma chave de descriptografia exclusiva, geralmente referida como sua chave privada.
- O receptor precisa publicar uma chave de criptografia, conhecida como sua chave pública.
- Alguma garantia da autenticidade de uma chave pública é necessária, nesse esquema, para evitar a falsificação do adversário como receptor.
- A criptografia assimétrica pode envolver terceiros confiáveis, que certificam que uma determinada chave pública pertence apenas a uma pessoa ou entidade específica.
- O algoritmo de criptografia é complexo o suficiente para impedir que o invasor consiga produzir um texto simples com base no texto cifrado e na chave de criptografia (pública).

Embora as chaves pública e privada estejam relacionadas matematicamente, não é possível calcular a chave privada com base na chave pública. Na verdade, a parte inteligente de qualquer sistema criptográfico de chave pública está no projeto da relação entre essas duas chaves. Existem três tipos de esquemas de criptografia de chave pública, os quais apresentaremos a seguir.

3.1 Criptografia RSA

A criptografia RSA é um dos primeiros sistemas criptográficos de chave

pública e o mais empregado atualmente. O sistema foi criado por Ron Rivest, Adi Shamir e Len Adleman. Veremos dois aspectos do sistema de criptografia RSA: primeiro, a geração de pares de chaves e, em segundo lugar, algoritmos de criptografia-descriptografia.

3.1.1 Geração de par de chaves RSA

Cada pessoa ou parte que deseja utilizar-se da comunicação usando criptografia precisa gerar um par de chaves, ou seja, uma chave pública e uma chave privada. O processo seguido na geração de chaves é descrito a seguir.

Para geração do módulo RSA (n):

1. Selecione dois primos grandes, **p** e **q**.
2. Calcule **n = p * q**. Para criptografia forte e inquebrável, deve haver um número grande, normalmente com um mínimo de 512 bits.
3. Encontre o número derivado (**e**): o número **e** deve ser maior que 1 e menor que **(p - 1) (q - 1)**.
4. Não deve haver nenhum fator comum para **e** e **(p - 1) (q - 1)**, exceto para 1. Em outras palavras, dois números **e** e **(p - 1) (q - 1)** são primos.
5. Forme a chave pública: o par de números (**n, e**) forma a **chave pública** RSA e é tornado público.

Embora **n** seja parte da chave pública, a dificuldade de se fatorar um grande número primo assegura que um atacante não encontre em tempo finito os dois primos (**p** e **q**) usados para obter **n**. Essa é a força do RSA.

Para geração da chave privada:

1. A chave privada **d** é calculada com base em **p**, **q** e **e**. Para dados **n** e **e**, existe um número único **d**.
2. O número **d** é o inverso de **e** módulo **(p - 1) (q - 1)**. Isso significa que **d** é o número menor que **(p - 1) (q - 1)**, tal que, quando multiplicado por **e**, é igual a **1 módulo (p - 1) (q - 1)**.
3. Essa relação é escrita matematicamente da seguinte maneira:

$$e \cdot d = 1 \bmod (p - 1)(q - 1).$$

4. O algoritmo euclideano estendido toma **p**, **q** e **e** como entrada e fornece **d** como saída.

3.1.2 Cifragem RSA

Um emissor que deseje enviar uma mensagem de texto para alguém cuja chave pública seja (**n**, **e**) representa o texto simples como uma série de números menores que **n**. Para criptografar o primeiro texto simples **P**, que é um número módulo **n**, o processo de criptografia é simples, representado matematicamente como:

$$C = P^e \bmod n$$

Isto é, o texto cifrado **C** é igual ao texto simples **P** multiplicado por si mesmo **e** vezes e depois reduzido ao módulo **n**. Isso significa que **C** também é um número menor que **n**.

