Criptografia Simétrica

Segurança e Auditoria em Sistemas

Profa. Natássya Barlate Floro da Silva

Universidade Tecnológica Federal do Paraná -– Câmpus Cornélio Procópio

10 de Março de 2020

Roteiro

Introdução

- *kryptós*: escondido.
- *graphein*: escrita.
- Criptografia: "Arte ou ciência de escrever em cifras (códigos)".

Introdução

- *kryptós*: escondido.
- *graphein*: escrita.
- Criptografia: "Arte ou ciência de escrever em cifras (códigos)".

Introdução

Criptografia

Conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que apenas o destinatário a decifre e a compreenda.

Criptoanálise

Estudo de técnicas para decifrar mensagens sem conhecimento dos detalhes dos algoritmos de criptografia; "quebra" da criptografia.

Criptologia

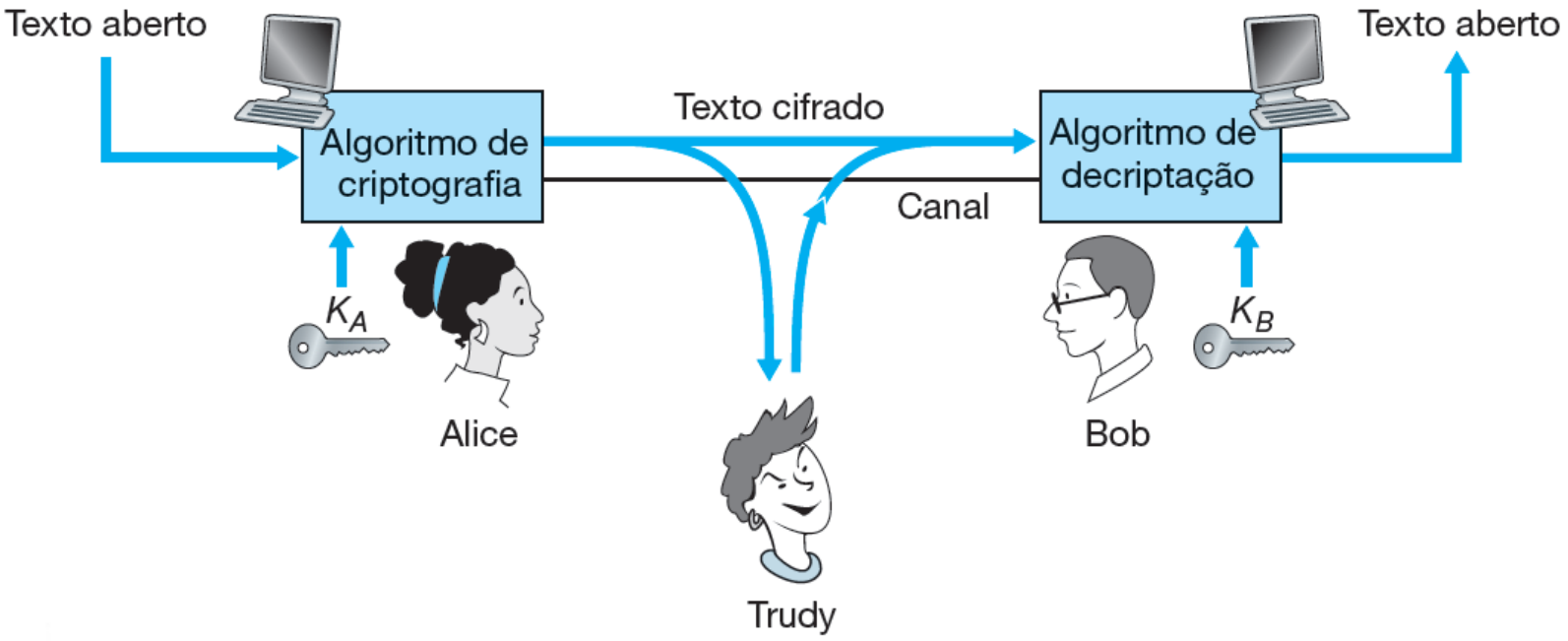
Criptografia + Criptoanálise.

