SEGURANÇA DA INFORMAÇÃO

Cifras simétricas

ROTEIRO

- Cifras simétricas
- Tipos
- Exemplos
- Algoritmos

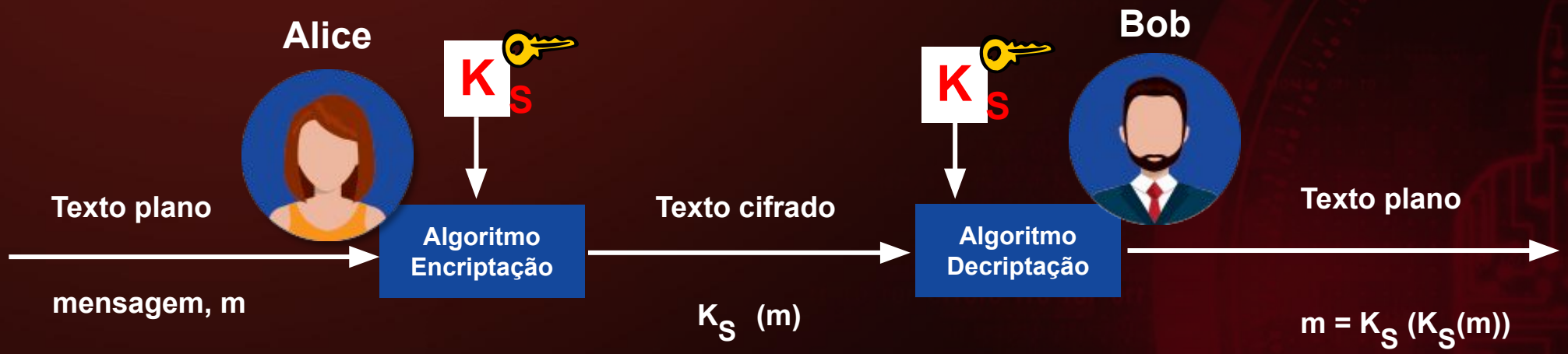
CIFRAS SIMÉTRICAS

A criptografia de chave simétrica, ou cifra simétrica, consiste em utilizar a mesma chave entre duas partes comunicantes. No exemplo anterior, Bob e Alice vão compartilhar a mesma chave para encriptar e decriptar a mensagem trocada entre eles

Chave do emissor e transmissor são idênticas.

A chave é um padrão de substituição de alguma coisa por outra.

CIFRAS SIMÉTRICAS



Etapas: Bob e Alice compartilham a mesma chave (simétrica) → K
A chave K é um padrão de substituição

CIFRAS SIMÉTRICAS

Exemplo padrão de substituição

```
Texto plano: abcdefghijklmnopqrstuvwxyz
```

```
Texto cifrado: mnbvcxzasdfghjklpoiuytrewq
```

Chave de encriptação: mapeamento de 26 letras para outras 26 letras

CIFRAS SIMÉTRICAS

Tipos de cifras simétricas

Cifras de fluxo

- ✔ Consiste em criptografar 1 bit de cada vez

Cifras de Bloco

- ✔ As mensagens de texto aberto são quebradas em blocos de mesmo tamanho
- ✔ Cada bloco corresponde a 1 unidade

