Criptografia

Gabriel Prates da Costa

Segurança e Auditoria de SI.

Instituto Federal de Educação Ciência e Tecnologia Farroupilha (IFFAR) -
Campus Alegrete
Curso: Análise e Desenvolvimento de Sistemas

16/11/2021

INSTITUTO FEDERAL
Farroupilha | Campus Alegrete

Roteiro

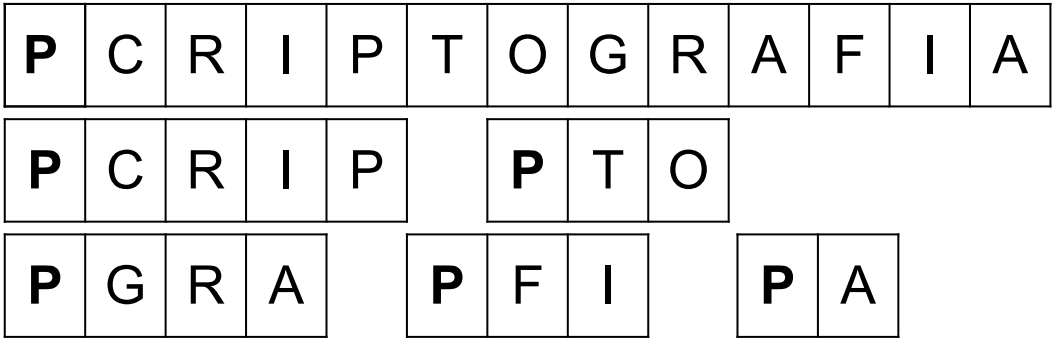
1. O que é criptografia?
2. Onde encontramos?
3. Divisões da criptografia:
    - Simétrica:
        - Cifras de bloco:
            - Prática.
        - Cifras de fluxo.
    - Assimétrica:
        - Prática.

Roteiro

1. O que é criptografia?
2. Onde encontramos?
3. Divisões da criptografia:
    - Simétrica:
        - Cifras de bloco:
            - Prática.
        - Cifras de fluxo.
    - Assimétrica:
        - Prática.

O que é criptografia?

- O conceito mais conhecido de criptografia é a “prática e o estudo de utilizar técnicas matemáticas para a comunicação segura na presença de terceiros”.



INSTITUTO FEDERAL
Farroupilha
Campus Alegrete

Roteiro

1. O que é criptografia?
2. Onde encontramos?
3. Divisões da criptografia:
    - Simétrica:
        - Cifras de bloco:
            - Prática.
        - Cifras de fluxo.
    - Assimétrica:
        - Prática.

Onde encontramos?

- A criptografia de uma informação pode estar presente em diversos locais diferentes mas pode ser lida apenas por quem tem posse do segredo para decodificá-la.
- Esse tipo de procedimento é utilizado geralmente quando precisamos armazenar informações sigilosas (como em arquivos ou banco de dados) ou também para trafegar dados em um canal não seguro.

Roteiro

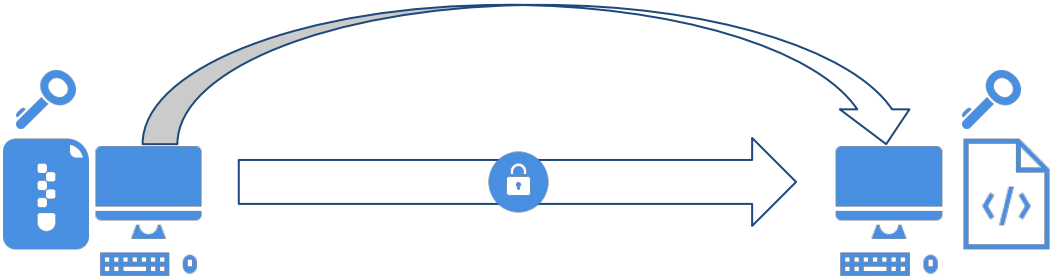
1. O que é criptografia?
2. Onde encontramos?
3. Divisões da criptografia:
    - Simétrica:
        - Cifras de bloco:
            - Prática.
        - Cifras de fluxo.
    - Assimétrica:
        - Prática.

Divisões da criptografia

- Dividimos a criptografia em 2 tipos:
  - Simétrica;
  - Assimétrica.

