



Insper

Tecnologias Hacker

Aula - Introdução a Criptografia

Insper

Tecnologias Hacker

Aula – Introdução a Criptografia

Prof. Dr. Rodolfo Avelino

Prof. João Eduardo Luisi

Objetivos da aula

Introdução a criptografia

Objetivos da criptografia computacional

Criptografia simétrica e assimétrica

Aplicações práticas

A criptografia consiste na ciência (e arte) da transformação de texto simples em texto ilegível, de tal modo que apenas quem saiba qual o processo de reverter a transformação possa recuperar o texto original

F hwnuytlwfkfnf fozif f rfsyju f nsyjlwnifij itx ifitx.

Contextualização

História da criptografia

Império romano – Cifra de César

Era medieval – Cifra de Vigenère

Segunda guerra mundial – Máquina de enigma e a quebra de sua cifra, ajudando os Aliados a vencer a guerra.

Era moderna – Curvas elípticas e computação quântica

Encriptação é o processo de cifrar ou seconder a informação

Decriptação é o processo de converter dados encriptados de volta a sua forma original

Alguns exemplos da criptografia na computação:

- Sistemas de arquivos (HD)
- Mensagens de e-mails
- Conexão WEB Segura
- Mensagens instantâneas

Por que a criptografia é essencial?

Proteção de dados em trânsito e em repouso;

Segurança de comunicações (WhatsApp, Signal, TLS/SSL);

Armazenamento seguro (banco de dados, senhas);

Blockchain e criptomoedas;

Casos reais

Vazamento de dados por falta de criptografia

Equifax (2017) – Vulnerabilidade em um servidor de código aberto

Yahoo (2012/2014) – 3 bilhões de usuários afetados

LinkedIn (2016) – 167 milhões de credenciais

Impacto das regulamentações (LGPD, GDPR, PCI-DSS, HIPAA)

Essas regulamentações exigem que empresas e organizações adotem medidas de segurança para proteger dados pessoais, financeiros ou de saúde, e a criptografia é uma das soluções mais importantes para cumprir esses requisitos.

Objetivos principais da Criptografia

Confidencialidade – Só o destinatário autorizado deve ser capaz de extrair o conteúdo da mensagem em sua forma cifrada.

Integridade – O destinatário deverá ser capaz de determinar se a mensagem foi alterada durante a transmissão

Autenticação do remetente – deverá ser capaz de identificar o remetente e verificar que foi ele mesmo quem enviou a mensagem

Não-repúdio ou irretratabilidade do remetente – não deverá ser possível ao remetente negar o envio da mensagem

Criptografia Simétrica

Criptografia simétrica

É um método de cifragem de dados em que a mesma chave é utilizada tanto para criptografar quanto para descriptografar uma mensagem. Em outras palavras, a informação é “embaralhada” usando uma chave secreta e só pode ser restaurada à forma original se essa mesma chave for fornecida. Por isso, o termo “simétrica”: a chave de cifra e de decifra é a mesma.

Como funciona?

1. **Geração ou escolha da chave** – o participante ou sistema gera uma chave aleatória;
2. **Criptografia (embaralhar texto)** – operações matemáticas para tornar a mensagem ilegível para quem não possuir a chave;
3. **Transmissão e/ou armazenamento** – o texto é enviado pela rede ou armazenado em algum lugar (disco, banco de dados, pen drive);
4. **Descriptografia** – o algoritmo faz o processo inverso usando a mesma chave que foi usada para cifrar a mensagem inicial.

Cifragem por substituição

Neste tipo de cifra, troca-se cada letra ou grupo de letras da mensagem de acordo com uma tabela de substituição. O receptor inverte a substituição e obtém o texto original.

Existem 4 tipos de substituição na criptografia clássica:

Cifra simples ou monoalfabética;

Cifra de substituição homofônica;

Cifra de substituição poligrâmica;

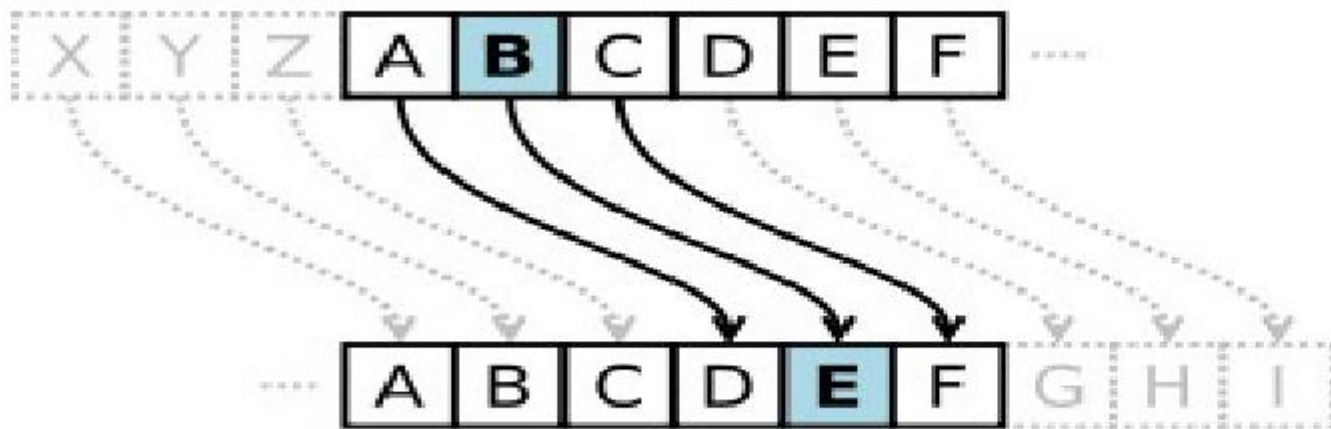
Cifra de substituição polialfabética;