CIFRAS SIMÉTRICAS

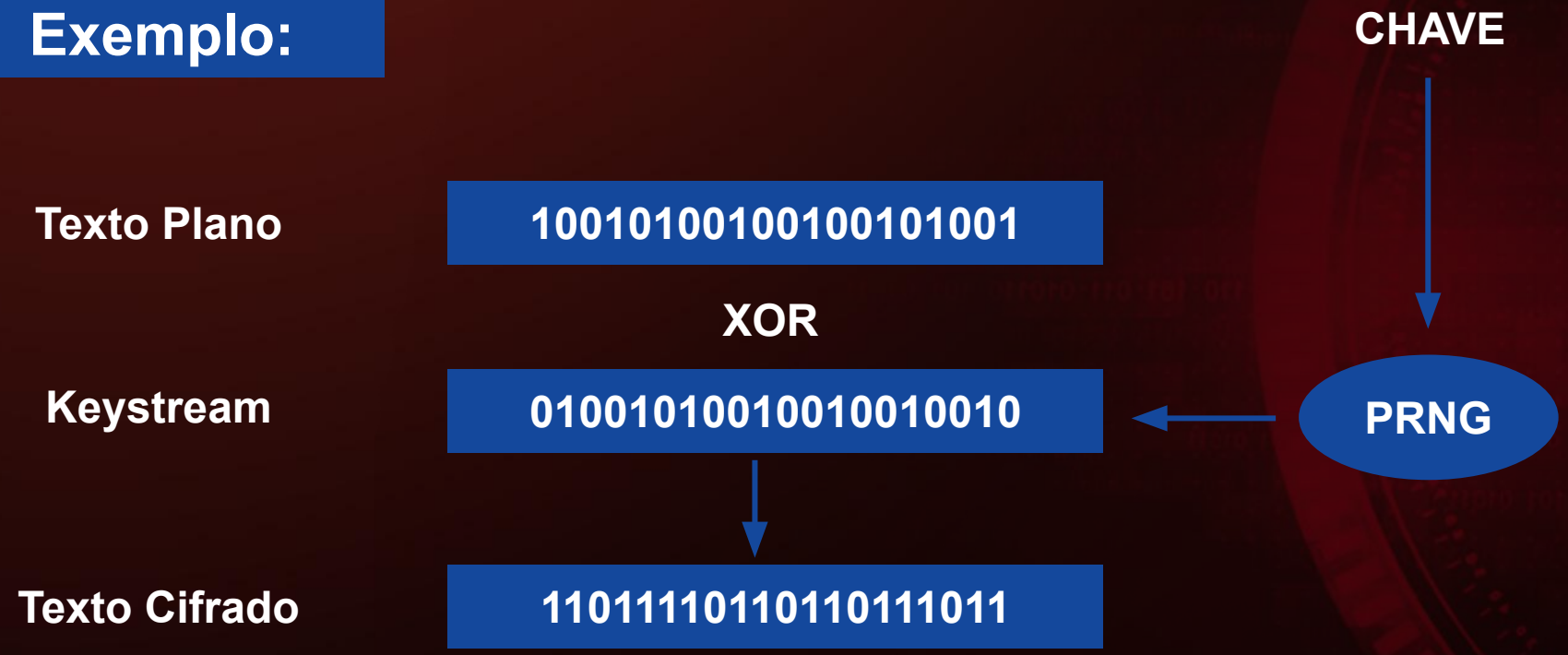
Cifras de Fluxo

- ✔ Vai combinar um a um os bits do texto plano com um fluxo de bits pseudoaleatório
- ✔ Cada dígito de uma mensagem vai ser encriptado combinado com um dígito do fluxo de bits pseudoaleatório
- ✔ É usado XOR para realizar essa combinação
- ✔ A cifra de fluxo vai usar uma chave de tamanho menor para gerar esse stream (64 ou 128 bits)
- ✔ Então, a chave vai ser usada para gerar um keystream pseudoaleatório que vai ser combinado com o texto plano para gerar o texto cifrado.

CIFRAS SIMÉTRICAS

Cifras de Fluxo

Exemplo:



CIFRAS SIMÉTRICAS

Cifras de Bloco

Ocorre sobre bloco de dados

- ✔ A mensagem/texto plano é dividida em blocos pelo algoritmo
- ✔ Algoritmo opera sobre cada bloco de forma independente

CIFRAS SIMÉTRICAS

Cifras de Bloco

Problema

- ✔ Um mesmo bloco de texto pode se repetir e quando o algoritmo divide sua mensagem em blocos, pode haver blocos iguais → texto cifrado será igual

Gera um padrão de repetição que vai ser identificado pelo invasor

Solução

Realimentação

- ✔ Evitar a repetição de bloco

CIFRAS SIMÉTRICAS

Cifras de Bloco

Modo de Realização – CBC (*Cipher Block Chaining*)