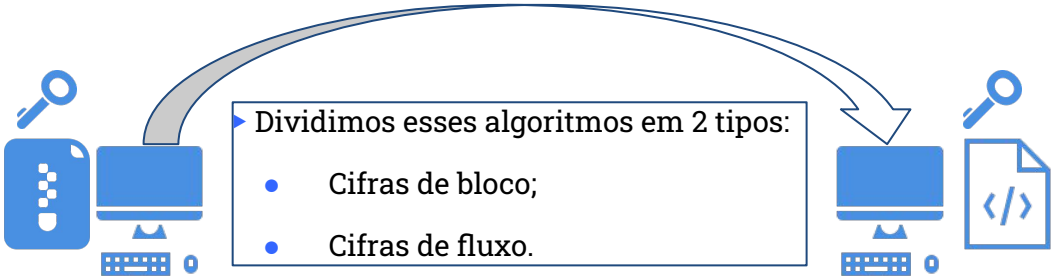
Divisões da criptografia

- Dividimos a criptografia em 2 tipos:
  - **Simétrica;**
  - Assimétrica.



Divisões da criptografia

- Dividimos a criptografia em 2 tipos:
  - **Simétrica;**
  - Assimétrica.



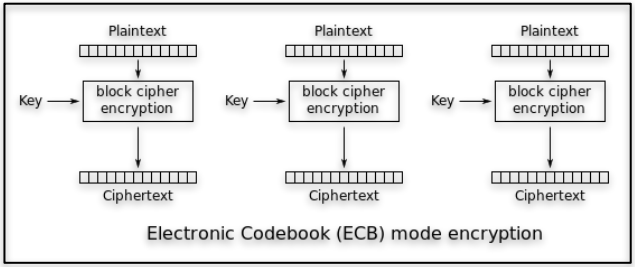
Divisões da criptografia

- Dividimos esses algoritmos em 2 tipos:
  - **Cifras de bloco;**
  - Cifras de fluxo.
- **A**dvanced **E**ncryption **S**tandart (AES) ⟹ blocos de 128 bits
- **E**lectronic **C**ode **B**ook (ECB);
- **C**ipher **B**lock **C**haining (CBC);
- **C**ipher **F**eedback **B**lock (CFB);
- **O**utput **F**eedback **B**lock (OFB).

} Modo de operação

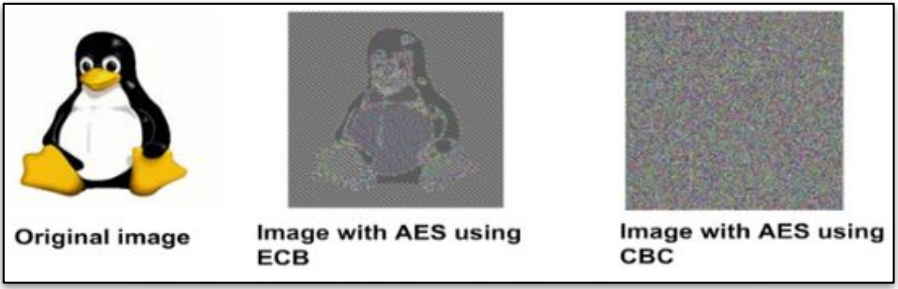
Divisões da criptografia

- Cifras de Bloco:
  - AES ⟹ Tamanho da chave simétrica: 128, 192 e 256 bits
    - ECB



Divisões da criptografia

- Cifras de Bloco:
  - AES ⟹ Tamanho da chave simétrica: 128, 192 e 256 bits
    - ECB



Prática

- Criptografando um texto com o AES:
  - Gerar uma chave simétrica (Ex.: AES-256-CTR):

```
$ openssl rand -hex -out crypto.key 32
```

  - Gerar um vetor de inicialização (IV):

```
$ openssl rand -hex -out crypto.iv 16
```

Prática

- Criptografando um texto com o AES:
  - Então criptografamos de fato:

```
$ openssl enc -e -aes-256-ctr -K `cat crypto.key` -iv `cat crypto.iv` -a <<< "criptografia"
```

- Para descriptografar um texto com o AES:
  - Utilizamos o mesmo código com outro argumento:

```
$ openssl enc -d -aes-256-ctr -K `cat crypto.key` -iv `cat crypto.iv` -a <<< "pR1uFovUV5DSvMlLYg=="
```

Divisões da criptografia

- Dividimos esse algoritmo em 2 tipos:
  - Cifras de bloco;
  - **Cifras de fluxo.**
- Trabalha com Streams de dados contínuos (corrente de bits);
- Geralmente utilizadas quando precisa-se de muita velocidade para processar os dados de entrada e conta com limitações de hardware;
- O mais recomendado é o Chacha20 (utilizado no TLS, OpenSSH e em VPNs).

