UPF

Conhecimento é a nossa natureza

CCC306 - CIBERSEGURANÇA

Aula II: Introdução à Criptografia

Prof. Leonardo Costella

Objetivos da aula

- Explicar os princípios criptográficos básicos
- Explicar os fundamentos da criptografia
- Descrever as cifras mais comuns em uso atualmente
- Discutir o uso da criptografia em diferentes cenários

Objetivos da aula

Origem da palavra:

- **Cryptos**: escondido, oculto
- **Graphos**: escrita

Não confundir com esteganografia

Conceitos básicos

Elementos básicos:

- **Texto aberto:** informação a codificar (x)
- **Texto cifrado:** informação codificada (x 0)
- **Chave**: informação complementar secreta (k)
- **Cifrar**: transformar o texto aberto em cifrado (x k $\longrightarrow$ x 0)
- **Decifrar**: transformar o texto cifrado em aberto (x 0 k $\longrightarrow$ x)
- **Cifrador**: mecanismo para cifrar/decifrar a informação

Conceitos básicos

Criptografia é a prática de proteger informações por meio do uso de algoritmos codificados, hashes e assinaturas. As informações podem estar:

- **em repouso**: como um arquivo em um disco rígido
- **em trânsito**: como comunicação eletrônica trocada entre duas ou mais partes
- **em uso:** durante a computação de dados

Introdução a criptografia

- **Confidencialidade**: disponibiliza as informações somente para usuários autorizados.
- **Integridade:** garante que as informações não tenham sido manipuladas.
- **Autenticação:** confirma a autenticidade das informações ou a identidade de um usuário.
- **Disponibilidade:** As informações precisam estar disponíveis para as pessoas, no momento certo em que precisarem,seguindo as regras de confidencialidade.
- **Não repúdio**: impede que um usuário negue compromissos ou ações anteriores.

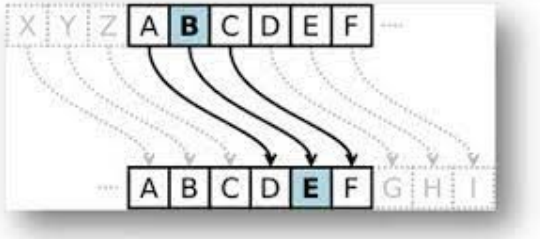
Introdução a criptografia

- **Confidencialidade**: disponibiliza as informações somente para usuários autorizados.
- **Integridade:** garante que as informações não tenham sido manipuladas.
- **Autenticação:** confirma a autenticidade das informações ou a identidade de um usuário.
- **Disponibilidade:** As informações precisam estar disponíveis para as pessoas, no momento certo em que precisarem,seguindo as regras de confidencialidade.
- **Não repúdio**: impede que um usuário negue compromissos ou ações anteriores.

História da Criptografia

- Cifra de César
  - Nomeada através de Júlio César, o general Romano que foi o principal responsável por transformar Roma em um império aproximadamente em 50 a.C.

  - Cifra de Substituição
    - Consistia originalmente em substituir cada letra da mensagem, pela letra N posições depois dela.



História da Criptografia

- Mensagem:
  - "ATAQUE AO AMANHECER"
- Deslocamento: 3 posições

- Texto CIFRADO:
  -

História da Criptografia

- Mensagem:
  - "ATAQUE AO AMANHECER"
- Deslocamento: 3 posições

- Texto CIFRADO:
  - DWDXHT DR DPDQKHFHU

História da Criptografia

- Cifra de Vigenère
  - A invenção da cifra de Vigenère é erradamente atribuída a Blaise de Vigenère encontra-se originalmente descrita por Giovan Battista Bellaso no seu livro datado de 1553 com o título La Cifra del Sig. Giovan Battista Bellaso.
  - Método de criptografia que usa uma série de diferentes cifras de César baseadas em letras de uma senha
  - Amplamente utilizada na guerra civil americana (1861 - 1865)
  - Serviu como base para a máquina Enigma

História da Criptografia

Mensagem:

ATACARBASENORTE

Chave:

FOGO

Chave estendida:

FOGOFOGOFOGOFOG

Texto cifrado:

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

História da Criptografia

Mensagem:

ATACARBASENORTE

Chave:

FOGO

Chave estendida:

FOGOFOGOFOGOFOG

Texto cifrado:

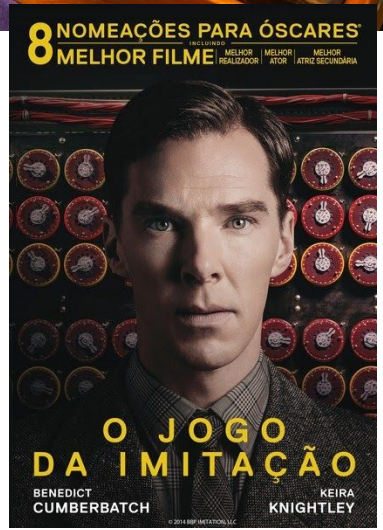
FHGQFWHOXSTCWHK

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

História da Criptografia

- Máquina Enigma
  - Máquina eletromecânica de criptografia com rotores. Utilizada tanto para criptografar como para descriptografar códigos de guerra

  - Amplamente utilizada pelo exército Alemão
    - Retratada no filme **O Jogo da Imitação**