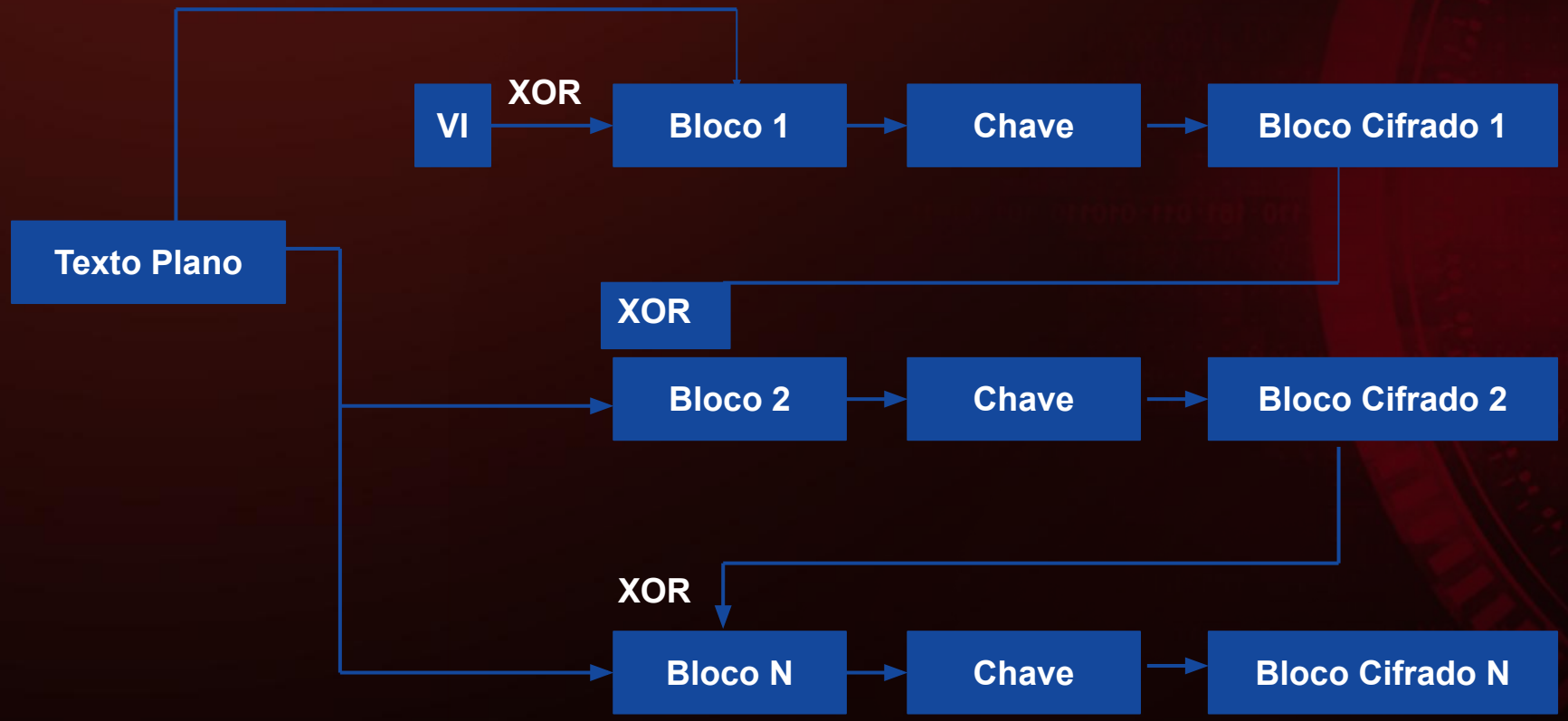
Funcionamento

- ✔ XOR no bloco atual do texto plano/aberto com o bloco anterior do texto cifrado
- ✔ Como o primeiro bloco não tem um bloco anterior, faz-se um XOR com um vetor de inicialização
- ✔ Vetor de inicialização é uma entrada (valor de tamanho fixo, sendo um número pseudoaleatório)
- ✔ Usado para aumentar o nível de segurança da criptografia de bloco