3.1.3 Decifragem RSA

O processo de descriptografia do RSA é igualmente simples. Considerando que o receptor, que gerou o par de chaves públicas (**n**, **e**) recebeu o texto cifrado **C**, basta então que eleve **C** à potência de sua chave privada **d**. O resultado no **módulo n** será o texto claro **P**, originalmente transmitido e representando matematicamente por:

$$P = C^d \bmod n$$

A segurança do RSA depende da complexidade de duas funções separadas. O sistema de criptografia RSA é o mais popular sistema criptográfico de chave pública, baseado na dificuldade prática de se fatorar números primos muito grandes. Sua **função de criptografia** é considerada uma função unidirecional de conversão de texto simples em texto cifrado que pode ser revertida somente com o conhecimento da chave privada **d**. A **geração da chave** é baseada na dificuldade de se determinar uma chave privada de uma chave pública RSA, o que é o equivalente a se fatorar o módulo **n**. Portanto, não se pode usar o conhecimento de uma chave pública RSA para se determinar uma chave privada RSA, a menos que se consiga fatorar **n**.

Também é uma função unidirecional: passar dos valores de **p** e **q** para o módulo **n** é fácil, mas o inverso é praticamente impossível. Se qualquer uma dessas duas funções for provada não unidirecional, o RSA será quebrado. De fato, se uma técnica de fatoração eficiente for desenvolvida, o RSA não será mais seguro. A força da criptografia RSA é reduzida drasticamente se os números **p** e

q não forem primos grandes, mas também se a chave pública escolhida **e** for um número pequeno.

3.2 Criptografia ElGamal

Existem diversos modelos de criptografia baseados em diferentes versões do **problema do logaritmo discreto**. O **ElGamal**, chamado de *variante de curva elíptica*, é um deles e a sua força vem do pressuposto de que os logaritmos discretos não podem ser encontrados em um período de tempo curto, para um determinado número, enquanto a operação inversa de potenciação pode ser calculada eficientemente. Apresentaremos uma versão simples do ElGamal, que trabalha com números **módulo p**. O caso de variantes de curvas elípticas é baseado em sistemas numéricos bem diferentes.

3.2.1 Geração do par de chaves ElGamal

Cada usuário do sistema criptográfico ElGamal gera o seu par de chaves do seguinte modo:

1. Escolhe um grande primo **p**. Geralmente, um número primo de 1.024 a 2.048 bits de comprimento é escolhido.
2. Escolhe um elemento gerador **g**. Esse número deve estar entre 1 e p - 1, mas não pode ser qualquer número: é um gerador do grupo de múltiplos inteiros de módulo **p**. Isso significa que, para todo inteiro **m** coprimo para **p**, existe um inteiro **k** tal que $\mathbf{g^k = a \bmod n}$. Por exemplo, 3 é gerador do grupo 5 (Z5 = {1, 2, 3, 4}), como podemos ver na Tabela 1.

Tabela 1 – Demonstração de geração de um elemento **g**

n	3^n	$3^n \bmod 5$
1	3	3
2	9	4
3	27	2
4	81	1

3. Escolhe a chave privada: a chave privada **x** é qualquer número maior que 1 e menor que p – 1.
4. Calcula parte da chave pública: o valor **y** é calculado com base nos parâmetros **p**, **g** e na chave privada **x** pela seguinte fórmula:

$y = g^x \bmod p$

5. Obtém a chave pública: a chave pública ElGamal consiste nos três parâmetros (**p**, **g**, **y**).

Vamos supor que p = 17 e que g = 6, pois podemos confirmar que 6 é um gerador do grupo Z17. A chave privada **x** pode ser qualquer número maior que 1 e menor que 17. Então escolhemos **x = 5**. O valor **y** é então calculado por:

$y = 6^5 \bmod 17 = 7$

Assim, nossa chave privada é 62 e a nossa chave pública é (17, 6, 7).

