

Segurança da Informação

Competências:

- Implementar práticas e condutas de segurança da informação no ambiente de TI.

Bases Tecnológicas, científicas e instrumentais (conteúdos):

- Criptografia Simétrica e Assimétrica;

Situação de Aprendizagem:

- Apresentação da criptografia.

Criptologia

Criptografia + Criptoanálise

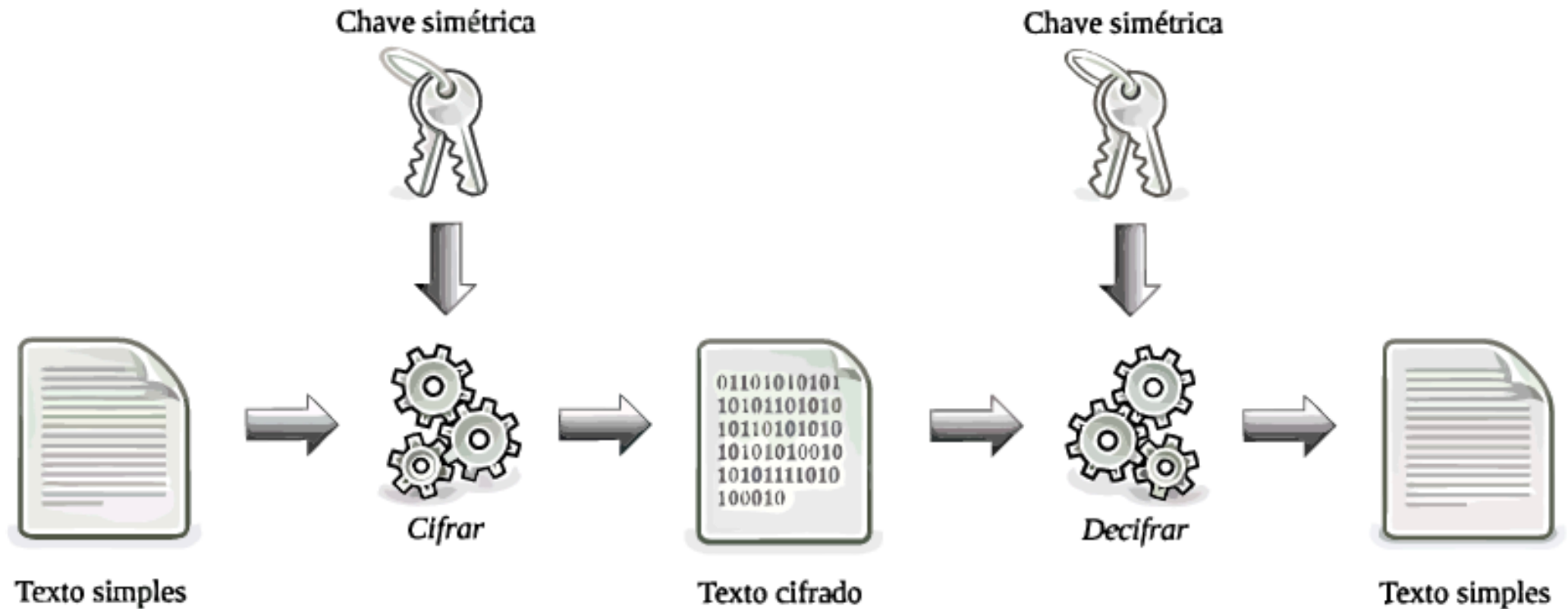
Criptografia

Métodos e protocolos para segurança de
informação

Criptóanálise

Testar e validar métodos criptográficos

Elementos da Criptografia



Objetivos da Criptografia

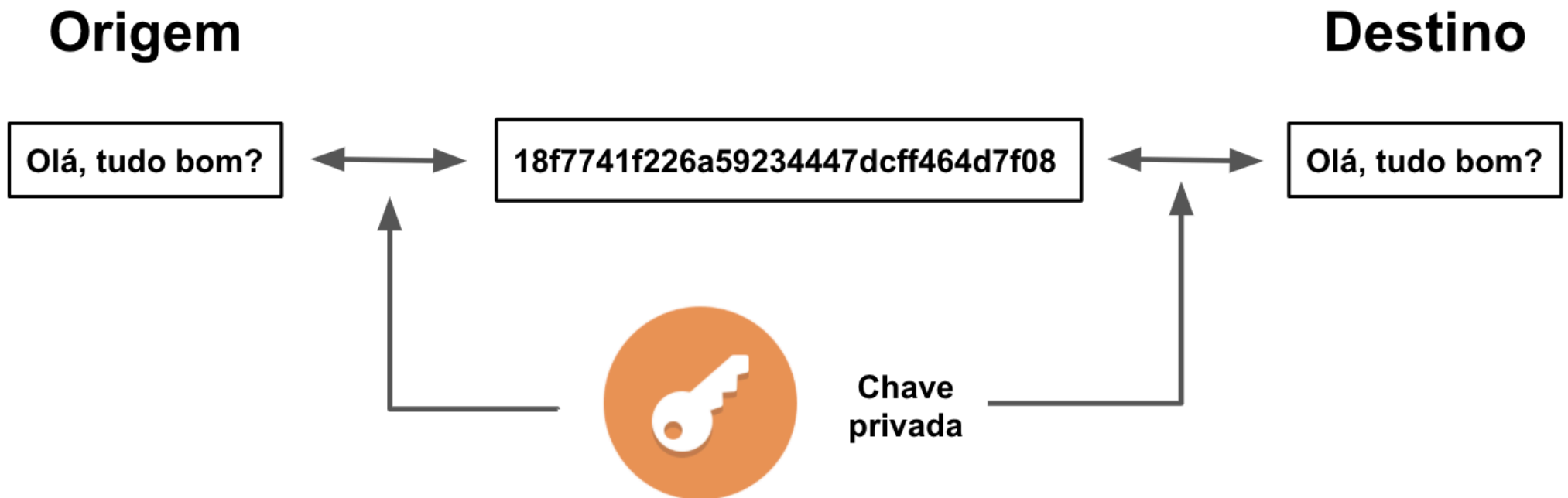
- Confidencialidade das mensagens
- Integridade de dados
- Identificação de entidades
- Autenticação de mensagens
- Autorização e Controle de acesso
- Certificação
- Anonimato
- Não-repúdio

Fatores de Sucesso

- A confidencialidade das chaves.
- A dificuldade de adivinhar as chaves.
- A dificuldade de inverter o algoritmo de criptografia sem saber a chave.