Substituição simples

Cada letra do texto original é substituído por uma correspondente no texto cifrado, de acordo com uma tabela baseada geralmente num deslocamento da letra original dentro do alfabeto. Ela é também chamada Cifra de César devido ao seu uso pelo imperador romano quando enviava mensagens secretas.

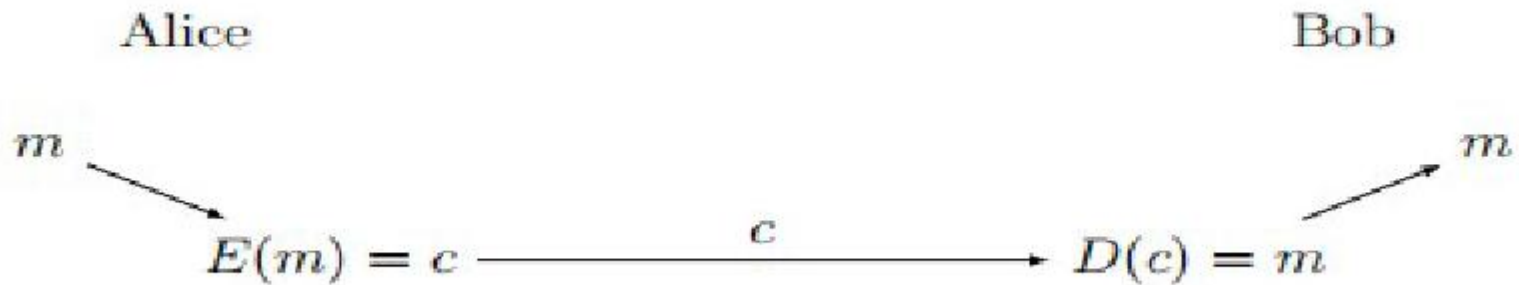
César quando queria enviar mensagens secretas a determinadas pessoas, substituía cada letra “A” de sua mensagem pela letra “D”, o “B” pelo “E”, etc. ou seja, cada letra estava três posições a frente no alfabeto.

Cifra de César



A ação de uma cifra de César é mover cada letra do alfabeto um número de vezes fixo abaixo no alfabeto. Este exemplo está com uma troca de três, então o B no texto normal se torna o E no texto cifrado.

Cifra de César



Alice usa a função E para encriptar a mensagem m ;
A função E desloca cada letra de m três posições para frente, produzindo assim a cifra c ;
Bob utiliza a função D que desloca cada letra da cifra três posições para trás e assim recupera a mensagem m ;

Tal esquema tem pelo menos um grande problema. Ele se torna completamente inseguro caso alguém descubra o mecanismo da função E.
Essas cifras são fáceis de quebrar e vulnerável à análise de frequência.

Substituição polialfabética

São construídas de múltiplas cifras de substituição simples.

Uma letra pode ser associada a múltiplas chaves

Cada uma das chaves é utilizada para encriptar uma letra do texto original.

Inventada por Leon Battista em 1568 e usadas pelo exército Americano na Guerra Civil Americana. A cifra de Vigenère, publicada em 1586 é um exemplo.

Cifra de Vigenère

	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	V
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	W
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	X
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

Por exemplo, supondo que se quer criptografar o texto:

ATACARBASESUL (“atacar base sul”)

Escolhendo a chave e repetindo-a até ter o comprimento do texto a cifrar, por exemplo, se a chave for “LIMAO”:

LIMAOLIMAOLIM

Cifra de Vigenère

	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	V
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	W
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	X
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

A primeira letra do texto, A, é cifrada usando o alfabeto na linha L, que é a primeira letra da chave.

Basta olhar para a letra na linha L e a coluna A na grelha de Vigenère, que é um L.

Cifra de Vigenère

	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	V
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	W
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	X
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

ATACARBASESUL
LIMAOLIMAOLIM

Para a segunda letra do texto, ver a segunda letra da chave: linha I e coluna T, que é B, continuando assim até obter o texto cifrado.