3.2.2 Cifragem ElGamal

A geração de um par de chaves ElGamal é comparativamente mais simples do que o processo equivalente para RSA, porém a criptografia e a descriptografia são um pouco mais complexas que as do RSA. Vamos supor que um emissor deseja enviar um texto simples para alguém cuja chave pública ElGamal seja (**p**, **g**, **y**), então ele representa o texto plano como uma série de números módulo **p**. Para criptografar o primeiro texto simples **P** – que é representado como um número módulo **p** –, de modo a obter o texto cifrado **C**, ele faz o seguinte:

1. Gera aleatoriamente um número k.
2. Calcula dois valores C1 e C2, de modo que:

$C1 = g^k \bmod p \qquad C2 = (P*y^k) \bmod p.$

3. Envia o texto cifrado C, consistindo nos dois valores separados (C1, C2), enviados juntos.

Retomando o exemplo de geração de chaves ElGamal anterior, o texto simples P = 13 é criptografado da seguinte forma:

1. Aleatoriamente, geramos um número, digamos **k = 10**.
2. Calculamos os dois valores **C1** e **C2**, de modo que:

$C1 = 6^{10} \bmod 17 = 15 \qquad C2 = (13*7^{10}) \bmod 17 = 9.$

3. Enviamos o texto cifrado C = (C1, C2) = (15, 9).

3.2.3 Decifragem ElGamal

Para descriptografar o texto cifrado (C1, C2) usando a chave privada x:

1. Calculamos o inverso modular de (C1) x módulo p, que é (C1) - x, chamado

de *fator de decodificação*.

2. Obtivemos o texto original (texto plano P) com base no seguinte cálculo:

$$P = C2 \times (C1)^{-x} \bmod p.$$

Para descriptografar o texto cifrado no exemplo que apresentamos, C = (C1, C2) = (15, 9), usando-se a chave privada x = 5, o fator de descriptografia é:

$$15^{-5} \bmod 17 = 9.$$

Assim, extraímos o texto plano P = (9 × 9) mod 17 = 13.

3.3 Criptografia de curva elíptica (ECC)

Elliptic curve cryptography (ECC) é um termo usado para descrever um conjunto de ferramentas e protocolos criptográficos cuja segurança é baseada em versões especiais do problema do logaritmo discreto. Não usa números módulo p. O ECC é baseado em conjuntos de números associados a objetos matemáticos chamados *curvas elípticas*. Existem regras para adicionar e calcular múltiplos desses números, assim como existem para os números módulo p.

O ECC inclui variantes de muitos esquemas criptográficos que foram inicialmente projetados para números modulares, como criptografia ElGamal e algoritmo de assinatura digital. Acredita-se que o problema do logaritmo discreto é muito mais difícil quando aplicado a pontos em uma curva elíptica. Isso implica a mudança do número módulo p para pontos em uma curva elíptica.

Também um nível de segurança equivalente pode ser obtido com chaves mais curtas se usarmos variantes baseadas em curvas elípticas. As chaves mais curtas resultam em dois benefícios, como a facilidade de gerenciamento de chaves e a computação eficiente. Esses benefícios tornam as variantes baseadas em curva elíptica do esquema de criptografia altamente atraentes para aplicativos em que os recursos de computação são restritos.

TEMA 4 – ASSINATURA DIGITAL

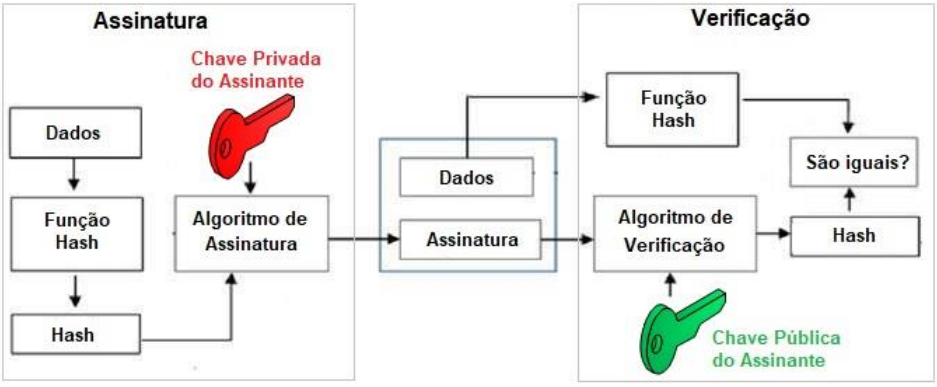
As assinaturas digitais são as primitivas de chave pública da autenticação de mensagens. É comum usarmos assinaturas manuscritas em documentos e mensagens manuscritos ou digitados, para vinculá-los ao signatário. Da mesma forma, uma assinatura digital é uma técnica que vincula uma pessoa ou entidade