  - **Simulador: [Enigma Simulator]**

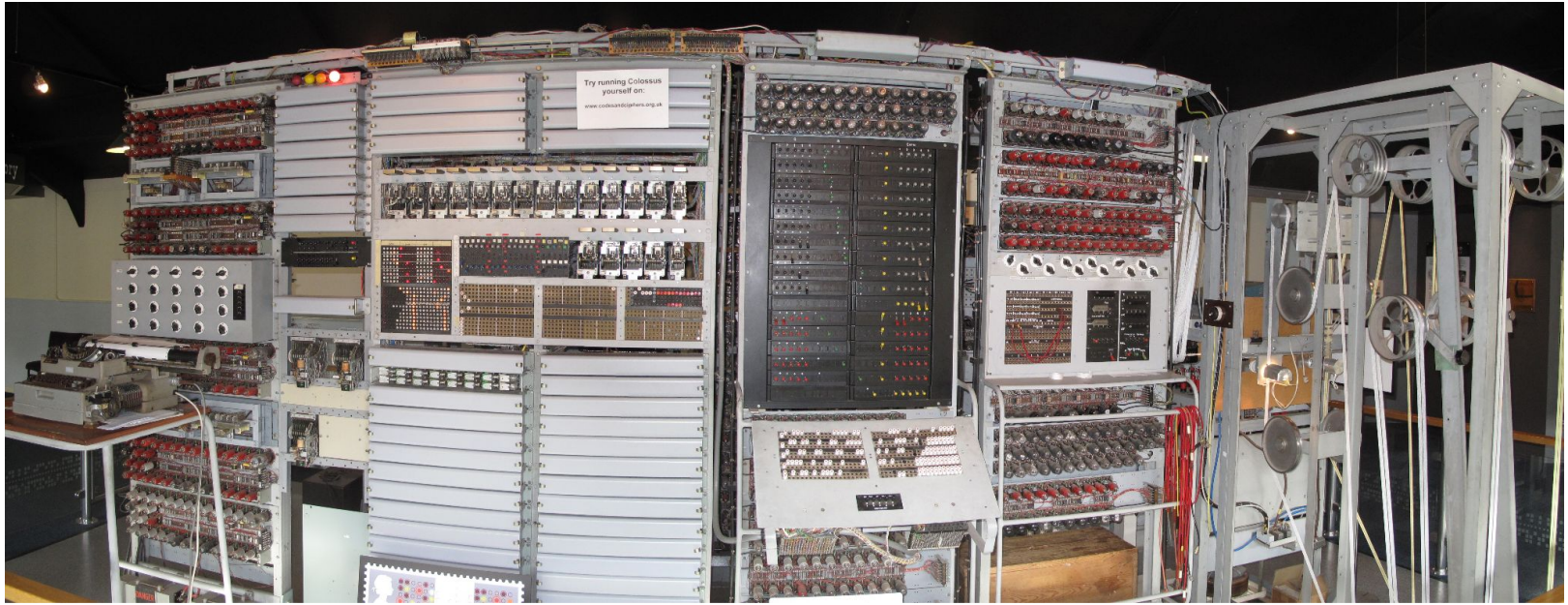
Criptoanálise

- Tentar descobrir o texto cifrado e/ou a lógica utilizada em sua encriptação
- Criptoanalistas
- Durante a 2ª Guerra Mundial 30,000 pessoas na Grã-Bretanha realizavam tal trabalho.

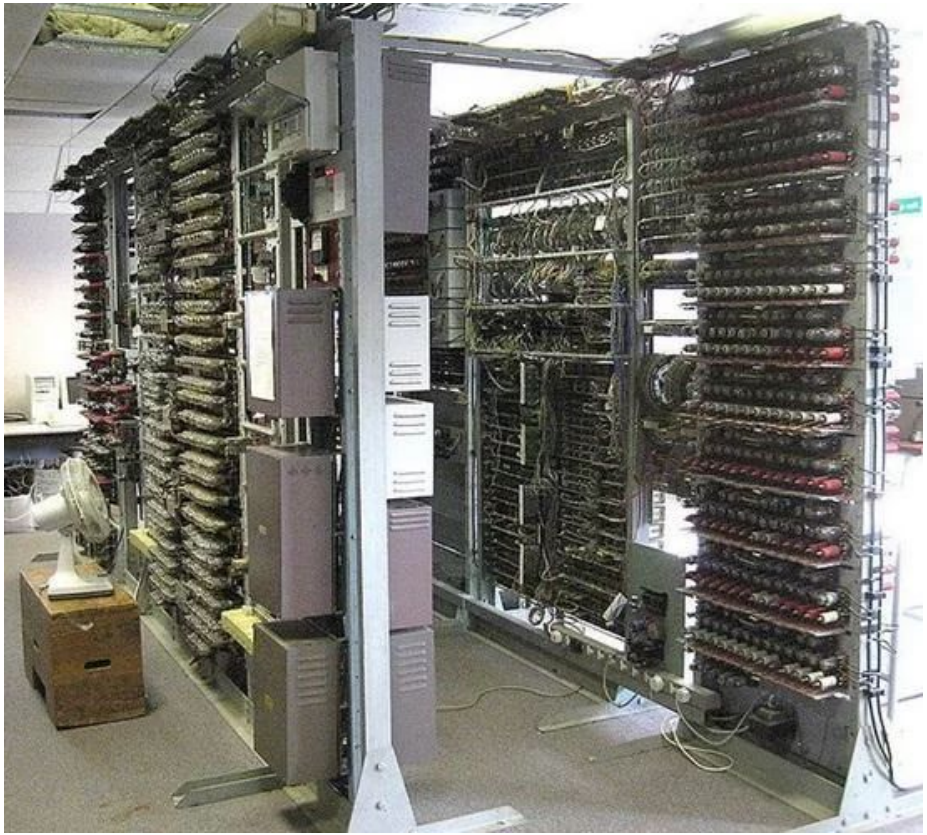
Criptografia e Computadores

Em 1943, influenciado pelo trabalho de Turing, o matemático e criptoanalista **Max Newman**, desenvolveu o Colossus, o primeiro computador eletrônico, digital e programável do mundo.

Criptografia e Computadores - Colossus



Criptografia e Computadores - Colossus



Criptografia

Criptografia e Computadores

- O emprego de computadores e evolução na capacidade de processamento fez com que se tornasse necessário evoluir constantemente os método de criptografia empregados.