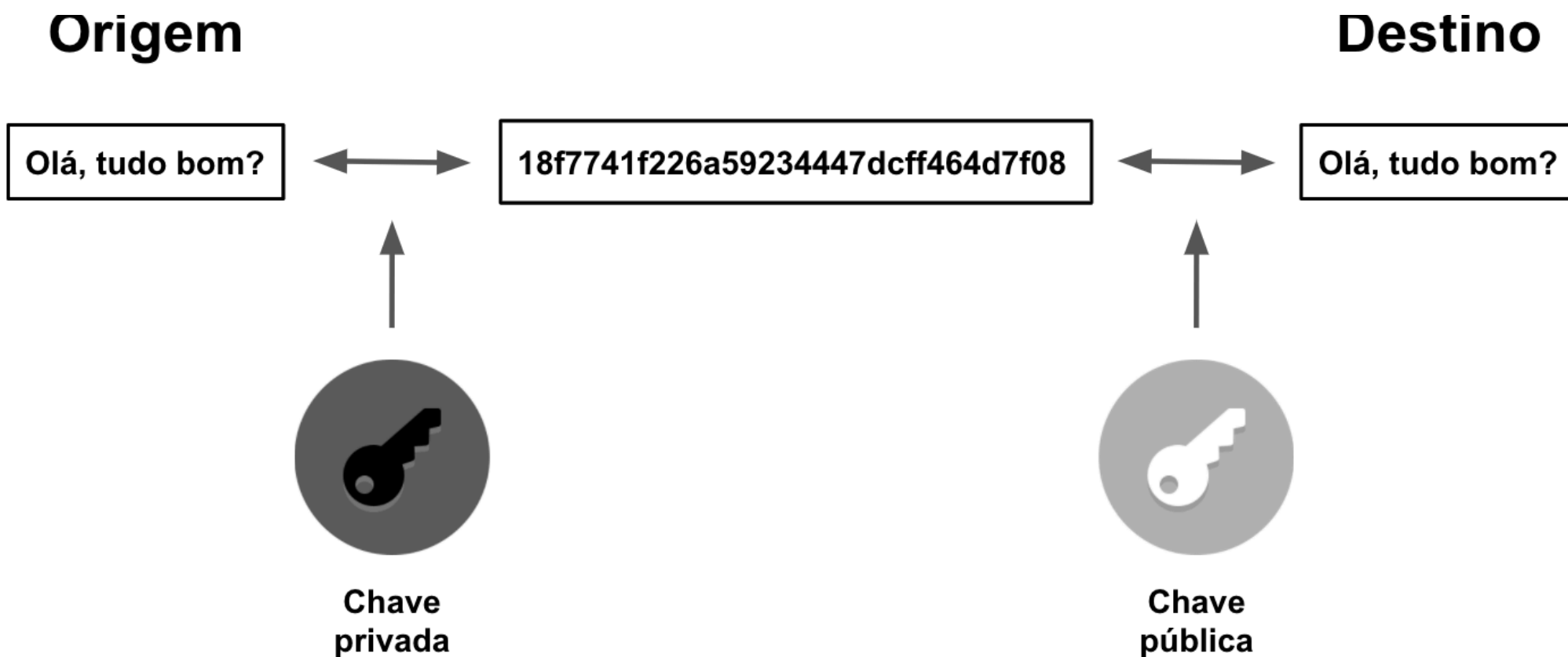
Tipos de Criptografia

Criptografia Simétrica

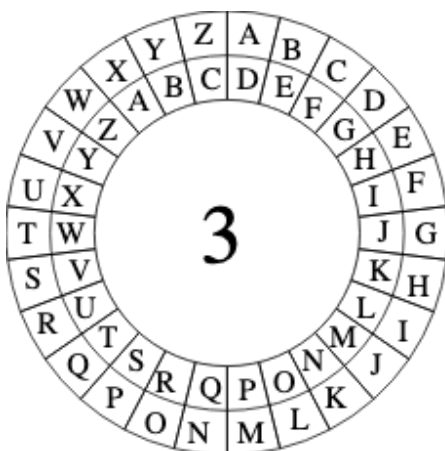


Tipos de Criptografia

Criptografia Assimétrica



Criptografia Simétrica



Criptografia Simétrica

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	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: **A**TACARBASESUL

Chave: **L**IMAOLIMAOLIM

Cifra: **L**BMCOCJMSSDCX

	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: A**T**ACARBASESUL

Chave: L**I**MAOLIMAOLIM

Cifra: L**B**MCOCJMSSDCX

	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: ATACAR**R**BASESUL

Chave: LIMAOL**L**IMAOLIM

Cifra: LBMCO**C**JMSSDCX

Criptografia Simétrica

Vigenère

Texto: ATACARBASESUL

Chave: LIMAOLIMAOLIM

Cifra: LBMCO CJMSDCX

Criptografia Simétrica

Vigenère - Criptoanálise

LBMCO CJMS SDCX

Passo 1: Verificar as frequências das letras para confirmar que se trata de uma cifra polialfabética. Isto ocorre pela semelhança das frequências.

Passo 2: Procuramos as repetições de pedaços das cifras que se repetem.

Passo 3: Procurar as distâncias entre estas ocorrências.