- Outra Cifra de fluxo comumente utilizada em nossos smartphones no dia a dia é o E0.

Divisões da criptografia

- Dividimos a criptografia em 2 tipos:
  - Simétrica;
  - **Assimétrica.**
- Para esse tipo de criptografia são utilizadas chaves diferentes para criptografar e descriptografar;
- Vamos utilizar como exemplo o RSA que também é muito utilizado em versões do TLS e usa como base números primos;
- O RSA utiliza um valor multiplicado para criptografar e os números primos originais para descriptografar. Juntamente com outros mecanismos e cálculos envolvidos no processo.

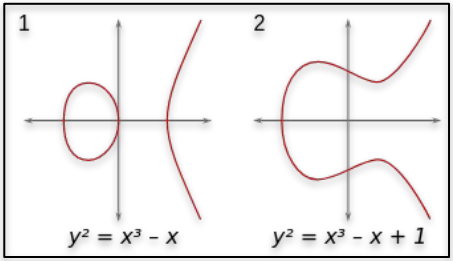
- Uma chave pública pode ser usada.

Divisões da criptografia

- Uma outra abordagem para criptografia assimétrica é o uso de curvas elípticas ao invés dos números primos do RSA.

- São equações de terceiro grau, muito utilizadas em diversas àreas matemáticas para provar teoremas e representar números complexos.

- São os representados pela unidade imaginária i.



- $\Delta=4^2-4*(-1)*(-16)$
  $\Delta=-100$

Prática

- Criptografando um texto com criptografia assimétrica:
  - Gerar uma chave privada:

```
$ openssl genrsa -out private.key
```

  - Gerar uma chave pública a partir dela:

```
$ openssl rsa -pubout -in private.key -out public.key
```

Prática

- Criptografando um texto com criptografia assimétrica:
  - Criptografando o texto desejado:

```
$ openssl rsautl -encrypt -inkey public.key -pubin -out crypt.bin <<< "criptografia"
```

  - Como essa criptografia gera um binário, utilizamos o seguinte código para visualizar o resultado:

```
$ base64 crypt.bin
```

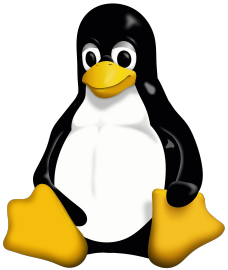
Prática

- Para descriptografar um texto com criptografia assimétrica:
  - Utilizamos a chave privada com um comando parecido com o de criptografar. Porém com algumas mudanças:

```
$ openssl rsautl -decrypt -inkey private.key -in crypt.bin
```

▸ Obrigado!

gabriel.prates.costa@gmail.com



INSTITUTO FEDERAL
Farroupilha
Campus
Alegrete

Referências

- Criptografia (Guia Básico para Entender Como Funciona) // Dicionário do Programador. 2021. Disponível em: <https://www.youtube.com/watch?v=qHFbuXpz7e4>
- Entendendo Conceitos Básicos de CRIPTOGRAFIA | Parte 1/2. 2019. Disponível em: <https://www.youtube.com/watch?v=CcU5Kc_FN_4>
- Entendendo Conceitos Básicos de CRIPTOGRAFIA | Parte 2/2. 2019. Disponível em: <https://www.youtube.com/watch?v=HCHqtpipwu4>
- PINHEIRO. José Mauricio Santos, 2010. Cifras em Bloco e Cifras de Fluxo. Disponível em: <https://www.projetoderedes.com.br/artigos/artigo_cifras_em_bloco_cifras_de_fluxo.php>
- AWATI. Rahul, 2021. Electronic Code Book (ECB). Disponível em: <https://searchsecurity.techtarget.com/definition/Electronic-Code-Book>
- OBE. Bill Buchanan, 2020. Surely No-one Uses ECB Mode in AES?. Disponível em: <https://medium.com/asecuritysite-when-bob-met-alice/surely-no-one-uses-ecb-mode-in-aes-332ed90f29d0>
- Icons8. 2021. Disponível em: <https://icons8.com/icons>