- Há algumas décadas atrás um criptoanalista levaria dez dias para criptografar uma página criptografada
  - Com um computador de processador 386 de 33MHz levaria apenas 2h
  - Com um Core i7 de mais de 3GHz, alguns poucos segundos

- O aumento no poder de processamento combinado as reduções nos custos, aumentou a ameaças de ataques.

Criptografia e Computadores

A criptografia moderna:

- se baseia em algoritmos públicos bem avaliados
- usa espaços de chaves MUITO grandes
- torna inviável a análise exaustiva

Exemplo:

- O espaço de chaves do cifrador de César é 26 (alfabeto)
- AES com chaves de 128 bits: 2^{128} chaves possíveis: 340.282.366.920.938.463.463.374.607.431.768.211.456
  - Testando um bilhão (10^9) de chaves por segundo, precisaremos de **10 sextilhões de anos** para testar todas as chaves!

Criptografia e Computadores

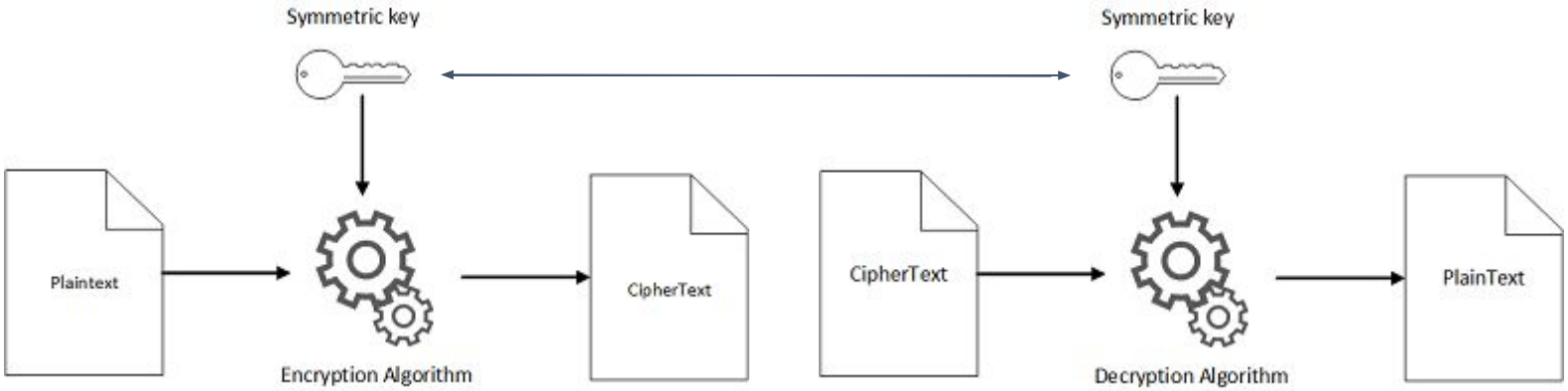
O segredo de uma técnica de criptografia não está no algoritmo em si, mas no espaço de chaves***(Keyspace)*** que ele provê. **Auguste Kerckhoffs**, famoso criptógrafo, nascido na Holanda, no século 19 elaborou a **doutrina de Kerckhoffs**, que diz:

“um sistema de criptografia deve ser seguro ainda que o adversário conheça todos os detalhes do sistema, com exceção da chave secreta”

Tipos de Criptografia

- **Chave simétrica:**
  - Mesmas chaves tanto para a encriptação quanto para a desencriptação
  - Requer que todos os destinatários da mensagem tenham acesso a uma chave compartilhada
- **Chave assimétrica (chave pública)**
  - Usa pares de chaves
    - chaves públicas, que podem ser compartilhadas - **Criptografar**
    - chaves privadas, conhecidas apenas pelo proprietário - **Decodificar**
    - **Chaves ligadas**
- **Híbrida**
  - Unir a segurança da criptografia assimétrica com a velocidade de processamento da simétrica.
    - Chaves públicas, chaves privadas e chaves de sessão

Algoritmos de Chave Simétrica



Algoritmos de Chave Simétrica

Alguns exemplos:

- **AES***(Advance Encryption Standard)*:
  - Cifra simétrica de bloco de chaves
  - Usa chaves de 128, 192 e 256 bits
  - Padrão de segurança do governo americano (2002)
  - Muito utilizada na internet e em cifragem de disco
- **DES:** *(Data Encryption Standard)*:
  - Usa chaves de 56 bits
  - Criado pela IBM em 1970
  - **3DES ou triplo DES**, realiza o processo de cifragem DES 3 vezes (168 bits)
- **Blowfish**:
  - cifra simétrica de blocos
  - Publicada em 1993 por Bruce Schneier com o intuito de substituir o DES
  - Chave variável de 32 a 448 bits
  - tem sua licença grátis e está a disposição para todos.

Algoritmos de Chave Simétrica

Tipos de algoritmos simétricos, quanto a estratégia de cifragem:

- Cifradores de **substituição**
- Cifradores de **transposição**

Tipos de algoritmos simétricos, quanto ao agrupamento dos dados:

- Cifradores de **fluxo**
- Cifradores de **bloco**

Algoritmos de Chave Simétrica

Cifradores de Substituição: Usados para substituir cada letra ou símbolo da mensagem original por outro, seguindo uma regra fixa.

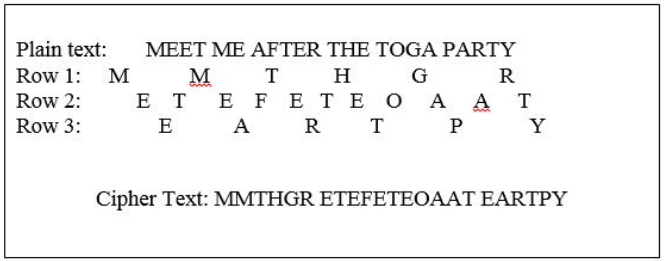
- **Exemplo:** Se "A" for substituído por "D", "B" por "E" e assim por diante, temos um deslocamento fixo.
- **Vantagem**: Simples de implementar
- **Desvantagem**: Fácil de quebrar por análise de frequência de letras.