CIFRAS SIMÉTRICAS

Cifras de Bloco

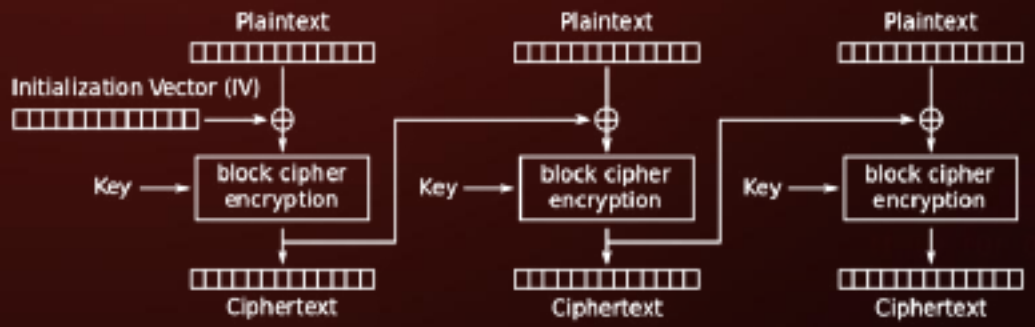
CBC (*Cipher Block Chaining*)



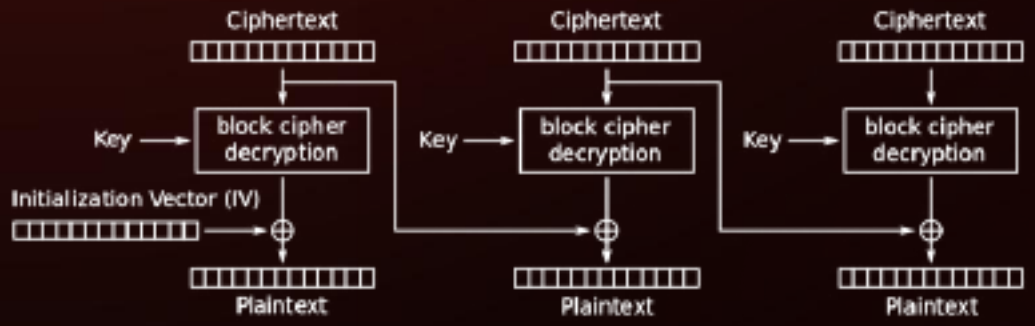
CIFRAS SIMÉTRICAS

Cifras de Bloco

CBC (*Cipher Block Chaining*)



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

CIFRAS SIMÉTRICAS

Cifras de Bloco

CBC (*Cipher Block Chaining*)

Exemplos de algoritmos

- ✔ RC6
- ✔ DES
- ✔ 3DES
- ✔ AES
- ✔ Rinjndael

CIFRAS SIMÉTRICAS

Cifras de Bloco

CBC (*Cipher Block Chaining*)

Algoritmos

DES (Data Encryption Standard)

- ✔ Bloco de textos simples (64 bits) sendo dividido em 2 partes antes do algoritmo principal de iniciar (baseado na estrutura de Fiestel)
- ✔ Tamanho de chave pequena
- ✔ 16 rodadas
- ✔ Lento se comparado ao AES

CIFRAS SIMÉTRICAS

Cifras de Bloco

CBC (*Cipher Block Chaining*)

Algoritmos

AES (Advanced Encryption Standard)

- ✔ Utiliza chaves criptográficas de 128. 192 e 256 bits para encriptar e decriptar dados em blocos de 128 bits (NIST – National Institute of Standards and Technology)
- ✔ Substituto do DES
- ✔ Tamanho de chave maior que o DES, o que sinaliza mais segurança
- ✔ Trabalha com o princípio de substituição e permutação
- ✔ Todo o bloco de dados é processado como uma única matriz

REFERÊNCIAS

1. https://cryptoid.com.br/criptografia/o-que-e-uma-cifra-de-bloco-e-como-ela-funciona-para-proteger-seus-dados/
2. Redes de Computadores e a Internet - 6ª Edição
3. Introdução à segurança de computadores - Michael T. Goodrich e Roberto Tamassia
4. https://www.gta.ufrj.br/grad/99_2/marcos/des.htm
5. https://www.gta.ufrj.br/grad/05_2/aes/
6. https://pt.living-in-belgium.com/difference-between-des-and-aes-152

SEGURANÇA DA INFORMAÇÃO

Cifras simétricas