Cifra de Vigenère

	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	V
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	W
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	X
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

Texto:
ATACARBASESUL

Chave:
LIMAOLIMAOLIM

Texto cifrado:
LBMCO CJMSSDCX

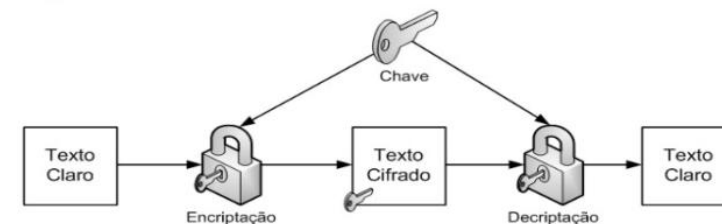
Exemplos de algoritmos simétricos

AES – padrão de criptografia adotado mundialmente;

DES – Antigo padrão de criptografia, considerado hoje inseguro;

3DES – Versão melhorada do DES, que aplica o algoritmo três vezes para aumentar a segurança;

Chacha20 – Algoritmo de fluxo (stream cipher) bastante rápido e seguro, usado em aplicações modernas, como criptografia em conexões HTTPS;



Vantagens VS Desvantagens da criptografia simétrica

Vantagens:

Desempenho superior

Fácil implementação

Eficiente para grandes dados

Desvantagens:

Distribuição da chave

Gerenciamento de chaves

Escalabilidade

Onde é usada?

Criptografia de disco completo – Bitlocker (Windows) e LUKS (Linux);

VPNs e Túnel seguro – tráfego contínuo;

Sistemas de backup – armazenamento de backups na nuvem ou dispositivos externos;

Criptografia Assimétrica

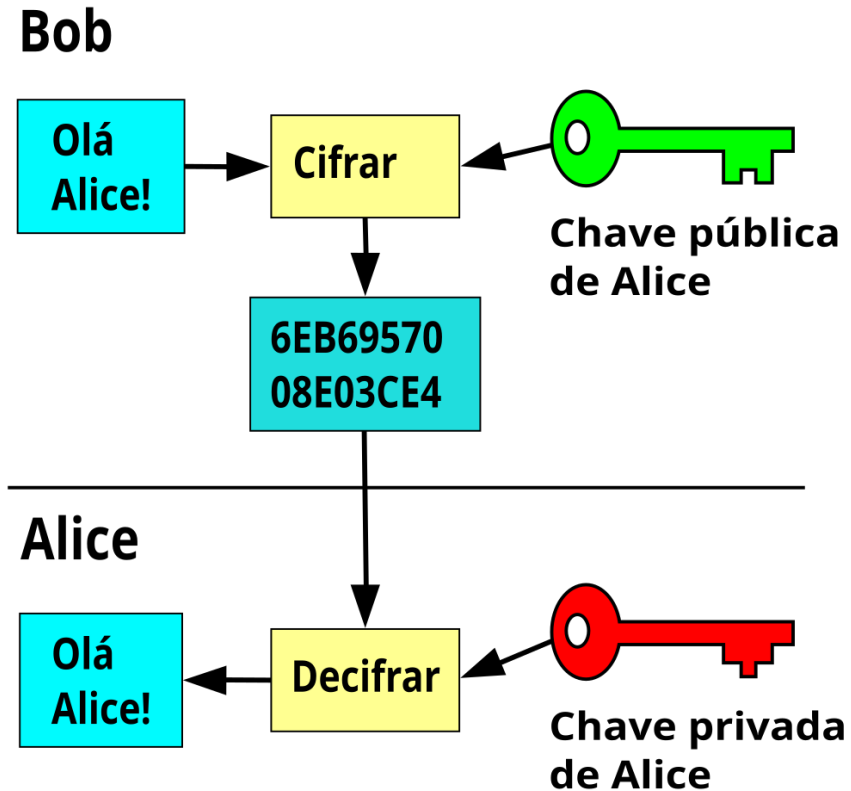
Criptografia assimétrica

Também conhecida como “criptografia de chave pública” é um método que utiliza **duas chaves diferentes**: uma chave pública para criptografar (ou verificar assinaturas) e uma chave privada para descriptografar (ou assinar). A criptografia assimétrica resolve muitos problemas de distribuição e gerenciamento de chaves.