aos dados digitais. Essa ligação pode ser verificada independentemente pelo destinatário, bem como por qualquer um interessado em fazê-lo.

4.1 O processo de assinatura digital

Assinatura digital é um valor criptográfico calculado com base em dados e em uma chave secreta conhecida apenas pelo signatário. O receptor da mensagem precisa ter certeza de que a mensagem pertence ao remetente, sem poder negar a origem dessa mensagem. Esse requisito é crucial, no mundo dos negócios, para manter a confiança nas negociações. A Figura 10 apresenta o processo completo, cujos detalhes são descritos nos itens a seguir.

Figura 10 – O processo completo de assinatura digital



Remetentes e destinatários do processo têm seu par de chaves público-privado. Geralmente, os pares de chaves usados para criptografia/descriptografia e assinatura/verificação são diferentes. A **chave privada** usada para assinatura é referida como *chave de assinatura* e a **chave pública** como *chave de verificação*. O processo então é executado com essas etapas:

1. O signatário fornece os dados da mensagem para a função *hash* e gera um *hash* de dados.
2. O *hash* e a chave de assinatura são então submetidos ao algoritmo de assinatura, que produz a assinatura digital em determinado *hash*.
3. A assinatura é anexada aos dados e ambos são enviados para o verificador.
4. O verificador fornece a assinatura digital e a chave de verificação ao algoritmo de verificação.
5. O algoritmo de verificação fornece um valor como saída.
6. O verificador também executa a mesma função de *hash*, nos dados

recebidos, para gerar o valor de *hash*.

7. Para a verificação, esse valor de *hash* dos dados e a saída do algoritmo de verificação são comparados.
8. Com base no resultado da comparação, o verificador decide se a assinatura digital é válida.
9. Como a assinatura digital é criada pela chave privada do assinante e ninguém mais pode ter essa chave, o signatário não pode repudiar a assinatura dos dados no futuro.

Devemos notar que, em vez de se assinar os dados diretamente com o algoritmo da assinatura, isso é feito com o *hash* dos dados. Como o *hash* de dados é uma representação única de dados, basta se assinar o *hash* no lugar dos dados. A razão mais importante do uso de *hash* em vez de dados diretamente para assinatura é a eficiência do processo. Considerando que o RSA seja usado como o algoritmo de assinatura, e conforme tratamos no tema sobre criptografia de chave pública, o processo de criptografia/assinatura usando RSA envolve exponenciação modular. Assinar grandes dados por meio de exponenciação modular é computacionalmente caro e demorado. O *hash* dos dados é um resumo relativamente pequeno dos dados; portanto, assinar um *hash* é mais eficiente do que assinar todos os dados.

4.2 Os objetivos da assinatura digital

Entre todos os processos criptográficos, a assinatura digital usando criptografia de chave pública é considerada uma ferramenta muito importante e útil para alcançar a segurança da informação. Além da capacidade de garantir o não repúdio à mensagem, a assinatura digital também fornece autenticação de mensagens e integridade de dados, como detalhado a seguir:

- **Autenticação da mensagem**: quando o verificador valida a assinatura digital usando a chave pública de um remetente, ele tem a garantia de que a assinatura foi criada apenas pelo remetente que possui a chave privada secreta correspondente e mais ninguém.
- **Integridade de dados**: no caso de acesso indevido e modificação dos dados, a verificação da assinatura digital no final do receptor falhará. O *hash* de dados modificados e a saída fornecida pelo algoritmo de verificação não corresponderão. Portanto, o receptor pode negar com

segurança a mensagem, assumindo que a integridade dos dados foi violada.

