



Faculdade de Ciência e Tecnologia

CRIPTOGRAFIA

**A CRIPTOGRAFIA NA
SEGURANÇA DE DADOS**

Rodrigo Alves
Silas Ribas
Zenilson



Apresentando

- “Cripto” vem do grego *kryptós* e significa oculto, envolto, escondido. Também do grego, “*graphos*” significa escrever, “*logos*” significa estudo, ciência e, “*analysis*” significa decomposição. Daí, CRIPTOLOGIA é o estudo da escrita cifrada e se ocupa com a CRIPTOGRAFIA, a escrita secreta, e a CRIPTOANÁLISE, a quebra do segredo.
- A criptografia é a ciência de escrever mensagens que ninguém deveria poder ler, exceto o remetente e o destinatário. A criptoanálise é a ciência de “quebrar” o método utilizado, decifrar e ler estas mensagens cifradas.

Apresentando

- Com a criação da escrita e o contato entre os povos, surge a necessidade de esconder informações, assim chega-se à base da Criptografia.
- Inicialmente é considerada como a arte de esconder informações.
- Hoje é tratada como ciência e possui estudos sigilosos e importantes realizados por empresas, governos e ainda por civis.

A Criptografia na História

- Método auto-chave – inventado por Girolamo Cardano (1501-1576).
- Esteganografia – apresentada por Sir Francis Bacon (1561-1626).
- Método de leitura Braille – adaptado por Louis Braille (1809-1852) que ficou cego aos 3 anos de idade. É universalmente aceito e utilizado até os dias de hoje.

A Criptografia na História

- Código Morse – desenvolvido pelo assistente de Samuel Morse (1791-1872). Na verdade não é um código, mas sim um alfabeto cifrado em sons curtos e longos.

A criptografia, através das “Máquinas de Cifragem”, foi uma das mais poderosas armas utilizadas na Primeira Guerra Mundial.

A Criptografia na História

- O Brasil também tem influência na Criptografia. Com o padre brasileiro José Francisco de Azevedo, o qual inventa a “Máquina de Escrever”. Além de matemático, era excelente mecânico.
- Código de César – que é o único da Antiguidade que continua sendo usado até hoje.

A Importância da Criptografia

- Os computadores são a expressão maior da era digital, marcando presença em praticamente todas as atividades humanas. Da mesma forma como revolucionaram a informação, também causaram uma reviravolta na criptologia: por um lado ampliaram seus horizontes, por outro tornaram a criptologia quase que indispensável.

A Criptografia à Serviço da Segurança de Dados

- A transmissão de dados, qualquer tipo, desde os menos até os mais importantes, tem uma rota, a qual passa-se por vários pontos, os quais podemos ou não confiar, muitas vezes nem sabemos quais são.
- Os dados podem ser roubados, sendo desviado ou copiados.

Técnicas de Criptografia

- Para implementação de um sistema seguro, pode-se utilizar de uma série de técnicas:
 - criptografia convencional
 - criptografia de chave pública
 - autenticação
 - certificação e assinatura digital.

Técnicas de Criptografia

- **Substituição Monoalfabética** (Código de César)
 - Imperador Romano Júlio César usava na sua correspondência um código de substituição no qual cada letra da mensagem original era substituída pela letra que a seguia em três posições no alfabeto: a letra A era substituída por D, a B por E, e assim sucessivamente.

Hoje em dia, porém, a denominação de Código de César é utilizada para qualquer cifra na qual cada letra da mensagem clara seja substituída por outra deslocada um número fixo de posições.

Técnicas de Criptografia

- **Substituição Monoalfabética** (Código de César)