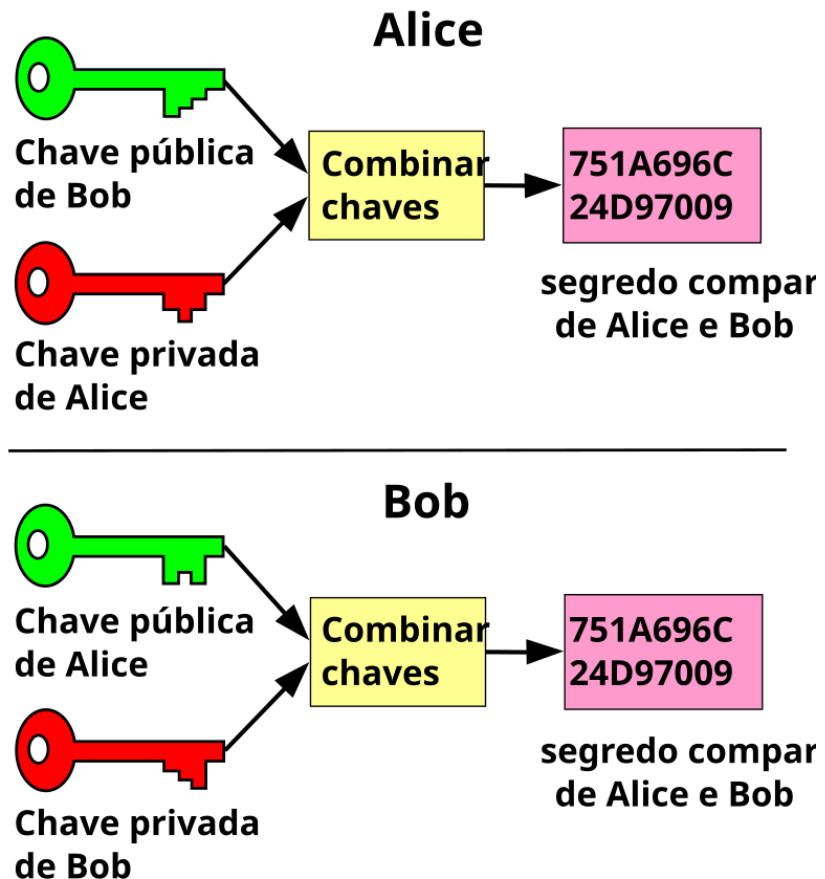
Como funciona?

1. **Geração do par de chaves**– o usuário/sistema gera uma chave pública e uma chave privada;
2. **Criptografia (com chave pública)** – o texto cifrado só poderá ser lido (descriptografado) pela chave privada correspondente;
3. **Descriptografia** – o destinatário utiliza a chave privada para descriptografar o texto;
4. **Assinaturas digitais** – o processo também funciona ao contrário. O dono da chave privada pode “assinar” digitalmente um documento e qualquer pessoa com a chave pública pode verificar se a assinatura é válida.

Criptografia Assimétrica



Criptografia Assimétrica – troca de chaves



Exemplos de algoritmos assimétricos

RSA (Rivest-Shamir-Adleman) – criado em 1977, é um dos algoritmos mais conhecidos. Baseia-se na dificuldade de fatorar grandes números primos;

ECC (Elliptic Curve Cryptography) – usa propriedades de curvas elípticas para fornecer o mesmo nível de segurança do RSA, com chaves menores;

Diffie-Hellman (DH) – não é exatamente um algoritmo de criptografia para mensagens, mas sim um método de troca de chaves segura;

Principais vantagens

1. **Facilidade de distribuição de chaves** – não é necessário um canal secreto para compartilhar a chave pública;
2. **Assinaturas digitais e autenticidade** – esse modelo permite verificar a identidade do remetente (quem assinou não pode negar a autoria);
3. **Segurança escalonável** – em ambientes com muitos usuários, simplifica a distribuição de chaves, pois cada usuário só precisa proteger sua chave privada e divulgar sua chave pública;

Onde é usada?

SSL/TLS (HTTPS): troca de chaves entre navegador e servidor web;

E-mail seguro (PGP/GPG): envio de mensagens criptografadas;

Blockchain e criptomoedas: chaves públicas e privadas são usadas para autenticar transações, garantindo que apenas o dono do endereço possa gastar seus criptoativos;