Passo 4: A partir destas distâncias, verificar o divisor comum.


Passo 5: A partir deste ponto, faz-se a análise monoalfabética.


Criptografia Simétrica

Vigenère - Criptoanálise

LBMCO CJMS SDCX

A 1111
B 11
C 11111
D 111111111
E
F
G 11111
H 1
I 1111
J 111111
K 111
L 1
M 1111
N 1111
O 1111111111111
P 1111
Q 1
R
S 1
T
U
V 1111
W 1
X 11
Y 1111
Z 111111111111111 

A 1111111111
B 1111111111
C 11
D 11
E
F 1
G
H
I 11111
J 1
K 1111
L 1
M 111111111111 
N 111
O 1111
P 111111
Q 111
R
S
T 111
U 11
V 1111111111
W 11111111
X 1
Y
Z 11111

A
B
C 11
D 111
E 11111
F 1111
G 111
H
I 111111111
J 11
K 11111111111
L 111
M
N
O
P 11
Q
R 111111111111
S 111
T 1
U 11
V 111111111111 
W 111
X 11
Y 111
Z 11111111

Criptografia Simétrica

Vigenère - Criptoanálise

LBMCO CJMSS DCX

LBMCO CJMSS DCX

Criptografia Simétrica

Vigenère - Criptoanálise

LBMCO CJMSS DCX

LBMCO C**J**MSS D**C**X

Análise de frequência do alfabeto

Criptografia Simétrica

Vigenère - Criptoanálise

LBMCO CJMSS DCX

LBMCO **C**JMSS **D**CX

L**B**MCO C**J**MSS D**C**X

L**B**MCO C**J**MSS D**C**X

LBM**C**O CJM**S**S DCX

LBMCO CJMSS**S** DCX

M = A ou E?