Cifra de César e Cifra de Vigenère são alguns dos exemplos

Algoritmos de Chave Simétrica

Cifradores de Transposição: Partes da mensagem são trocados entre si usando regras

- **Vantagem**: Mantém a mesma frequência de letras, tornando a análise de frequências ineficaz
- **Desvantagem**: Pode ser quebrado se padrões de transposição forem descobertos
- **Exemplo:**



O Algoritmo **Rail Fence** utiliza essa técnica

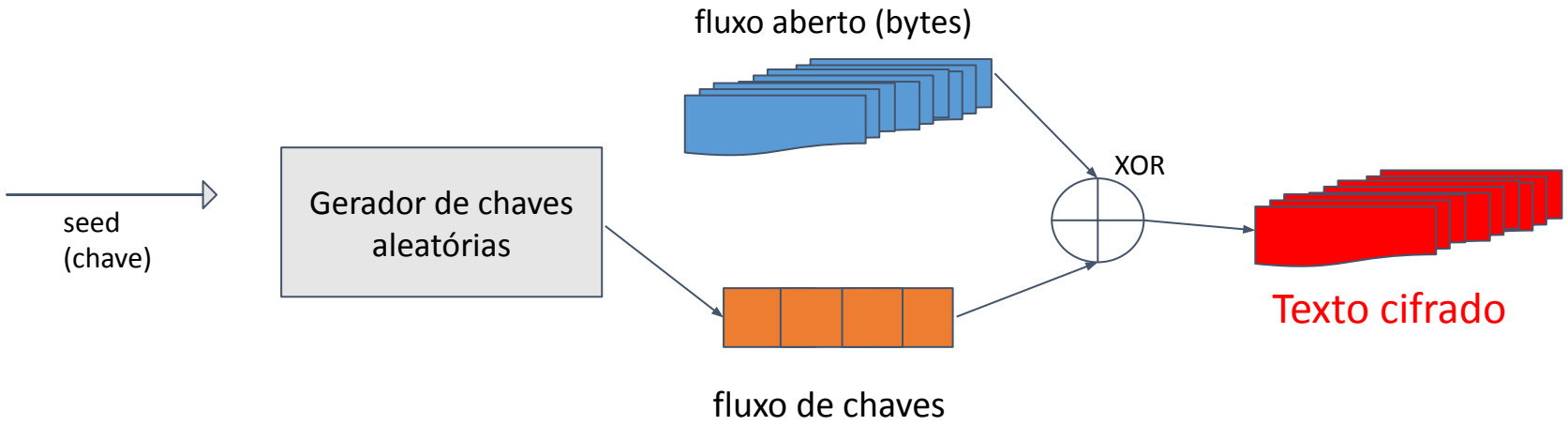
Algoritmos de Chave Simétrica

Cifradores de Fluxo:

- Cifram os dados byte a byte, em sequência
- Importantes para multimídia, VoIP…
- Chave produzida por gerador pseudo-aleatório
- Conceito de chave de um só uso (One-Time Pad
- **Exemplos**: RC4, A5/1
- **Vantagem:** Rápidos e eficientes para transmissão contínua de dados.
- **Desvantagem:** Se a chave ou o fluxo forem previsíveis, o sistema é comprometido.

Algoritmos de Chave Simétrica

Cifradores de Fluxo:



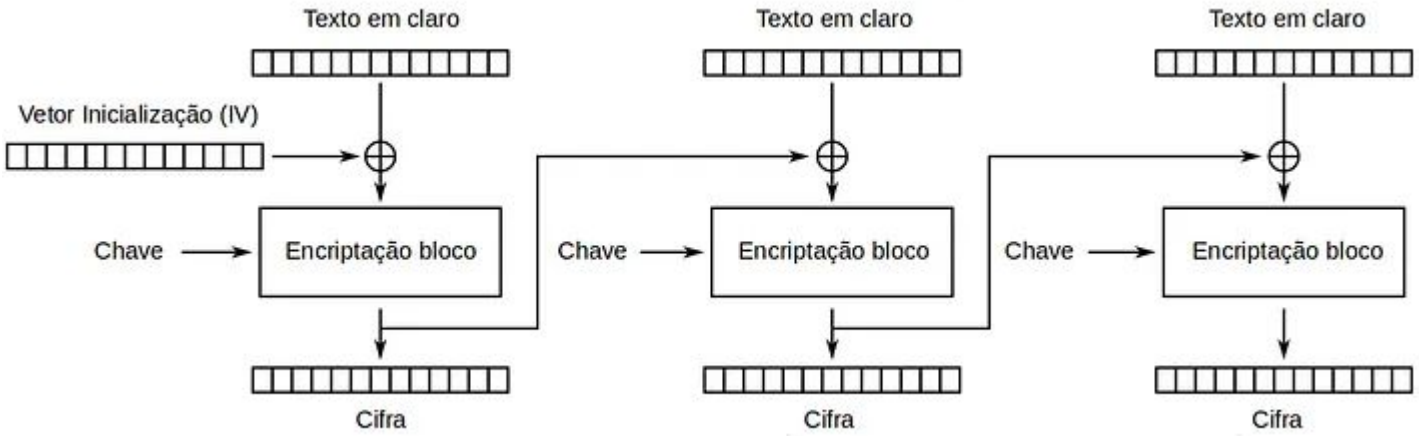
Algoritmos de Chave Simétrica

Cifradores de Bloco:

- Cifram os dados em blocos de mesmo tamanho: entre 64 e 128 bits
- Cada bloco é processado com a mesma chave
- **Vantagem**: Segurança forte contra ataques de análise estatística
- **Desvantagem**: Pode ser lento para dados pequenos e exigir preenchimento (padding) para blocos incompletos.
- **Exemplo**: DES, AES, Blowfish

