SEGURANÇA DA INFORMAÇÃO

O que é criptografia?

ROTEIRO

- Introdução à criptografia
- Termos comuns
- Comunicação segura
- Tipos de criptografia

INTRODUÇÃO À CRIPTOGRAFIA

No contexto de tecnologia da informação, a criptografia é importante para garantir a segurança e o sigilo de informações em todo o ambiente computacional.

A palavra é derivada do grego “escrita oculta” sendo o estudo das técnicas de ocultação de informações.

INTRODUÇÃO À CRIPTOGRAFIA

Muitos são os cálculos e manipulações realizadas a cada operação de codificação e decodificação da informação.

A natureza segura de técnicas de criptografia está atrelada à computabilidade dos algoritmos aplicados.

Criptologia, Criptografia e Criptoanálise

- ✔ **Criptologia** é uma área de estudo que envolve a criptografia e criptoanálise
- ✔ **Criptografia** → oculta informações
- ✔ **Criptoanálise** → objetiva quebrar técnicas utilizadas e tentar obter informações a partir dos dados codificados, mas sem acesso aos segredos requisitados pela decodificação normal

INTRODUÇÃO À CRIPTOGRAFIA

Mas desde quando existe a criptografia?

- ✔ Há registro de quase 3 mil anos

Espartanos e Romanos fizeram uso da criptografia em suas trocas de mensagens

Divisão: Criptografia Clássica x Criptografia Moderna

Criptografia Clássica

- ✔ Povos antigos, idade média até máquinas eletromecânicas (usadas em guerras)
- ✔ Exemplos de cifras clássicas: Scytale, Cifra de César, Cifra de Vigenère

INTRODUÇÃO À CRIPTOGRAFIA

Criptografia Moderna

- ✔ Início a partir da Segunda Guerra Mundial
- ✔ Claude Shannon – Pai da Criptografia Matmática
  - *Communication Theory of Secrecy Systems*
  - *Mathematical Theory of Communication*

1970 – Avanços com a criação de um padrão

- ✔ Publicação do projeto DES

1976 – Chaves públicas e criptografia assimétrica

2001 – Substituição do DES pelo AES

INTRODUÇÃO À CRIPTOGRAFIA

Termos Comuns

Texto plano:

- ✔ Informação legível – pode ser compreendida por quem tem acesso

Texto cifrado:

- ✔ Informação que não pode se compreendida por aqueles que não possuem acesso

Cifrar:

- ✔ Utilizar um segredo para transformar um texto claro em um texto cifrado – *quem souber o segredo correto pode reverter o processo*

INTRODUÇÃO À CRIPTOGRAFIA

Termos Comuns

Algoritmo:

- ✔ Sequência de operações realizadas sobre um conjunto de dados de entrada para gerar uma saída correspondente

Cifra:

- ✔ Algoritmo usado para criptografar ou descriptografar dados

INTRODUÇÃO À CRIPTOGRAFIA

Usos da criptografia

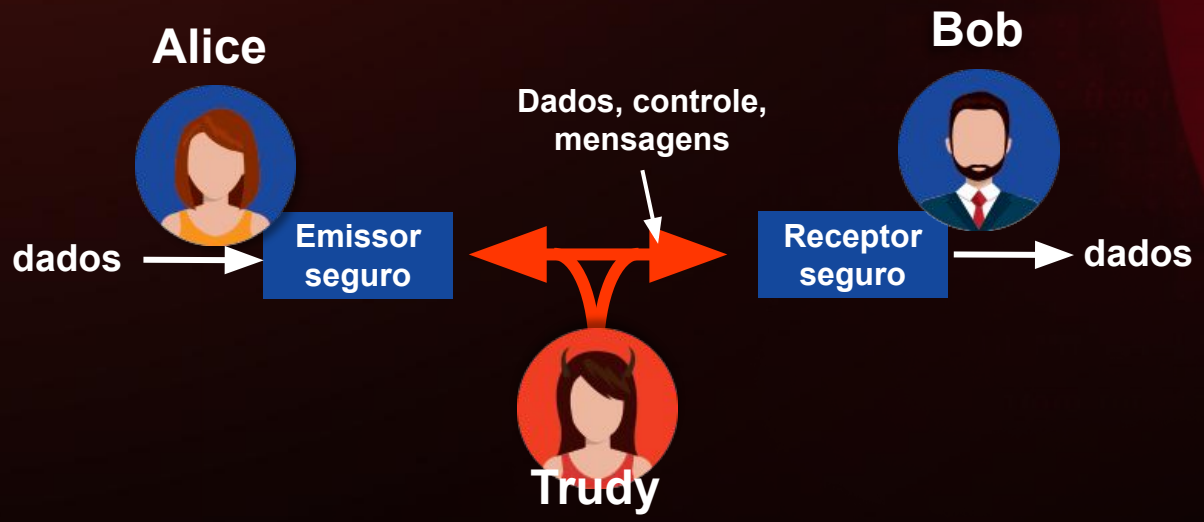
- ✔ *Proteção de dispositivos*
- ✔ *Mensagens de WhatsApp*
- ✔ *VPNs*
- ✔ *Para provar a integridade e autenticidade das informações*
- ✔ *Proteção dos e-mails com protocolos como o OpenPGP*
- ✔ *Etc.*

COMUNICAÇÃO SEGURA

Dois personagens desejam se comunicar

Bob e Alice são conhecidos no universo de Redes de Computadores

Mas temos a Trudy, uma intrusa que pode: interceptar, apagar e modificar as mensagens trocadas entre Bob e Alice



COMUNICAÇÃO SEGURA

Quem poderia ser Bob e Alice no exemplo anterior?