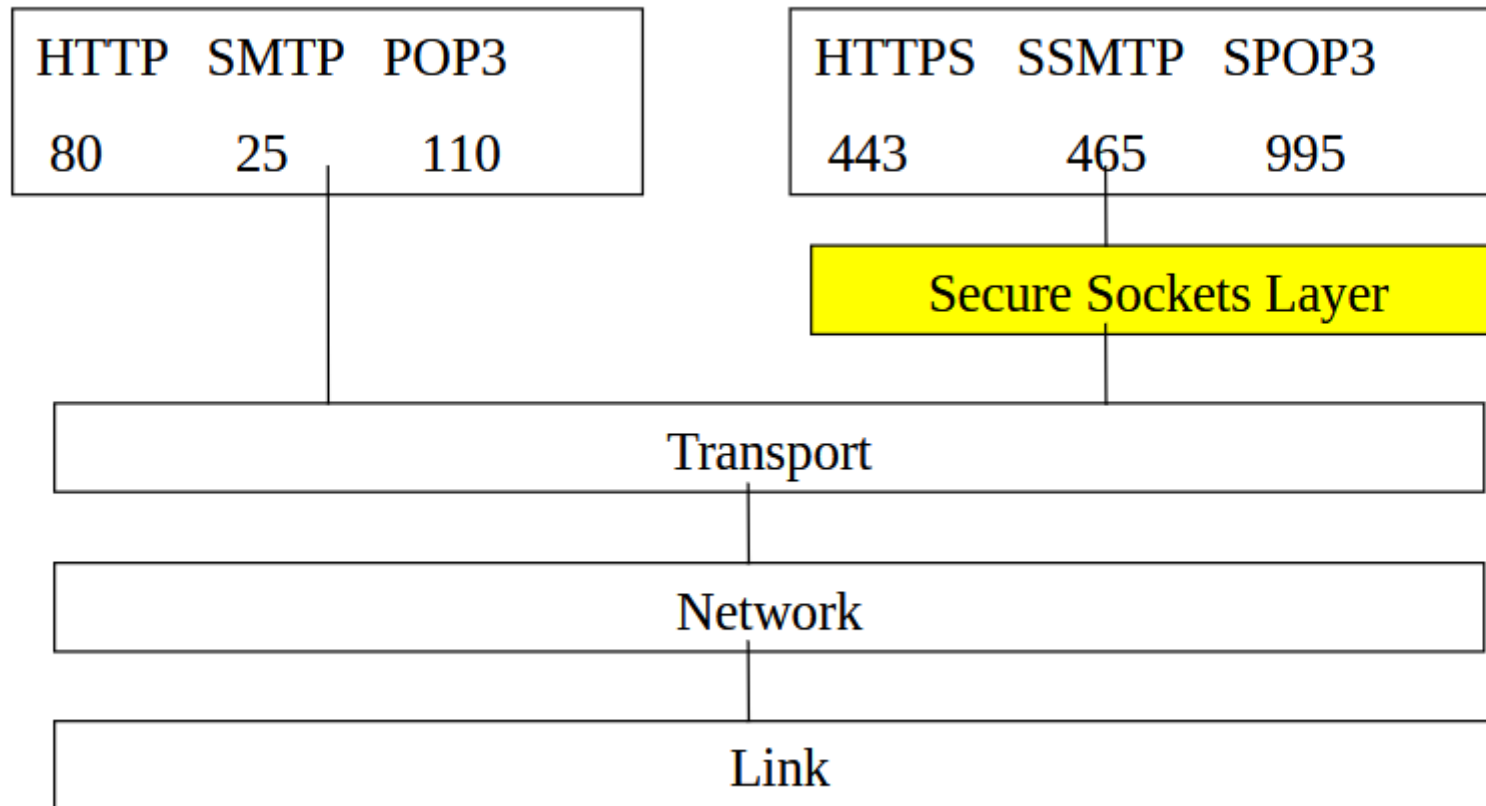
Autenticação e assinaturas digitais: sistemas de governo eletrônico, votação digital e documentos oficiais usam chaves públicas para verificar assinaturas eletrônicas;

SSL (Secure Sockets Layer)

- Protocolo de segurança usado para estabelecer uma conexão criptografada entre um servidor e um cliente, por exemplo: navegador e webserver. Provendo integridade de dados entre duas aplicações que se comunicam pela internet.