- **Não repúdio**: como se presume que somente o signatário tem o conhecimento da chave de assinatura, somente ele poderá criar uma assinatura exclusiva em um determinado dado. Assim, o destinatário pode apresentar dados e a assinatura digital a terceiros como evidência, em caso de dúvida da autenticidade da origem.

Ao adicionar a criptografia de chave pública ao processo de assinatura digital, criamos um sistema criptográfico que pode fornecer quatro elementos essenciais à segurança: **privacidade**, **autenticação**, **integridade** e **não repúdio**.

TEMA 5 – INFRAESTRUTURA DE CHAVES PÚBLICAS

A principal característica da infraestrutura de chave pública (ICP) ou *public key infrastructure* (PKI) é que ela usa um par de chaves para prover os serviços de segurança subjacente. Como já vimos, o par de chaves é composto por chave privada e chave pública. Como as chaves públicas estão em domínio aberto, elas podem ser violadas, então é necessário se estabelecer e manter algum tipo de infraestrutura confiável para gerenciar essas chaves.

5.1 Gerenciamento de chaves

Já repetimos diversas vezes que a segurança de qualquer sistema criptográfico depende de quão seguramente suas chaves são gerenciadas. Sem procedimentos seguros para o manuseio de chaves criptográficas, os benefícios do uso de esquemas criptográficos fortes são potencialmente perdidos. Observamos que modelos criptográficos raramente são comprometidos por pontos fracos em seu *design*. No entanto, eles geralmente são comprometidos por meio do gerenciamento inadequado de chaves. Os aspectos mais importantes da gestão de chaves são os seguintes:

1. Chaves criptográficas não são nada mais que dados especiais.
2. Gerenciamento de chaves refere-se à administração segura de chaves criptográficas.
3. O gerenciamento de chaves lida com todo o ciclo de vida da chave, conforme mostrado na Figura 11.
4. Existem dois requisitos específicos de gerenciamento de chaves para

criptografia de chave pública:

4.1. **o segredo das chaves privadas**: durante todo o ciclo de vida da chave, as chaves secretas devem permanecer em segredo de todas as partes, exceto daquelas que são proprietárias e estão autorizadas a usá-las;

4.2. **a garantia das chaves públicas**: na criptografia de chave pública, as chaves públicas estão em ambiente aberto e são dados públicos. Por padrão, não há garantias de que uma chave pública está correta, a quem ela pode ser associada ou para o que ela pode ser usada. Então o gerenciamento de chaves públicas deve visar à garantia do propósito das chaves públicas.

O requisito mais importante da garantia da chave pública pode ser alcançado por meio da PKI, um dos principais sistemas de gerenciamento para apoiar a criptografia de chave pública.

Figura 11 – O ciclo de vida das chaves

A PKI fornece garantia de chave pública. Ela fornece a identificação de chaves públicas e sua distribuição. Uma estrutura de PKI compreende os seguintes componentes:

- certificado de chave pública, comumente chamado de *certificado digital*;
- *tokens* de chave privada;
- autoridade certificadora;
- autoridade de registro;
- sistema de gerenciamento de certificados.

5.2 Certificados digitais

Por analogia, um certificado pode ser considerado como a carteira de identidade para a pessoa. As pessoas usam a carteira de identidade, a carteira de motorista e o passaporte para provar sua identidade. Um certificado digital faz a mesma coisa no mundo eletrônico, mas com uma diferença: os certificados digitais não são emitidos apenas para pessoas – podem ser emitidos para computadores, pacotes de *software* ou qualquer outra coisa que precise provar sua identidade no mundo eletrônico.