Criptografia Simétrica

Vigenère - Criptoanálise

Criptografia

Algoritmos

- » Tipos de cifradores simétricos:
 - De bloco: os dados são processados em blocos
 - De fluxo: os dados são processados bit-a-bit ou byte-a-byte
- » Alguns cifradores simétricos:
 - DES, 3DES
 - BLOWFISH
 - RC2
 - RC4
 - IDEA
 - RC5
 - TWOFISH
 - SERPENT
 - RIJNDAEL (AES)

Criptografia

DES(Data Encryption Standard)

- » Cifrador mais conhecido do mundo
- » Originado a partir do LUCIFER (IBM - Feistel)
- » Aprovado como padrão em 1977
- » Mensagem: 64 bits
- » Chave: 64 bits = 56 utilizados + 8 paridade
- » Mensagem cifrada: 64 bits

Criptografia

3DES(Triple Data Encryption Standard)

- » Autor: IBM, início de 1979.
- » Chave: 168 bits
- » Comentário: **Segunda melhor escolha.**

Criptografia

Blowfish

- » Autor: Bruce Schneier
- » Chave: 1 a 448 bits
- » Comentário: Velho e lento.

Criptografia RC2

- » Autor: Ronald Rivest, RSA Data Security
Meado dos anos 80.
- » Chave: 1 a 2048 bits
40 bits para exportação
- » Comentário: quebrado em 1996.

Criptografia RC4

- » Autor: **Ronald Rivest, RSA Data Security, 1987**
- » Chave: 1 a 2048 bits
- » Comentário: **Algumas chaves são fracas.**
- » Usado como componente do SSL (Netscape)

Criptografia

IDEA – International Data Encryption Algorithm

- » Autor: **Massey & Xuejia, 1990.**
- » Chave: 128 bits
- » Comentário: **Bom, mas patenteado.**
- » Usado no PGP.

Criptografia

RC5

- » Autor: Ronald Rivest,
RSA Data Security, 1994.
- » Chave: 128 a 256 bits
- » Comentário: **Bom, mas patenteado.**

Criptografia Twofish

- » Autor: Bruce Schneier, 1997
- » Chave: 128 a 256 bits
- » Comentário: **Muito forte,
amplamente utilizado.**

Criptografia Serpent

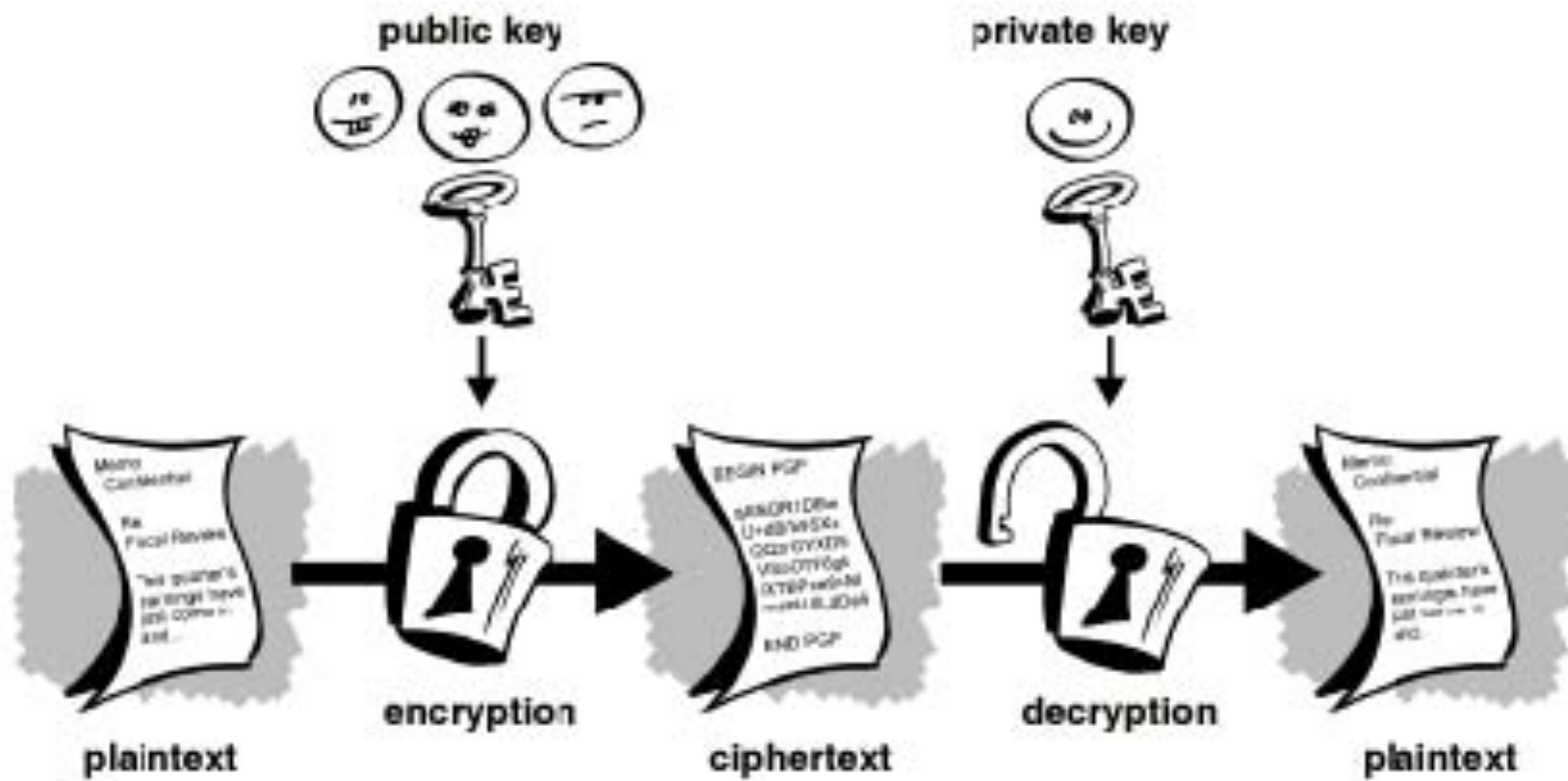
- » Autor: Anderson, Biham, Knudsen 1997
- » Chave: 128 a 256 bits
- » Comentário: **Muito forte.**