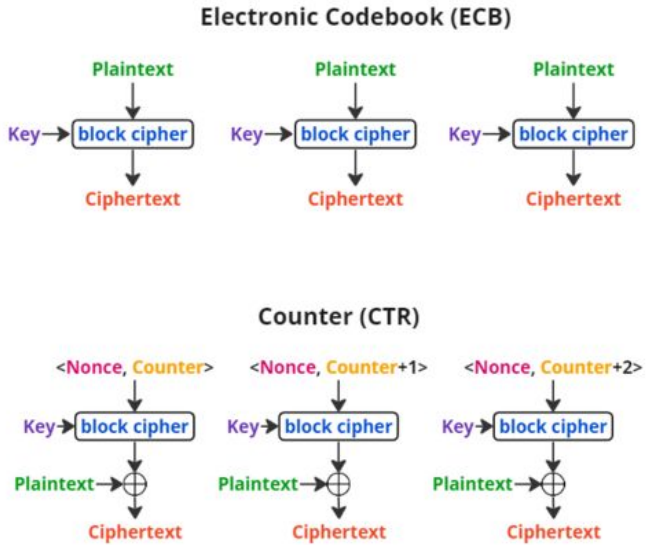
Algoritmo de Chave Simétrica

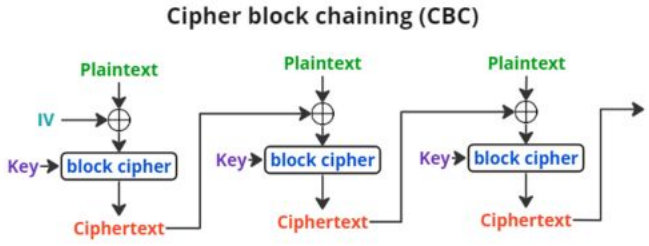
Cifradores de Bloco



Algoritmo de Chave Simétrica

Alguns exemplos de cifradores de bloco:





Algoritmo de Chave Simétrica

Características:

- São geralmente muito rápidos
- Usam chaves pequenas (80-256 bits)
- Muito usados na cifragem de dados arquivos em um disco pacotes de rede fluxos multimídia

Algoritmo de Chave Simétrica

Características:

- São geralmente muito rápidos
- Usam chaves pequenas (80-256 bits)
- Muito usados na cifragem de dados arquivos em um disco pacotes de rede fluxos multimídia

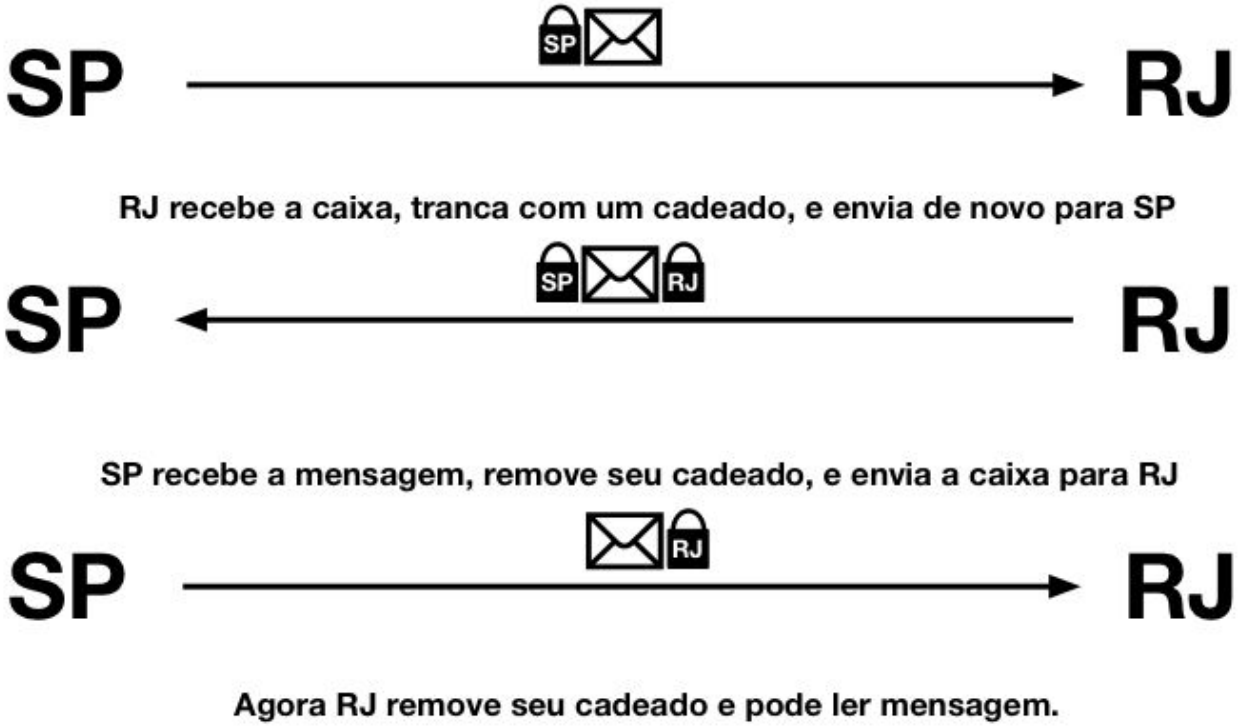
Problema: Como transmitir a chave????

Criptografia Simétrica

Problema do acordo de chaves:

- Alice e Bob querem trocar mensagens via rede
- As mensagens serão cifradas com um algoritmo simétrico
- Eles precisam definir uma chave comum
- Como definir a chave comum através da rede?

Criptografia assimétrica



Criptografia assimétrica

- Usam um par de chaves complementares:
  - Uma chave pública kp: conhecida por todos os usuários
  - Uma chave privada kv: conhecida só pelo proprietário
  - O que kp cifrar, kv decifra, e vice-versa (nem sempre!)