Os certificados digitais são baseados no padrão X.509 da ITU, que define um formato de certificado-padrão para certificados de chave pública e validação de certificação. Portanto, os certificados digitais às vezes também são chamados de *certificados X.509*. A chave pública referente ao cliente do usuário é armazenada em certificados digitais pela autoridade certificadora (CA, de *Certification Autority*), juntamente com outras informações relevantes, como informações do cliente, data de validade, uso, emissor etc.

A CA assina digitalmente toda essa informação e inclui assinatura digital no certificado. Qualquer pessoa que precise da garantia sobre a chave pública e as informações associadas do cliente pode realizar o processo de validação de assinatura usando a chave pública da CA. A validação bem-sucedida assegura que a chave pública fornecida no certificado pertença à pessoa cujos detalhes são fornecidos no certificado. O processo de obtenção do certificado digital por uma pessoa/entidade é descrito na Figura 12. Conforme mostrado, a CA aceita o aplicativo de um cliente para certificar sua chave pública. A CA, depois de verificar devidamente a identidade do cliente, emite um certificado digital para esse cliente.

5.3 Autoridade certificadora (CA)

Como dissemos, a CA emite o certificado para um cliente e ajuda outros usuários a verificar o certificado. A CA assume a responsabilidade de identificar corretamente a identidade do cliente que está solicitando a emissão de um certificado e garante que as informações contidas no certificado estejam corretas e as assina digitalmente.

Figura 12 – A obtenção do certificado digital

As principais funções de uma CA são:

- **Geração dos pares de chaves**: a CA pode gerar um par de chaves independentemente ou em conjunto com o cliente.
- **Emissão de certificados digitais**: a CA pode ser considerada o equivalente PKI de uma agência de passaportes – a CA emite um certificado depois que o cliente fornece as credenciais para confirmar sua identidade. Então a CA assina o certificado para impedir a modificação de suas informações.
- **Publicação de certificados**: a CA precisa publicar certificados para que os usuários possam encontrá-los. Existem duas maneiras de se conseguir isso. Uma delas é publicar os certificados no equivalente a uma lista telefônica eletrônica. A outra é enviar seu certificado para as pessoas que você acha que podem precisar dele, de uma forma ou de outra.
- **Verificar certificados**: a autoridade certificadora disponibiliza sua chave pública no ambiente para auxiliar na verificação de sua assinatura no certificado digital dos clientes.
- **Revogação de certificados**: às vezes, a CA revoga o certificado emitido devido a algum motivo, como comprometimento da chave privada pelo usuário ou perda de confiança no cliente. Após a revogação, a CA mantém a lista de todos os certificados revogados disponíveis para o ambiente.

5.4 Classes de certificados

Existem quatro classes típicas de certificados:

- **Classe 1**: podem ser facilmente adquiridos por meio do fornecimento de um endereço de *e-mail*.
- **Classe 2**: exigem informações pessoais adicionais a serem fornecidas.
- **Classe 3**: só podem ser adquiridos após a verificação da identidade do solicitante.
- **Classe 4**: usados por governos e organizações financeiras que precisam de níveis muito altos de confiança.

5.5 Autoridade de registro (RA)

A CA pode usar uma autoridade de registro (*registration authority* – RA) terceirizada para executar as verificações necessárias da pessoa ou organização que solicita o certificado, para confirmar sua identidade. A RA pode parecer uma autoridade certificadora para o cliente, porém não assina o certificado emitido. O sistema de gerenciamento de certificados (*certificate management system* – CMS) é o sistema de gestão pelo qual os certificados são publicados, temporária ou permanentemente suspensos, renovados ou revogados.

Os sistemas de gerenciamento de certificados normalmente não excluem certificados porque pode ser necessário provar seu *status* em um determinado momento, talvez por motivos legais. Uma CA, juntamente com a RA associada, executa sistemas de gerenciamento de certificados para poder controlar suas responsabilidades e obrigações.

