# Redes de computadores II

## Segurança em Redes de Computadores - Criptografia

**Conteúdo:** Criptografia

A criptografia pode ser utilizada para prover confidencialidade, mas ela também é essencial para prover autenticação, integridade de mensagem, não repudiação e controle de acesso. A criptografia permite que o remetente disfarce os dados de modo que um intruso não consiga obter nenhuma informação dos dados interceptados. O destinatário deve estar habilitado a recuperar os dados originais a partir dos dados disfarçados.

A mensagem em sua forma original é conhecida como **texto aberto** ou **texto claro**, um texto aberto pode ser criptografado usando um **algoritmo de criptografia**, de modo que a mensagem criptografada, conhecida como **texto cifrado**, pareça ininteligível para qualquer intruso.

Em sistemas criptográficos modernos, a técnica de codificação é conhecida, até mesmo por um intruso em potencial, por isso, é necessário uma informação secreta que impede que um intruso decifre os dados transmitidos, essa informação secreta é o que se conhece como **chave**.

A ideia é que o remetente forneça uma chave (vamos chamar de Kr) e uma cadeia de números ou caracteres como entrada para o algoritmo de criptografia. O algoritmo pega essa chave e o texto aberto da mensagem (m) como entrada e produz texto cifrado como saída. A notação Kr(m) refere-se à forma do texto cifrado (criptografado usando a chave Kr) da mensagem em texto aberto m.

De maneira semelhante, o destinatário fornecerá uma chave Kd ao **algoritmo de decodificação**, que pega o texto cifrado e a chave do destinatário como entrada e produz o texto aberto original como saída. Isto é, se o destinatário receber uma mensagem criptografada Kr(m), ele a decodificará calculando Kd(Kr(m)) = m.

Em **sistemas de chaves simétricas**, as chaves do remetente e destinatário são idênticas e secretas. Em **sistemas de chaves públicas** (**assimétricas)** é usado um par de chaves. Uma das chaves é conhecida pelo remetente e o destinatário (na verdade é conhecida pelo mundo inteiro). A outra chave é conhecida apenas pelo remetente ou pelo destinatário (mas não por ambos).

**Criptografia de chaves simétricas**

Todos os algoritmos criptográficos envolvem a substituição de um dado por outro, como tomar um trecho de um texto aberto e transformá-lo em um texto cifrado.

*Cifra de César

Um algoritmo de criptografia de chaves simétricas muito antigo e simples é o da **cifra de César** (uma cifra é um método para criptografar dados). A cifra de César funciona tomando cada letra do texto aberto e substituindo pela K-ésima letra sucessiva do alfabeto (o alfabeto é rotativo nesse caso, então a sucessora de Z volta a ser A e assim por diante).

Por exemplo: K=4

Texto aberto: UNIPAC

Texto cifrado: YRMTEG

O problema da cifra de César é que ela é simples de quebrar, pois há somente 25 valores possíveis para as chaves.

*Cifra monoalfabética

Esse tipo de cifra é um aprimoramento da cifra de César e também consiste em trocar uma letra do alfabeto por outra, mas, em vez de substituir usando um padrão regular, qualquer letra pode ser substituída por qualquer outra, contanto que cada letra tenha uma única letra substituta e vice-versa.

Exemplo:

| Letra no texto aberto: | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Letra no texto cifrado: | M | N | B | V | C | X | Z | A | S | D | F | G | H | J | K | L | P | O | I | U | Y | T | R | E | W | Q |

Esse tipo de cifra possibilita 26! (da ordem de $10^{26}$) possíveis pares de letras, em vez de apenas 25 usando a cifra de César. Embora esse métodos demande muito esforço para ser quebrado por meio de força bruta, pela análise estatística ele pode ser quebrado de maneira mais simples. Por exemplo, sabendo quais letras estão mais presentes em um determinado idioma, pode-se observar isso no texto cifrado e substituir a letra mais presente no texto cifrado pela letra mais frequente do idioma. Se tiver alguma noção do conteúdo da mensagem, pode-se buscar palavras específicas.

Dependendo do tipo de informação que o intruso tem, pode-se distinguir três cenários:

Ataque exclusivo a texto cifrado → O intruso pode ter acesso somente ao texto cifrado, sem nenhuma informação extra. Poderia, por exemplo, usar análise estatística.

Ataque com texto aberto conhecido → Se o intruso, por alguma razão, tiver certeza de que alguma palavra vai aparecer no texto cifrado, ele pode determinar os pares (texto aberto, texto cifrado) para as letras das palavras conhecidas. Quando um intruso conhece algum dos pares (texto aberto, texto cifrado), referimos a isso como ataque ao esquema criptográfico a partir de texto aberto conhecido.

Ataque com texto aberto escolhido → Nesse tipo de ataque, o intruso pode escolher a mensagem em texto aberto e obter seu texto cifrado correspondente. Nesse caso, o intruso precisa conseguir que a mensagem que ele quer seja enviada. Para técnicas de criptografia mais sofisticadas, um ataque com um texto aberto escolhido não significa necessariamente que a técnica criptográfica possa ser decifrada.

*Cifras polialfabéticas

Essa técnica tem como objetivo aprimorar a cifra monoalfabética. A ideia aqui é utilizar várias cifras monoalfabéticas com uma cifra monoalfabética específica para codificar uma letra em uma posição específica no texto aberto da mensagem.