- **Estas chaves estão fortemente relacionadas**:
  - para cada kp há uma única kv correspondente
  - para cada kv há uma única kp correspondente
  - Não é possível calcular uma chave a partir da outra

Criptografia assimétrica

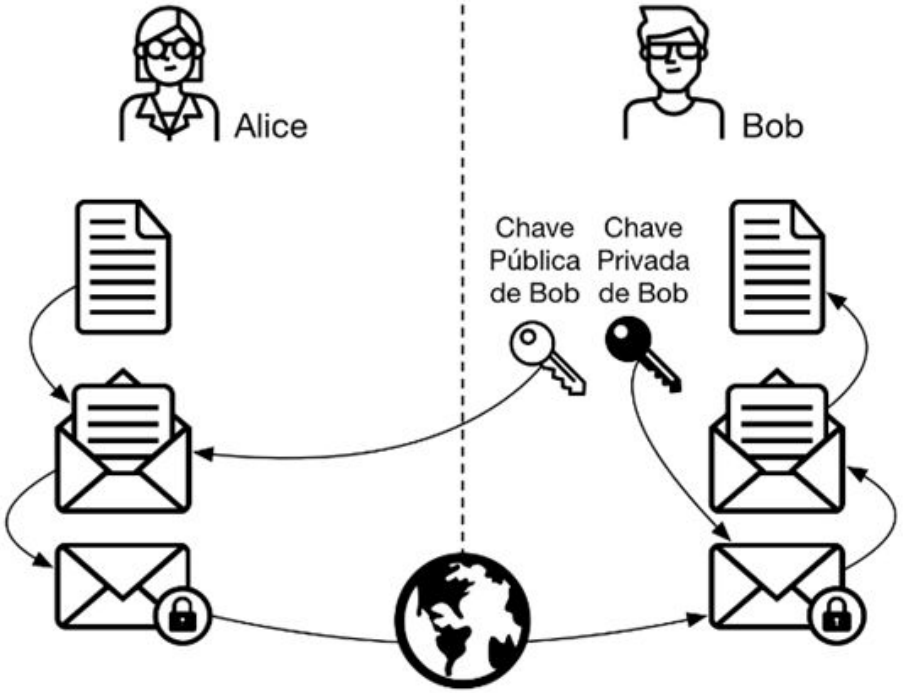
```
-----BEGIN RSA PRIVATE KEY-----
MIIEoAIBAAKCAQEAwlFZGDWv15Gwu2OJlT5/gJdFGGnX+YqnCh8NFtcUt7TXxJsP
/64DOWY6A8ebJEcFRAPuiypDC3f0XQJYd0EcwNCLXUCMjJwkVguvRX+CO7+cXnhu
MD9kYZ0Hl/33Cq5rMd26FNSK0wCgKE+fbqY1p5zFHXqgVGAvaEcrqvDkFV5nwOvK
E3w3SmHBLMDfI8hUBsK9ndMVaAnqnxjhW49K4sR2YYzoBiLgQXpLSefYzBPLRfyq
I/RczDD7RrxrBQAoqi7juRG6DwOUDQajK+k50otEMBALRjv9rMQa4ym8aS+NtxJo
s0jla7ZohSvvTPiJwnBxE6RW9cVHWKUaQkEvUQIDAQABAoIBAAW6eDHqg0CLnvYn
PQsVSJT14KeTlzZYDAyUVcJynL29qw60s4gKDTZH+TXbUIuFPHaA1ytrF4bjBmUn
iIwbc0mL3E/ncz1B7SBMP+KAm8o/H9D5I+ZwN/lYs7ybVAkQk0BpFO9ARMdroU0O
69hLNhG24Wi5ELjsDPm5/2OOrmqizKtJeJID6HGt10PeFQen3MAAkyEL8hvbXtte
mS514Jx/RwlcZixia8xjm8pB6nxz5OTc1cuRisnc44PWlaPorPxqSjF7bIa8jDbu
u9vkosIlPBnbSNbbsSdXI52cRizkxLGrFm9EacWVoRAd0Ml3bUST033A2BPzsjBm
TeG/2AECgYEA1qfe33B/rT6mPqv1MZ0vOLjEU8XJEUN1MFxFLhrDYw455JYYrsBX
dcebr8PBFuSJpq5r9tIAzKx+2ziiJx5TH4u8itZhRudRzV0F8akHAuDveE+7eN9H
HunrrcZ1bZqcO2OzqKkS09HHuyDrC9HJhM6KZ2PXTbNmnGle0sLLlXECgYEA576p
01Lj1Rk10cejzq/SS43zZes+EfMX0CipwWxiBkG9g2ZLeU0i2FkWPGcvI6T4vSNC
9xv6JBQT/xj0cBepNPdSM0jE2sC6ZTuJmU/vpNHO6SXYMJgtlK+50sbbBxlyx6ra
OzkBdYKw2BeMj9VCRI39WYK0aZ4X5CoKnVqox+ECf1w7xYg8zp+iS8yiFrk60Q+O
VM2qLrs8QR6GhzNITKxDcJzH4dM00l/JZRwhANbVXFBCoiFsGuvXMqr/qq0kWpMz
d9AwTZwpyPx0/BjaiCi0fjE0EVnelrCx0pLYs5xk0ryyGoBeJbjeavP9MQHjIrPu
C4phXCIG9BBBNn1ZNiECgYA2tsQ/fQR/fnk/cyQQm2BKKFSL/pNkB4Hayo7xtNYb
5g+JY3B0Tiro63edgTsW7k8v0JBx6TAQrpDeDJVBlcSEVdQZeZfIkfIwDnN5N+87
ebGhSCcXqgYw8aAszHhP381CrOrjSp02kkmQa1brao0/xEpJhNt1iDbZzrc82Xe5
4QKBgB4BlAfigLKp9JWHfN8Cg9BA/gZ7b1hRJ9VGBH6oz9Eka/K1xycVomeyWDoT
Xym9otxVWYm9NAVIYSoGuKQUDZZni8xa4XvGCY+aoKxNwvznhWwO+X1t4RIIgaoZ
ghA2Cp63ylEs2xSwX1kZTkj92ZOK2Ls/w21xgRhUB3V/fOo+
-----END RSA PRIVATE KEY-----
```