5.6 *Token* de chave privada

Enquanto a chave pública de um cliente é armazenada no certificado, a sua chave privada secreta associada pode ser armazenada no computador do proprietário da chave. Esse método geralmente não é adotado. Se um invasor obtiver acesso ao computador, ele poderá obter acesso à chave privada com facilidade. Por esse motivo, uma chave privada é armazenada em um acesso seguro, vinculado ao *token* de armazenamento removível protegido por uma senha. Diferentes fornecedores costumam usar formatos de armazenamento diferentes e, por vezes, proprietários, para armazenar chaves. Por exemplo, o Entrust usa o formato proprietário **.epf**, enquanto a Verisign, a GlobalSign e a Baltimore usam o formato padrão **.p12**.

5.7 Hierarquia de CAs

Com as redes de comunicações globais da atualidade e a ampla gama de requisitos de segurança, não é viável ter apenas uma CA confiável, da qual todos os usuários obtêm seus certificados. E a disponibilidade de apenas uma CA pode causar dificuldades, tanto pelo desempenho como se a CA for comprometida por um ataque ou vazamento. Nesse caso, o modelo de certificação hierárquica é de interesse, pois permite que certificados de chave pública sejam usados em ambientes em que duas partes em comunicação não têm relações de confiança com a mesma CA.

A **CA raiz** está no topo da hierarquia da CA e o certificado da CA raiz é um certificado autoassinado. As autoridades certificadoras secundárias, subordinadas diretamente à autoridade certificadora raiz, possuem certificados de autoridade certificadora assinados pela autoridade certificadora raiz. As autoridades certificadoras vinculadas às autoridades certificadoras subordinadas na hierarquia têm seus certificados de autoridade certificadora assinados pelas autoridades certificadoras subordinadas de nível superior e assim sucessivamente.

As hierarquias da CA são refletidas nas cadeias de certificados. Uma cadeia de certificados rastreia um caminho de certificados de uma ramificação na hierarquia até a raiz da hierarquia. A verificação de uma cadeia de certificados é o processo de garantir que uma cadeia de certificados específica seja válida, corretamente assinada e confiável. O procedimento descrito a seguir verifica uma cadeia de certificados, começando com o certificado apresentado para autenticação:

1. Um cliente cuja autenticidade está sendo verificada fornece seu certificado, geralmente junto com a cadeia de certificados até a CA raiz.
2. O verificador recebe o certificado e o valida, usando a chave pública do emissor.
3. A chave pública do emissor é encontrada no certificado do emissor, que está na cadeia ao lado do certificado do cliente.
4. Se a autoridade certificadora mais alta que assinou o certificado do emissor tiver a confiança do verificador, a verificação será bem-sucedida e será interrompida.
5. Além disso, o certificado do emissor é verificado de maneira semelhante à

do cliente, nas etapas antes descritas.

6. Esse processo continua até que uma CA confiável seja encontrada.

No Brasil, a infraestrutura de chaves públicas ICP-Brasil, vinculada ao Instituto Nacional de Tecnologia da Informação da Casa Civil da Presidência da República, é quem responde pela AC-raiz. A ela estão vinculadas todas as ACs de primeiro e segundo níveis e as autoridades de registro (ARs) da ICP-Brasil (Brasil, 2017).

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. **Coletânea de normas técnicas de segurança da informação**. Rio de Janeiro: ABNT, 2013.

BRASIL. Casa Civil da Presidência da República. Instituto Nacional de Tecnologia da Informação. **ICP-Brasil**. Brasília, 27 jun. 2017. Disponível em: <https://www.iti.gov.br/icp-brasil>. Acesso em: 8 dez. 2018.

FONTES, E. **Segurança da informação**. São Paulo: Saraiva, 2001.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw Hill, 2008.

KIM, D. **Fundamentos de segurança de sistemas de informação**. Rio de Janeiro: LTC, 2014.

STALINGS, W. **Criptografia e segurança de redes**: princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

TANENBAUM, A. S. **Redes de computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2001.