- Ajuda a prevenir que intermediários entre as duas extremidades das comunicações obtenham acesso indevido ou falsifiquem os dados transmitidos (Man in the Middle);
- Evoluiu para o TLS, a versão mais segura do protocolo – RFC 2246
- Comando para verificar o certificado SSL de um site:

```
openssl s_client --connect google.com:443
```

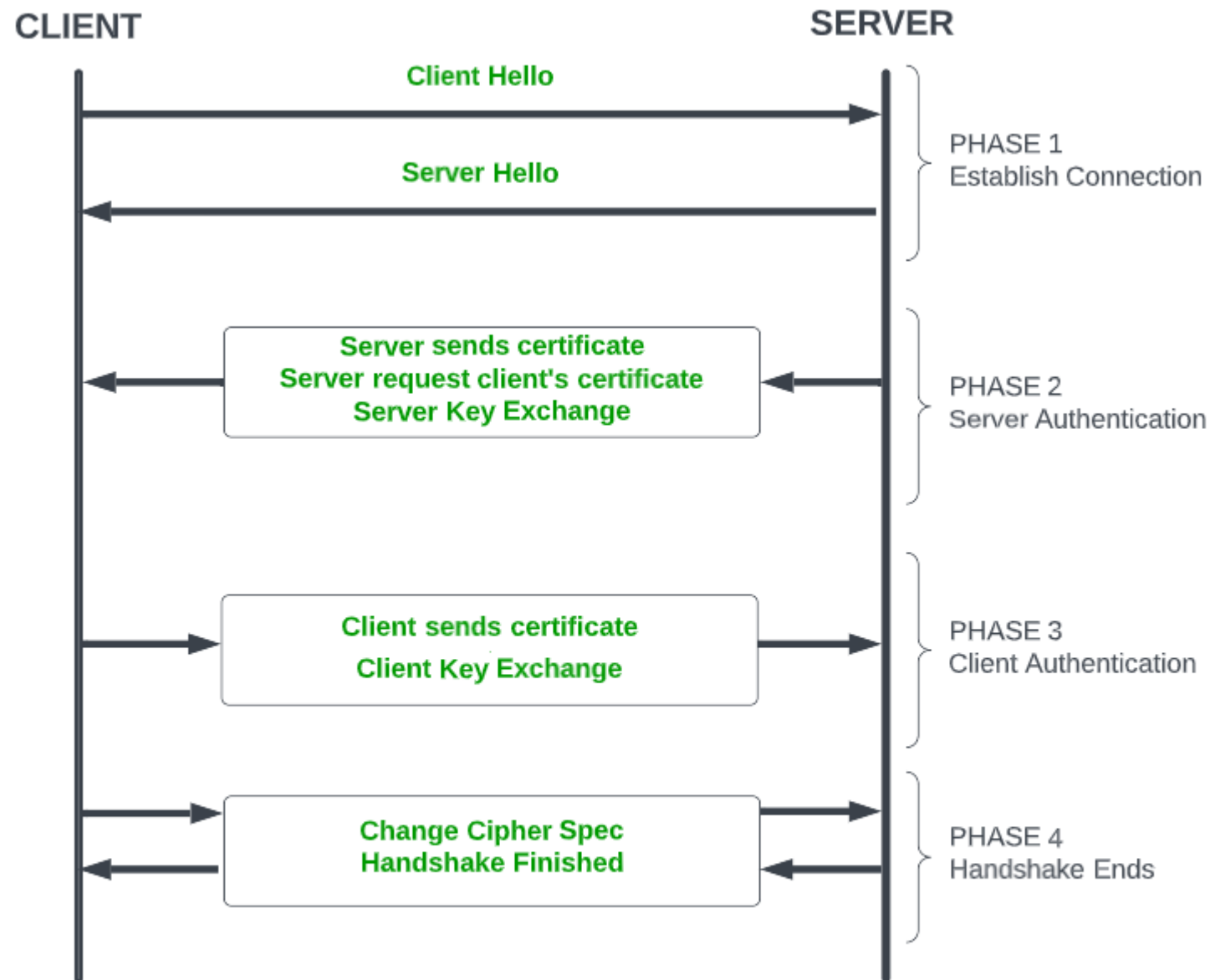
SSL (Secure Sockets Layer)