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAiwRgoCzQrVOLDzlm4arF
4Pw1L4QrAzyo3in+KaI3J6/mbZ2Dl3W7wGF1qzJRWqRFZ9Tgo3SJs+Pypkm1k1v0
OuRcSZxEwOdO5QZ46pQFi9y5w36ci+7FfAp1c88gARuCcn7dxc3rJHN8yn5ab9DA
NPtXRDtbjJox219Lo6phrCA9yPQAPd+7sjf3PzxYs2xDXsuR62pfbrJ9adJM8DAY
+gxvqC6SAPlFMxRBh6K4Iawos+q0u/p30lbrN5dLJzbr+bKCE93Klr0w0f/P9KDl
QP/EEcI7b5SVjYnKGOBylAyB2SrFejRIBCYO+iiUGDMOIKZPjOC5aO+sRKJdKLjX
JwIDAQAB
-----END PUBLIC KEY-----
```

Criptografia assimétrica

Alice quer enviar um documento secreto a Bob

1. Bob compartilha sua chave pública com Alice
2. Alice usa a chave pública de Bob para cifrar o documento
3. Alice envia o documento cifrado a Bob
4. Bob usa sua chave privada para decifrar o documento



Outros usuários podem ler o texto cifrado mas não podem decifrá-lo

Chave assimétrica (chave pública)

- RSA:
  - Rivest-Shamir-Adleman – criadores do modelo
  - Um dos mais utilizados e seguros
  - Utiliza chaves baseadas em números primos.
    - Quanto maior o número, mais segura a chave é
  - As chaves pública e privada são geradas com base na multiplicação de dois números primos. O resultado desta multiplicação será público mas, se o número for grande o suficiente, fatorar este número para descobrir os primos que multiplicamos para formá-lo pode demorar anos.
    - Não é impossível quebrar a criptografia RSA, mas como para fazer isto seriam necessários alguns bons anos ou décadas, a ideia se torna inviável.
  - Por exemplo: Utilizando chaves de 2048 bits, teremos um número de **617 dígitos**

Criptografia de chave assimétrica RSA:

Exemplo didático (com números pequenos o que não é a realidade):

1. Sortear dois números primos
    - P = 17 e Q = 11
2. Calcular dois novos números N e Z de acordo com os escolhidos no passo 1
    - N = P * Q
        - N = 17 * 11 = **187**
    - Z = (P - 1) * (Q -1)
        - Z = 16 * 10 =**160**
3. Define-se um número D que tenha a propriedade de ser primo em relação à Z.
    - D = 7
      Obs: geralmente utilizado: 65537(0x010001)

Criptografia de chave assimétrica RSA:

Exemplo didático (com números pequenos o que não é a realidade):

4. Criação das chaves públicas e privadas
   - Encontrar um número E que: **E * D mod Z = 1**
     - E = 1 => (1 * 7) mod 160 = 7
     - E = 2 => (2 * 7) mod 160 = 14
     - E = 3 => (3 * 7) mod 160 = 21
     - **E = 23 => (23 * 7) mod 160 = 1**
     - **E = 183 => (183 * 7) mod 160 = 1**
     - **E = 343 => (343 * 7) mod 160 = 1**
     - **E = 503 => (503 * 7) mod 160 = 1**

5. **Passo 5: Escolher um dos números que satisfez o cálculo anterior**
   - **E = 23**
     - **Chave pública: E e N (23,187)**
     - **Chave privada: D e N (7,187)**

Criptografia de chave assimétrica RSA:

Exemplo didático (com números pequenos o que não é a realidade):

Chave pública: E e N (23,187)

Chave privada: D e N (7,187)

Para criptografar:

- TEXTO ORIGINAL = **19**
- TEXTO CRIPTOGRAFADO = **(19 ^ 23) mod 187**
- TEXTO CRIPTOGRAFADO = **257829627945307727248226067259 mod 187**
- TEXTO CRIPTOGRAFADO = **94**

Para desencriptar:

- TEXTO CRIPTOGRAFADO = **94**
- TEXTO ORIGINAL = **(94 ^ 7) mod 187**
- TEXTO ORIGINAL = **19**