- ✔ Servidores DNS
- ✔ Bancos on-line
- ✔ Roteadores fazendo atualizações de tabelas de rotas
- ✔ Servidores de aplicação
- ✔ Servidores Web
- ✔ Proxies
- ✔ Usuários de serviços implantados em alguma nuvem computacional

COMUNICAÇÃO SEGURA

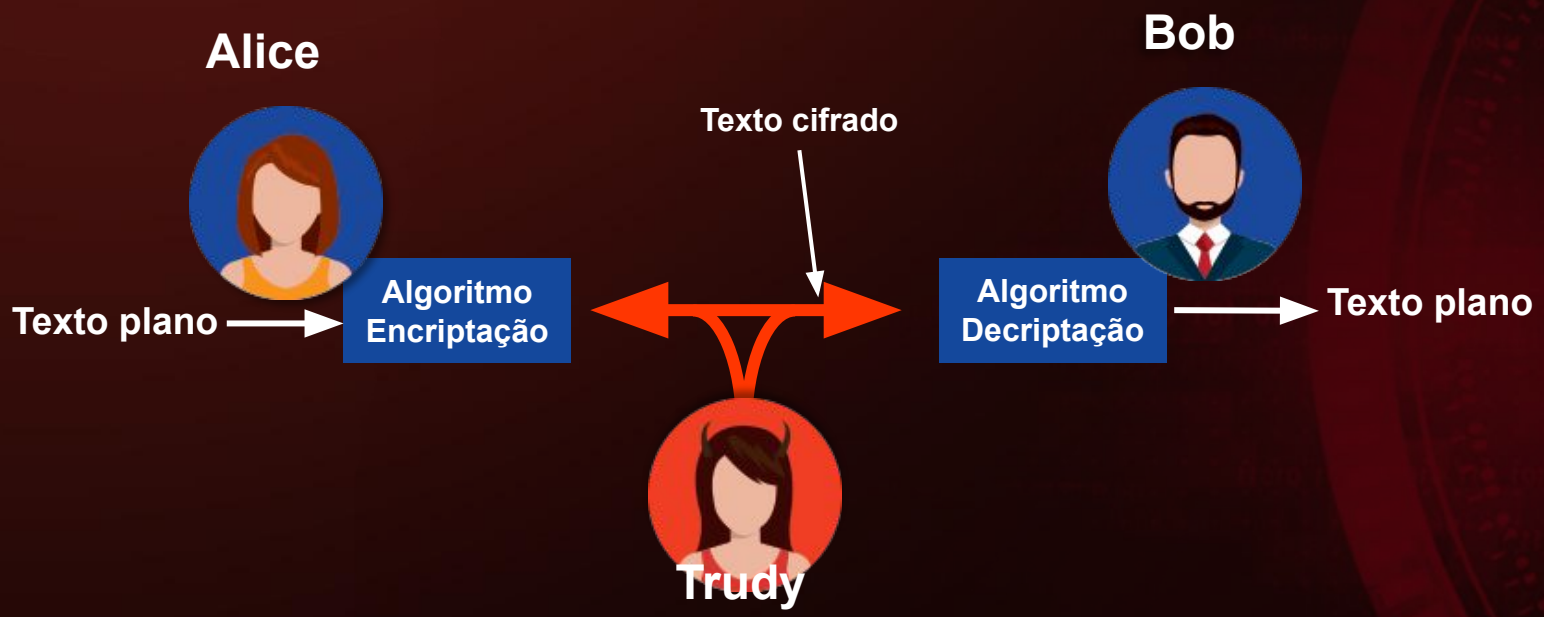
Como discutimos na semana anterior, quando ocorre comunicação entre duas partes alguma vulnerabilidade pode existir e isso pode ser explorado por intrusos

O que um intruso pode fazer?

- ✔ **Interceptar** mensagens
- ✔ **Inserir** mensagens na conexão entre as partes
- ✔ **Falsificar** o endereço de origem no pacote/datagrama ou qualquer campo neste datagrama
- ✔ **Sequestro da conexão**, removendo o transmissor ou receptor e se passar por um deles
- ✔ **Negar serviço**, ou seja, impedir que determinado serviço seja utilizado pelos outros

COMUNICAÇÃO SEGURA

Linguagem básica de criptografia



$m \rightarrow$ mensagem em texto plano

$K_A(m)$ texto cifrado encriptado com a chave K_A

$m = K_B(K_A(m)) \rightarrow$ mensagem original obtida com a decriptação

REFERÊNCIAS

https://cryptoid.com.br/criptografia/o-que-e-uma-cifra-de-bloco-e-como-ela-funciona-para-proteger-seus-dados/

Redes de Computadores e a Internet - 6ª Edição

Introdução à segurança de computadores - Michael T. Goodrich e Roberto Tamassia

SEGURANÇA DA INFORMAÇÃO

O que é criptografia?