SSL (Secure Sockets Layer)

Cada cliente-servidor usa um par de chaves

- 2 chaves públicas
 - Uma para o cliente (browser), criado quando o navegador é instalado na máquina
 - Uma para o servidor (http servidor), geralmente criado na instalação do servidor
- 2 chaves privadas
 - Uma para o browser do cliente
 - Uma para o servidor



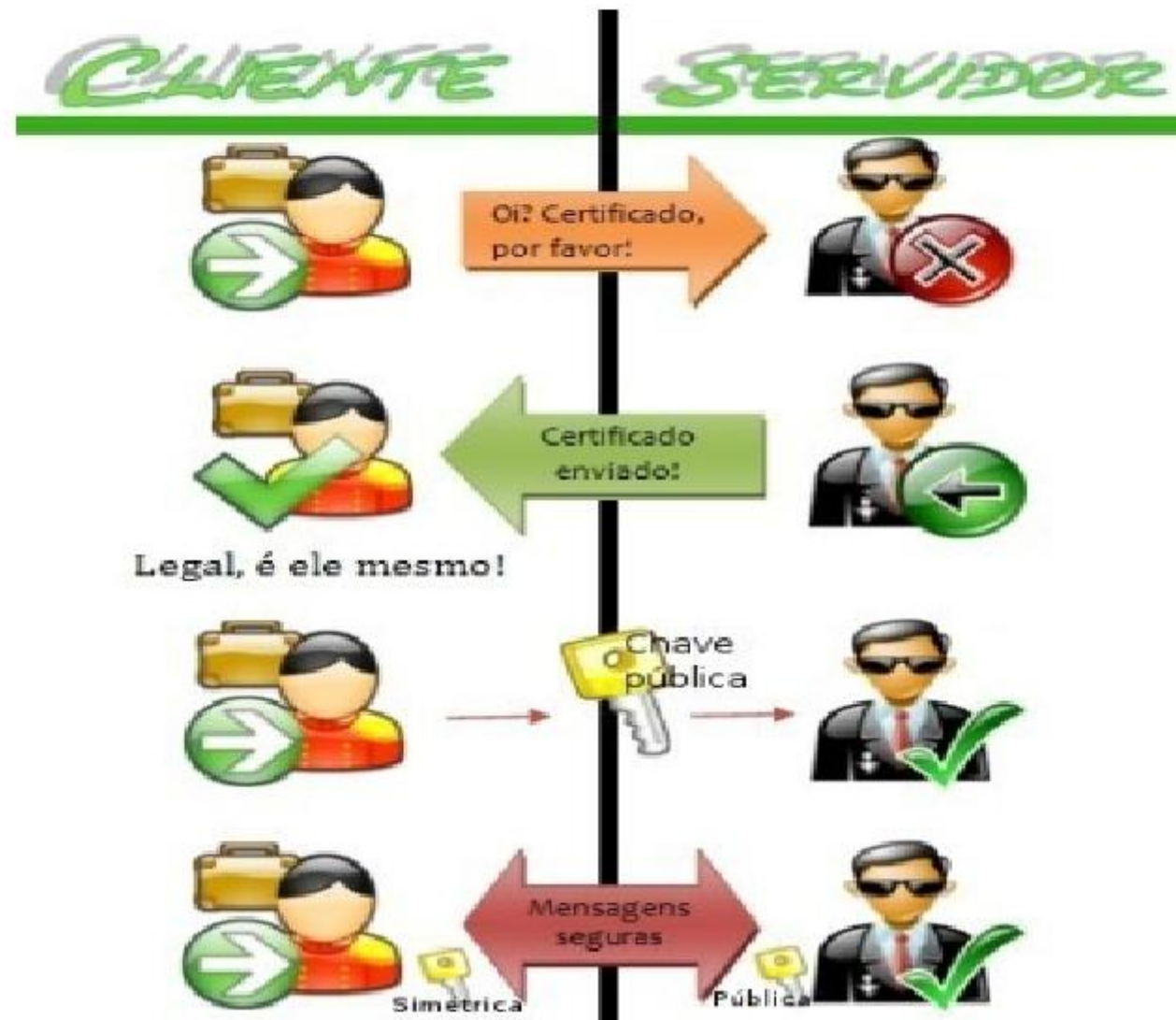
SSL HANDSHAKE PROTOCOL

HTTPS (Hyper Text Transfer Protocol Secure)

É a versão segura do HTTP. Meios seguros de transferência de dados usando o protocolo https na internet são necessários para efetuar transações online seguras, como os serviços bancários ou compras online.

O HTTP criptografa a sessão com um certificado digital, utilizando o HTTP sobre SSL utilizado pelos navegadores.

HTTPS



Hash

Hash é uma função matemática que transforma uma entrada de qualquer tamanho em uma saída de tamanho fixo.

O processo é Unidirecional, ou seja, não é possível reverter um hash para recuperar a entrada original.

Hash - tipos

- MD5 – Gera um hash de 128 bits (32 caracteres hexadecimais)
- SHA-1 – Produz um hash de 160 bits (40 caracteres hexadecimais)
- SHA-256 e SHA-512 – amplamente usado para segurança
- Bcrypt e argon2 – hashes modernos utilizados para armazenar senhas com proteção contra ataques de força bruta.

Diferenças entre hash e criptografia

Característica	Hash	Criptografia
Objetivo	Garantir integridade de dados	Proteger dados contra acesso não autorizado
Unidirecional?	Sim	Não
Pode ser revertido?	Não	Sim
Exemplos	SHA-256, MD5	AES, RSA, ECC

Senhas armazenadas em hash nunca devem ser descriptografadas. Em vez disso, quando o usuário digita uma senha, o sistema gera um novo hash e compara com o hash armazenado.

Aplicações Práticas

Criptografia simétrica

Crie um arquivo de texto no seu host
Para criptografar usaremos o openssl:

Comando: openssl enc -aes-256-cbc -salt -pbkdf2 -in [nome do arquivo].txt -out [nome do arquivo].txt.enc

Criptografia simétrica

Crie um arquivo de texto com uma frase no conteúdo no seu host.

Para criptografar usaremos o openssl:

Comando: openssl enc -aes-256-cbc -salt -pbkdf2 -in [nome do arquivo].txt -out [nome do arquivo].txt.enc

Criptografia simétrica

Comando	Explicação
-aes-256-cbc	define o algoritmo AES com chave de 256 bits no modo CBC (cipher block chaining)
-salt	adiciona um salt aleatório para aumentar a segurança contra ataques de força bruta
-pbkdf2	usa o algoritmo PBKDF2 para derivação da chave a partir da senha digitada
-in [nome do arquivo].txt	indica o arquivo de entrada a ser criptografado
-out [nome do arquivo].txt.enc	define o arquivo de saída que conterá o texto cifrado

Criptografia simétrica

Após executar o comando, o openssl solicitará uma senha para proteger o arquivo e salvará a nova versão criptografada do arquivo;

O conteúdo será ilegível se você tentar visualizá-lo com um editor de texto;

Para descriptografar e recuperar o conteúdo original do arquivo, use o comando:

```
openssl enc -aes-256-cbc -d -salt -pbkdf2 -in [nome do arquivo].txt.enc -out [nome do arquivo]_decifrado.txt
```

Novamente, o openssl pedirá a mesma senha usada na criptografia. Se a senha for correta, o conteúdo original será restaurado

Criptografia Assimétrica

Vamos agora criar um par de chaves (pública e privada) para criptografar um documento usando criptografia assimétrica.

Comando:

```
openssl genpkey -algorithm RSA -out chave_privada.pem -pkeyopt rsa_keygen_bits:2048
```

Comando	Explicação
genpkey -algorithm RSA	Gera uma chave privada do tipo RSA
-out chave_privada.pem	Salva a chave privada
-pkeyopt rsa_keygen_bits:2048	Define o tamanho da chave para 2048 bits

Criptografia Assimétrica

Extraindo a chave pública da chave privada

Comando:

```
openssl rsa -in chave_privada.pem -pubout -out chave_publica.pem
```

Comando	Explicação
-in chave_privada.pem	Usa chave privada como base
-pubout	Extrai apenas a parte pública da chave
-out chave_publica.pem	Salve a chave pública

Criptografia Assimétrica

Temos:

chave_privada.pem – usada para descriptografar e assinar.

chave_publica.pem – usada para criptografar e verificar assinaturas.