Desse modo, a mesma letra, quando aparece em posições diferentes no texto aberto da mensagem, pode ser codificada de maneira diferente.

Um exemplo de esquema criptográfico polialfabético, seria utilizar as cifras de César com K1=5 e K2=19, pode-se então utilizar as cifras de César C1 e C2, onde C1 utiliza a chave K1 e C2 a chave K2. Com isso, pode-se utilizar um modelo de repetição C1, C2, C2, C1, C2. Dessa forma, a primeira letra seria codificada com a chave K1, a segunda e a terceira com K2, a quarta com K1 e a quinta com K2. A partir da sexta letra, o modelo se repete e assim por diante.

Nesse exemplo, a “chave” da codificação e da decodificação é o conhecimento das duas cifras de César (K1=5, K2=19) e do modelo C1, C2, C2, C1, C2.

*Cifras de bloco

Na cifra de bloco, a mensagem a ser criptografada é processada em blocos de K bits. Por exemplo, se K=64, então a mensagem é dividida em blocos de 64 bits, cada bloco é criptografado de maneira independente.

Para criptografar um bloco, a cifra utiliza um mapeamento um para um, no intuito de mapear o bloco de K bits de texto aberto para um bloco de K bits de texto cifrado. Por exemplo, se a cifra de bloco mapear entradas de 3 bits (texto aberto) para saídas de 3 bits (texto cifrado), um possível mapeamento seria:

| Entrada | Saída |
|---|---|
| 000 | 110 |
| 001 | 111 |
| 010 | 101 |
| 011 | 100 |

| Entrada | Saída |
|---|---|
| 100 | 011 |
| 101 | 010 |
| 110 | 000 |
| 111 | 001 |

Nesse caso, a mensagem 010 110 001 111 é criptografada para 101 000 111 001.

Esse é apenas um de muitos mapeamentos possíveis, nesse caso existem $2^3$ entradas e 8! mapeamentos possíveis. Para criptografar e decodificar mensagens desse tipo, basta saber o mapeamento (chave). Nesse caso, como existem 8! mapeamentos possíveis, um computador de mesa pode quebrar isso facilmente utilizando força bruta.

Para impedir esse tipo de ataque, as cifras de bloco normalmente usam blocos maiores, por exemplo K=64 bits ou mais. Nesse caso, o número de mapeamentos possíveis é $2^{k!}$, para K=64 é um alto número. A desvantagem disso é que se torna um esquema difícil de implementar, pois é necessário manter uma tabela com muitos valores de entrada, supondo que o valor de K é elevado.

Para amenizar essa situação, as cifras de bloco normalmente usam funções para simular, de maneira aleatória, as tabelas permutadas. Supondo o K=64 bits, um exemplo disso seria dividir o bloco em blocos menores de 8 bits e criar tabelas para cada bloco de 8 bits.

**Criptografia de chave pública (assimétrica)**

Na criptografia de chaves simétricas, a chave simétrica é usada para codificar e decodificar, ou seja, a chave deve ser compartilhada entre as partes e isso deve ser feito de forma segura, pois se um intruso obtiver a chave, ele consegue decodificar a mensagem desde que conheça o algoritmo.

Em 1976, Diffie e Hellman apresentaram um algoritmo que permite que as chaves se comuniquem por criptografia sem compartilhar uma chave comum secreta conhecida com antecedência. Esse algoritmo é conhecido como **troca de chaves DiffieHellman**.

Essa abordagem levou ao desenvolvimento dos atuais sistemas de criptografia de chaves públicas. O conceito de criptografia de chaves públicas é simples. Em vez do remetente e o destinatário compartilharem uma única chave secreta, o destinatário tem duas chaves, uma **chave pública ($K_d^+$)**, que está a disposição do mundo todo e uma **chave privada ($K_d^-$)**, que apenas o destinatário conhece.

O remetente busca primeiro a chave pública do destinatário, em seguida ele criptografa sua mensagem m usando a chave pública do destinatário e um algoritmo de criptografia padronizado, ou seja, o remetente calcula $K_d^+(m)$.

O destinatário recebe a mensagem criptografada e usa sua chave privada e um algoritmo de decodificação conhecido para decifrar a mensagem, ou seja, o destinatário calcula $K_d^-(K_d^+(m))$. Isso é possível, pois há algoritmos de criptografia e decodificação para escolher chaves públicas e privadas de modo que:

$$K_d^-(K_d^+(m)) = m$$

Também é possível permutar as chaves e obter o mesmo resultado, ou seja:

$$K_d^-(K_d^+(m)) = K_d^+(K_d^-(m)) = m$$

Uma preocupação é que um intruso conhece tanto a chave pública, quanto o algoritmo de criptografia usado pelo remetente. Obviamente, para a criptografia de chave pública funcionar, a escolha da chave e códigos de criptografia deve ser feita de modo que torne extremamente difícil para um intruso determinar a chave privada do destinatário ou conseguir decifrar ou adivinhar a mensagem.

Outra preocupação é que, como a chave é pública, qualquer um pode enviar uma mensagem cifrada ao destinatário. Nesse caso, é necessário vincular um remetente a uma mensagem.

**Referências bibliográficas:**

TANENBAUM, Andrew. S. Redes de Computadores. São Paulo: *Pearson*, 5ª Ed. 2011.

KUROSE, James F.; ROSS, Keith W. Redes de Computadores e a Internet – Uma Abordagem Top-Down. *São Paulo: Pearson*, 6ª Ed. 2013.