Texto Claro

S I L A S

Texto Cifrado

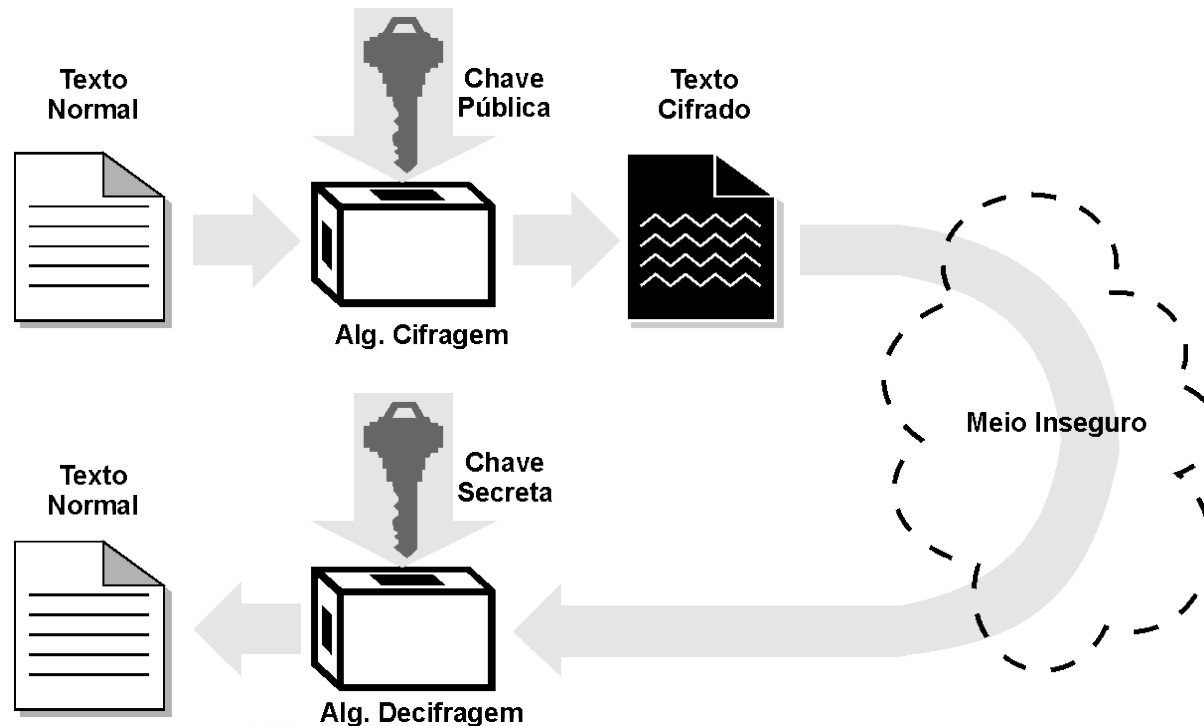
V L O D V

Usando deslocamento de 3 casas.

Técnicas de Criptografia

■ Chave Pública

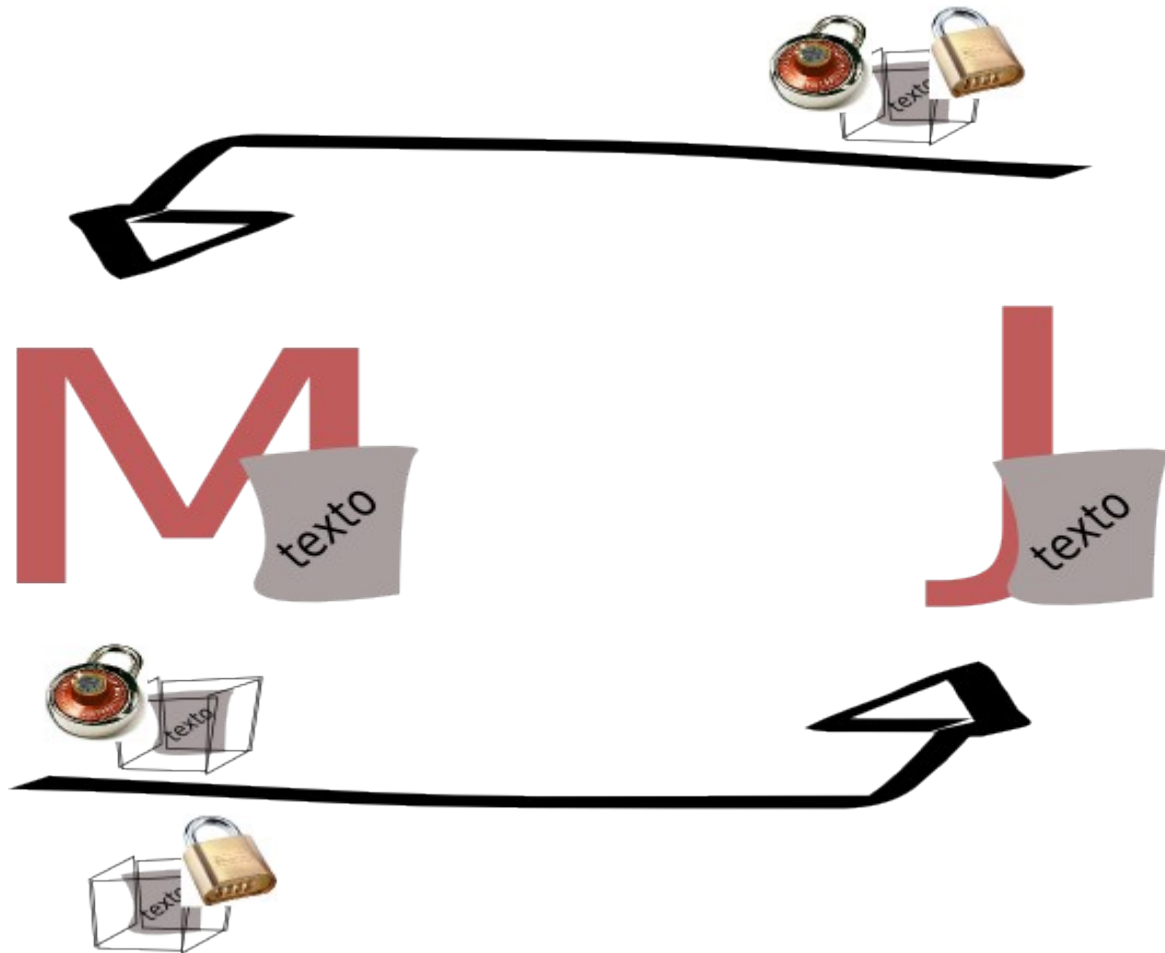
- Cifragem é feita através de uma chave pública;
- Decifração é feita através de uma chave privada;



Técnicas de Criptografia

- Digamos que Maria queira enviar uma mensagem para João. Ela coloca a mensagem numa caixa de metal, fecha a caixa com um cadeado (só ela tem a chave deste cadeado) e a envia para João. João também coloca um cadeado na caixa (só ele tem a chave deste segundo cadeado) e devolve a caixa para Maria. Ao receber a caixa, Maria abre e retira o seu cadeado e, novamente, envia a caixa para João. Agora, João pode tirar o seu cadeado, abrir a caixa e ler a mensagem.

Técnicas de Criptografia



criptografia

Criptografia

- A segurança de dados é algo indispensável, desde a antiguidade já sabíamos disso.
- A sua aliança com, a arte que virou ciência, a criptografia é útil e muito importante, garantindo o mínimo de segurança contra roubos e qualquer meio de uso indevido de informação.
- Informação é poder, manter-se seguro do roubo de informações, além de muito importante, é muito necessário.