Criprografia Simétrica

Criptografia

António Santos

ISTEC

Tópicos

Definição

A encriptação simétrica, também chamada de encriptação convencional, encriptação de chave única ou chave privada, era o único tipo de criptografia em uso antes do desenvolvimento da encriptação por chave pública na década de 1970.

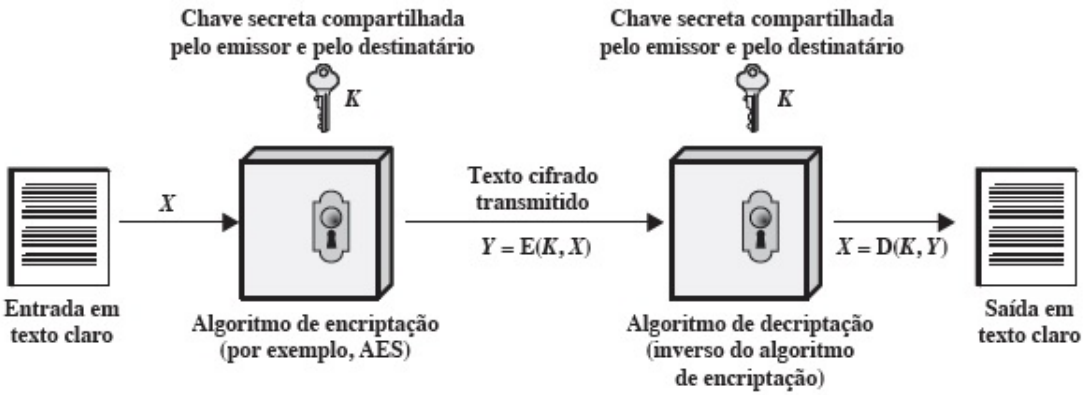
Texto Claro vs Texto Cifrado

Uma mensagem original é conhecida como texto claro (ou plaintext), enquanto a mensagem codificada é chamada de texto cifrado (ou ciphertext).

Encriptação vs Decriptação

O processo de converter um texto claro num texto cifrado é conhecido como cifração ou encriptação
Restaurar o texto claro a partir do texto cifrado é apelidado de decifração ou decriptação.

Modelo simplificado da encriptação simétrica.



Esquema de encriptação simétrica

- Texto claro: essa é a mensagem ou dados originais, inteligíveis, que servem como entrada do algoritmo de encriptação.
- Algoritmo de encriptação: realiza diversas substituições e transformações no texto claro.
- Chave secreta: também é uma entrada para o algoritmo de encriptação. A chave é um valor independente do texto claro e do algoritmo. O algoritmo produzirá uma saída diferente, dependendo da chave usada no momento. As substituições e transformações exatas realizadas pelo algoritmo dependem da chave.

Esquema de encriptação simétrica

- Texto cifrado: essa é a mensagem embaralhada, produzida como saída do algoritmo de encriptação. Ela depende do texto claro e da chave secreta. Para determinada mensagem, duas chaves diferentes produzirão dois textos cifrados distintos. O texto cifrado é um conjunto de dados aparentemente aleatório e, nesse formato, ininteligível.
- Algoritmo de decriptação: esse é basicamente o algoritmo de encriptação executado de modo inverso. Ele pega no texto cifrado e a chave secreta e produz o texto claro original.

Requisitos para o uso seguro da encriptação simétrica

1. Precisamos de um algoritmo de encriptação forte. No mínimo, gostaríamos que o algoritmo fosse tal que um oponente que conheça o algoritmo e tenha acesso a um ou mais textos cifrados seja incapaz de decifrar o texto cifrado ou descobrir a chave. Esse requisito normalmente é indicado de maneira mais forte: o invasor deverá ser incapaz de decriptar o texto cifrado ou descobrir a chave, mesmo que possua diversos textos cifrados com seus respetivos textos claros.
2. Emissor e recetor precisam ter obtido cópias da chave secreta de uma forma segura e mantê-la protegida. Se alguém conseguir descobrir a chave e o algoritmo, toda a comunicação usando essa chave poderá ser lida.

Esquema de encriptação simétrica

Com a mensagem X e a chave de encriptação K como entradas, o algoritmo de encriptação produz o texto cifrado $Y = [Y_1, Y_2, \cdots, Y_N]$. Podemos escrever isso como:

$$Y = E(K, X)$$

O receptor legítimo, de posse da chave, é capaz de inverter a transformação:

$$X = D(K, Y)$$

Segurança Criptográfica

- Não deve haver maneira de recuperar o texto não criptografado do criptograma (segurança contra o primeiro ataque).
- Todo sistema criptográfico deve ser composto de dois tipos de informações:
  - Público: refere-se à família de algoritmos que definem o sistema criptográfico.
  - Privado: é conhecido apenas pelo utilizador. A chave de criptografia de cada utilizador em particular.

Segurança Criptográfica

- A maneira de escolher a chave deve ser fácil de lembrar e modificar.
- Deve ser possível comunicar o criptograma com os meios habituais de transmissão.
- A complexidade do processo de recuperação de texto original deve corresponder ao benefício obtido (o custo é proporcional ao segredo que você deseja manter).

Segurança do Algoritmo

- Segredo Perfeito: A mensagem é segura contra tempo e recursos ilimitados.
  Nesse tipo de criptografia, o tamanho da chave é maior ou igual ao tamanho do texto a ser criptografado.
- Segredo computacional: a mensagem é segura contra ataques com tempo e recursos limitados.
  Exemplo: sistemas de criptografia de chave pública.

Segurança do Algoritmo

- Provável segredo: a mensagem provavelmente está segura.
  Exemplo: sistemas de criptografia de chave privada.
- Segredo condicional: a segurança da mensagem depende das características da sua vizinhança.
  Exemplo: uma mensagem não criptografada ou criptografada usando sistemas de criptografia clássicos, que é enviada por uma rede "segura".