```
print((19 ** 23) % 187)
print((94 ** 7) % 187)
```

Criptografia Simétrica x Assimétrica

Característica	Simétrico	**Assimétrico**
Chaves	Uma única chave	Chaves complementares para cifrar e decifrar
Tamanho da chave	Pequena (AES: 64 a 256 bits)	Grande (RSA: 2.048 a 15.360 bits)
Velocidade	Alta (centenas de MB/s)	Baixa (centenas de KB/s)
Uso	Grandes volumes de dados (tráfego de rede, arquivos, áudio, etc)	Pequenos volumes de dados (troca de chaves, assinaturas digitais)
Algoritmos	RC4, A/51, DES, 3DES, AES, Blowfish	Diie-Hellman, RSA, ElGamal, ECC

AES x RSA - Performance

- **Velocidade:**
  - AES: Extremamente rápido em comparação com algoritmos assimétricos. Isso ocorre porque AES opera em blocos de dados de tamanho fixo (128 bits, 192 bits ou 256 bits) e utiliza operações que são eficientes em hardware e software.
  - RSA: Significativamente mais lento que AES. Isso se deve à complexidade matemática das operações de chave pública/privada, que envolvem exponenciação modular e operações com números grandes.

AES x RSA - Performance

- **Uso de Recursos:**
  - **AES:** Eficiente em termos de recursos, sendo adequado para dispositivos com poder de processamento limitado, como smartphones e dispositivos IoT.
  - **RSA:** Exige muito mais poder de processamento, especialmente à medida que o tamanho das chaves aumenta. A geração de chaves, em particular, pode ser muito demorada.

AES x RSA - Performance

- **Uso de Recursos:**
  - **AES:** Eficiente em termos de recursos, sendo adequado para dispositivos com poder de processamento limitado, como smartphones e dispositivos IoT.
  - **RSA:** Exige muito mais poder de processamento, especialmente à medida que o tamanho das chaves aumenta. A geração de chaves, em particular, pode ser muito demorada.

AES x RSA - Fator de Segurança

- **Segurança vs. Performance:**
  - **AES:** Oferece segurança confiável, com comprimentos de chave de 128, 192 ou 256 bits. A força da criptografia AES depende principalmente do tamanho da chave, sendo que chaves mais longas proporcionam maior segurança.
    - Ideal para criptografar grandes volumes de dados
  - **RSA:** Também se baseia no comprimento da chave, com chaves mais longas proporcionando melhor proteção. O RSA é seguro, desde que as chaves sejam selecionadas adequadamente. Os comprimentos ideais de chave variam de 2048 e 4096 bits.
    - Menos eficiente para criptografar grandes volumes de dados, mas é crucial para operações como a troca segura de chaves.

AES x RSA - Casos de uso

- **AES:**
  - Criptografia de dados em repouso. O AES criptografa dados confidenciais armazenados em dispositivos ou servidores. Por exemplo, quando você bloqueia seu smartphone com uma senha.

  - Comunicação segura em sistemas fechados. Em sistemas fechados, como aplicativos de mensagens e redes privadas virtuais (VPNs), o AES garante a confidencialidade da comunicação entre os usuários.

  - Criptografia de arquivos e discos. Muitos softwares e sistemas operacionais usam a criptografia AES para proteger arquivos e unidades de disco.

AES x RSA - Casos de uso

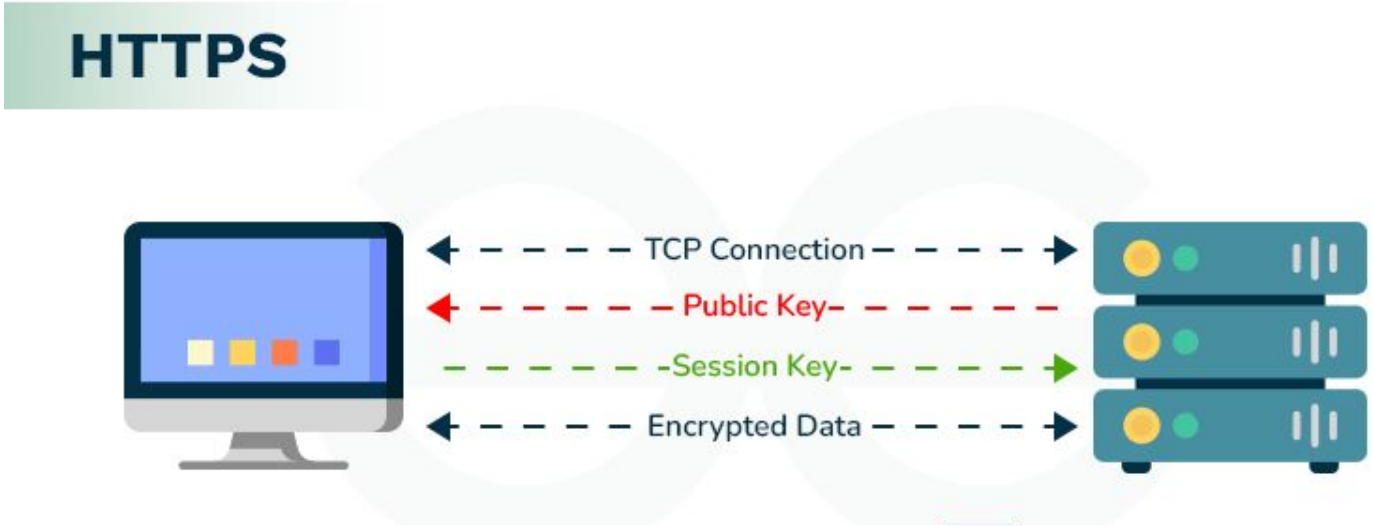
- **RSA:**
  - Comunicação segura pela Internet. O protocolo T*ransport Layer Security* (anteriormente *Secure Sockets Layer*) usa RSA para proteger a comunicação de dados confidenciais em trânsito entre navegadores e servidores da Web. Por exemplo, o ícone de cadeado no navegador da Web indica que a criptografia RSA protege seus dados durante as transações on-line e a navegação segura na Web.

  - Assinaturas digitais e troca de chaves. O RSA é usado para criar assinaturas digitais, que verificam a autenticidade e a integridade de documentos digitais. Por exemplo, as empresas usam certificados SSL de e-mail para proteger as comunicações corporativas e a documentação legal.

Criptografia Simétrica e Assimétrica juntas?

Devido à diferença de performance, em muitas aplicações práticas, os dois tipos de criptografia são usados em conjunto. Por exemplo, em uma conexão segura (como HTTPS), o RSA é usado para trocar uma chave AES, e então essa chave AES é usada para criptografar o restante da comunicação.

Criptografia híbrida



Referências Bibliográficas

- SILVA, Michel Bernardo Fernandes da. Cibersegurança: uma visão panorâmica sobre a segurança da informação na internet. Rio de Janeiro: Freitas Bastos, 2023. E-book. Disponível em: https://plataforma.bvirtual.com.br.

- Pfleeger, C. P., & Pfleeger, S. L. (2015). Security in Computing (5th ed.). Pearson.

- BARRETO, Jeanine S.; ZANIN, Aline; MORAIS, Izabelly S.; et al. Fundamentos de segurança da informação. Porto Alegre: SAGAH, 2018. E-book. p.2. ISBN 9788595025875. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788595025875/