Introdução

- **Texto claro (*plaintext*)**: mensagem original;
- **Criptografia:** processo que torna a mensagem incompreensível;
- **Texto cifrado (*ciphertext*):** conjunto de dados aparentemente aleatório, ininteligível (mensagem embaralhada);
- **Decriptografia:** processo inverso ao de criptografia, recuperando a mensagem original a partir do texto cifrado;
- **Chave secreta:** entrada do algoritmo de criptografia, usada para criptografar o texto claro;

Introdução

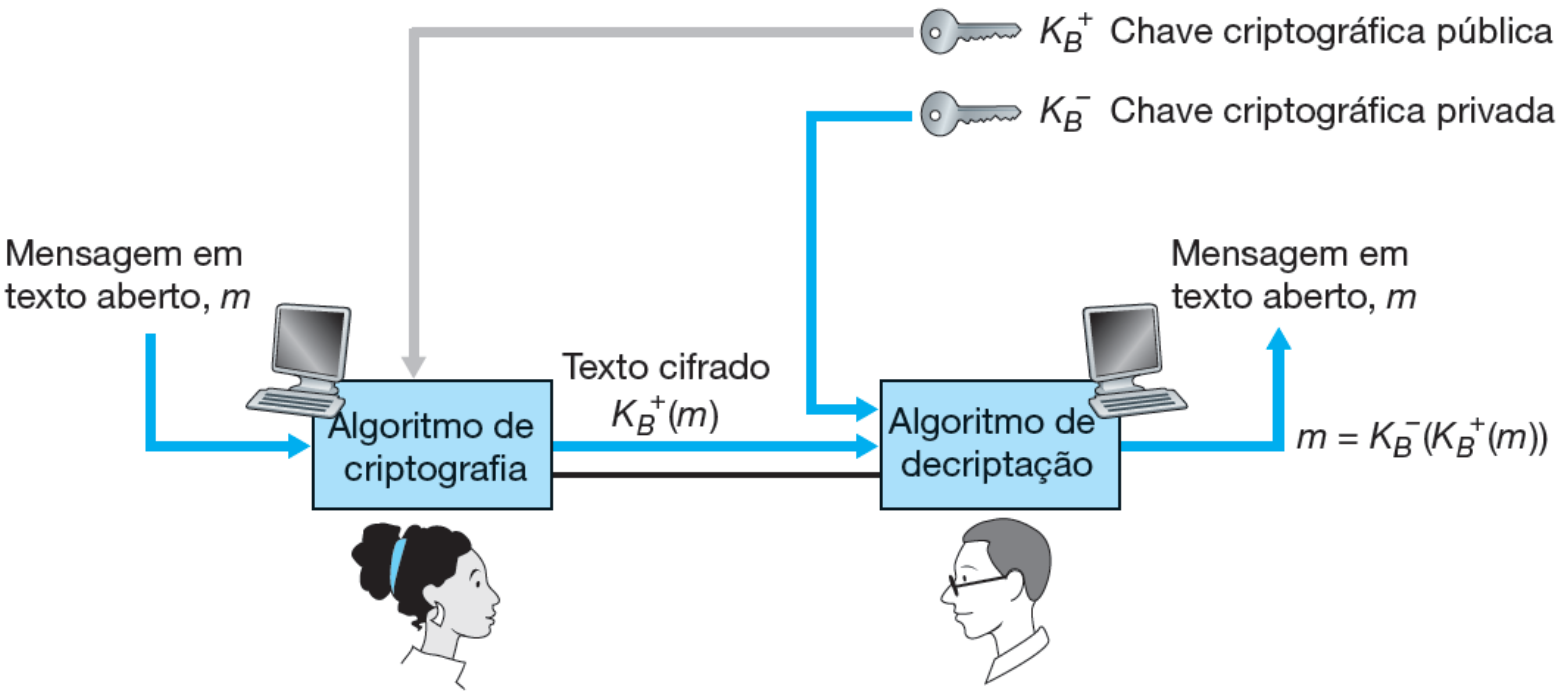
- Criptografia simétrica:



- Exemplos: AES, DES, 3DES.

Introdução

- Criptografia assimétrica:



- Exemplos: RSA e ECC.

Introdução

- Ataques de algoritmos de criptografia:
  - **Ataque de força bruta**: o atacante testa todas as chaves possíveis em um trecho do texto cifrado, até obter uma tradução inteligível para o texto claro. Na média, metade de todas as chaves possíveis precisam ser experimentadas para então se obter sucesso.
  - **Criptoanálise**: o atacante analisa propriedades dos algoritmos ou utiliza de ferramentas matemáticas para reduzir consideravelmente o universo de busca de chaves possíveis ou a própria chave.

Criptografia Simétrica

- **Técnicas de substituição**: letras do texto claro são substituídos por outras letras, números ou símbolos.
- **Técnicas de transposição**: trocas de posições das letras do texto claro.

Criptografia Simétrica

- **Técnicas de substituição**: letras do texto claro são substituídos por outras letras, números ou símbolos.
- **Técnicas de transposição**: trocas de posições das letras do texto claro.

- **Cifra de fluxo**: criptografia de um bit ou byte por vez.
- **Cifra de bloco**: um bloco do texto claro é tratado como um todo e usado para produzir o texto cifrado com o mesmo tamanho.

Criptografia Simétrica

- **Técnicas de substituição**: letras do texto claro são substituídos por outras letras, números ou símbolos.
- **Técnicas de transposição**: trocas de posições das letras do texto claro.