Para criptografar um arquivo usando a chave pública:

```
openssl rsautl -encrypt -pubin -inkey chave_publica.pem -in mensagem.txt -out mensagem.enc
```

Criptografia Assimétrica

Comando	Explicação
rsautl -encrypt	Indica que queremos criptografar
-pubin	Especifica que estamos usando uma chave pública
-inkey chave_publica.pem	Especifica o arquivo da chave pública
-in mensagem.txt	Define o arquivo de entrada (plaintext)
-out mensagem.enc	Define o arquivo de saída (criptografado)

O arquivo mensagem.enc agora contém a mensagem criptografada e **não pode ser lido sem a chave privada.**

Criptografia Assimétrica

Para descriptografar o arquivo “mensagem.enc” usando a nossa chave privada usamos o comando:

```
openssl rsautl -decrypt -inkey chave_privada.pem -in mensagem.enc -out mensagem_decifrada.txt
```

Agora o conteúdo original está salvo no arquivo mensagem_decifrada.txt

Criptografia Assimétrica – Criando assinatura digital

A assinatura digital permite garantir que um arquivo ou mensagem foi criado por uma pessoa específica e que não foi alterado.

Para assinar um arquivo chamado documento.txt usamos o comando:

```
openssl dgst -sha256 -sign chave_privada.pem -out assinatura.bin documento.txt
```

Comando	Explicação
dgst -sha256	Gera um hash SHA-256 do arquivo
-sign chave_privada.pem	Usa a chave privada para assinar o hash
-out assinatura.bin	Salva a assinatura digital no arquivo assinatura.bin

Criptografia Assimétrica – Criando assinatura digital

Agora temos um arquivo assinado. Mas como verificar se ele é autêntico???

Qualquer pessoa com a chave pública pode verificar se o documento foi realmente assinado pela chave privada correspondente.

```
openssl dgst -sha256 -verify chave_publica.pem -signature assinatura.bin documento.txt
```

Se a assinatura for válida, OpenSSL retornará algo como: **Verified OK**

Criptografia Assimétrica – Certificado digital

The screenshot shows the Itaú website with a digital certificate viewer overlay. The overlay is titled "Visualizador do certificado: www.ita.com.br" and has tabs for "Geral" and "Detalhes". The "Geral" tab is active, displaying the following information:

Emitido para	
Nome comum (CN)	www.ita.com.br
O (Organização)	Itau Unibanco S.A.
Unidade organizacional (OU)	<Não faz parte do certificado>







Emitido por	
Nome comum (CN)	DigiCert TLS RSA SHA256 2020 CA1
O (Organização)	DigiCert Inc
Unidade organizacional (OU)	<Não faz parte do certificado>

Período de validade	
Emitido em	domingo, 11 de agosto de 2024 às 21:00:00
Expira em	terça-feira, 12 de agosto de 2025 às 20:59:59

Impressões digitais SHA-256	
Certificado	1d01b54b6063d0886f1ae59d593a5fec62d1ba4507c33fe4edaf0647101eed5c
Chave pública	e0a02aca0e8a28e36bbfe5a4ca1e1faa3a9d45c7c5690abed1016564ea254558

A yellow arrow points from the "Venha conferir" button on the website to the "Certificado" field in the certificate viewer.

Resolva as questões do dia a dia

 Boleto Emita 2ª via de boletos Itaú	 Desbloqueio de cartão Saiba como fazer	 Aplicativos Baixe os apps do banco Itaú	 Fatura digital Receba a fatura do seu cartão	 Comprovantes Gere uma 2ª via do comprovante	 Atendimento Conheça nossos canais de ajuda
--	---	--	---	--	---

Hash

Crie dois arquivos de texto simples iguais e gere os hashes SHA-256 para os arquivos. Observe que a saída esperada é igual para os dois arquivos.

```
openssl dgst -sha256 arquivo1.txt
```

```
openssl dgst -sha256 arquivo2.txt
```

Modifique um dos arquivos e gere o hash novamente

```
echo "Agora este arquivo foi modificado." >> arquivo2.txt
```

Compare os hashes novamente. Após a modificação do arquivo2.txt os hashes ficaram completamente diferentes.

Hash

Atividade – Utilizando os conhecimentos passados em aula e pesquisas, quebre o hash abaixo:

55a5e9e78207b4df8699d60886fa070079463547b095d1a05bc719bb4e6cd251

Você pode usar o hashcat dentro do Kali Linux que instalou na virtual box na semana passada.

Materiais complementares

- Ferramentas: OpenSSL, Hashcat, Wireshark
- Links úteis: OWASP cryptography Storage Cheat Sheet, NIST Recommendations.
- Leituras recomendadas:

Applied Cryptography – Bruce Schneier
Cryptography and Network Security – William Stallings
OWASP Cryptography Failures Top 10