- **Cifra de fluxo**: criptografia de um bit ou byte por vez.
- **Cifra de bloco**: um bloco do texto claro é tratado como um todo e usado para produzir o texto cifrado com o mesmo tamanho.

- **Mono-alfabética**: alfabeto de entrada igual ao de saída.
- **Poli-alfabética**: alfabeto de entrada diferente do de saída.

Cifra de César

- Um dos usos mais antigos usos de cifra de substituição mono-alfabética.
- Cada letra do alfabeto é substituída por uma letra disposta 3 adiante.
- Exemplo:

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
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Texto claro: m e d i v i r t o n e s s a a u l a
Texto cifrado: P H GLYLUWR QHVVD DXOD

Cifra de Deslocamento

- Generalização da Cifra de César.
  - Criptografia: $c = (m + k) \mod n$
  - Decriptografia: $m = (c - k) \mod n$
  - c: texto cifrado
  - m: texto claro
  - k: chave (deslocamento)
  - n: quantidade de símbolos ou letras

Cifra de Deslocamento

- Exemplo: n = 26 e k = 20

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
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T

Texto claro: me divirto nessa aula
Texto cifrado: GY XCPCLNI HYMMU UOFU

Cifra de Deslocamento

- Criptoanálise: possível quebrar com apenas 26 tentativas.
- Exemplo: vdrcx ojlru mn zdnkaja

Cifra de Deslocamento

- Criptoanálise: possível quebrar com apenas 26 tentativas.
- Exemplo: vdrcx ojlru mn zdnkaja
- Possibilidades:
  - ucqbw nikqt lm ycmjziz
  - tbpav mhjps kl xbliyhy
  - saozu lgior jk wakhxgx
  - rznyt kfhnq ij vzjgwfw
  - qymxs jegmp hi uyifvev
  - pxlwr idflo gh txheudu
  - owkvq hcekn fg swgdtct
  - nvjup gbdjm ef rvfcsbs
  - muito facil de quebrar $\rightarrow$ k=9

Cifra de Vigenère

- A mais conhecida cifra de substituição poli-alfabética.
- Uso da substituição e de uma chave que define uma variação da regra para a transformação.
- Exemplo:

Chave:	e n g a n o e n g a n o e n g a n o
Texto claro:	m e d i v i r t o n e s s a a u l a
Texto cifrado:	Q R J I I W V G U N R G W N G U Y O

- Numericamente:

Chave:	4 13 6 0 13 14 4 13 6 0 13 14 4 13 6 0 13 14
Texto claro:	12 4 3 8 21 8 17 19 14 13 4 18 18 0 0 20 11 0
Texto cifrado:	16 17 9 8 8 22 21 6 20 13 17 6 22 13 6 20 24 14

Cifra de Vigenère

- Segurança maior do que da Cifra de Deslocamento pois há uma maior combinação de chaves possíveis.
- Exemplo: $26^6 = 308915776$ combinações possíveis.

One-time Pad

- *One-time Pad*:
  - Chaves geradas de forma aleatória: 1 chave para cada mensagem.
  - Chave do tamanho da mensagem.
  - Cifra inquebrável.
- Exemplo:

Texto cifrado:	A N K Y O D K Y U R E P F J B Y
Chave:	p x l m v m s y d o f u y r v z
Texto claro:	m r m u s t a r d w i t h t h e

Texto cifrado:	A N K Y O D K Y U R E P F J B Y
Chave:	m f u g p m i y d g a x g o u f
Texto claro:	m i s s s c a r l e t w i t h t

One-time Pad

- Problemas:
  - Segurança depende da aleatoriedade da chave.
  - A distribuição de chaves é um problema muito grande.
- Na prática, não é utilizado.

Exercício

Exercício 1

Faça um ataque de força bruta ou criptoanálise e encontre o texto claro e a chave das seguintes mensagens:

a. Cifra de deslocamento: zktnuasykmxkjuvgxgktbogx.
b. Cifra de Vigenère cuja chave se encontra dentro do texto desse slide (sem acentos): awssfhvwxwhiexfwacpe.

Exercício

Exercício 2

Este problema explora o uso do *one-time pad*. Nesse esquema, a chave é um fluxo de números aleatórios entre 0 e 26. por exemplo, se a chave for 3 19 5..., então a primeira letra do texto claro é encriptada com um deslocamento de três letras, a segunda com um deslocamento de 19 letras, a terceira com um deslocamento de cinco letras, e assim por diante.

a. Encripte o texto claro *sendmoremoney* com o fluxo de chaves 9 0 1 7 23 15 21 14 11 11 2 8 9.

b. Usando o texto cifrado produzido na parte a, encontre uma chave, de modo que o texto cifrado seja decriptado para o texto claro cashnotneeded.