Criptografia Rijndael

- » **Advanced Encryption Standard**
- » **Tamanho do Bloco: 128 bits**
- » **Comprimento da Chave: 128, 192, 256 bits.**

Criptografia

Criptografia Assimétrica



Criptografia

Algoritmos de chave pública/privada

- » Proposto por W. Diffie e M. Hellman(1976)
- » Baseia-se num par de chaves **(e,d)**
 - **e**: pública, serve para cifrar
 - **d**: privada, serve para decifrar
- » Necessita garantir autenticidade de **e**
- » Objetivo principal: prover confidencialidade
- » Chave pública: provê identificação
- » Mais lento que algoritmos de chave secreta
- » Exemplos: RSA, ElGamal, Rabin

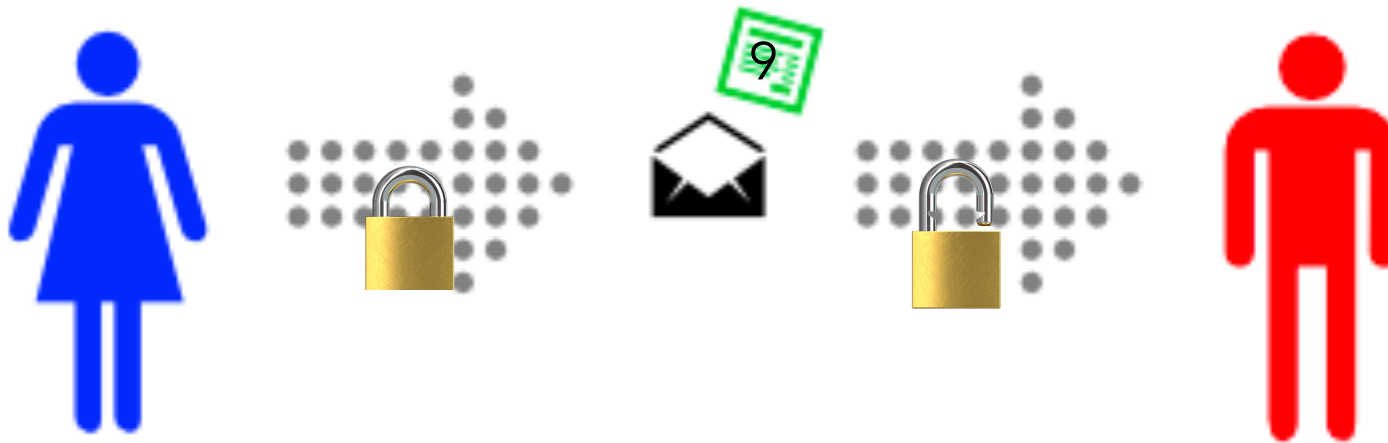
Criptografia

RSA (Rivest-Shamir-Adleman)

- » Primeiro algoritmo prático (1978)
- » Mais usado algoritmo de chave pública
- » Provê confidencialidade e assinatura digital
- » Segurança: Fatoração de Números Grandes

Criptografia

RSA (Rivest-Shamir-Adleman)

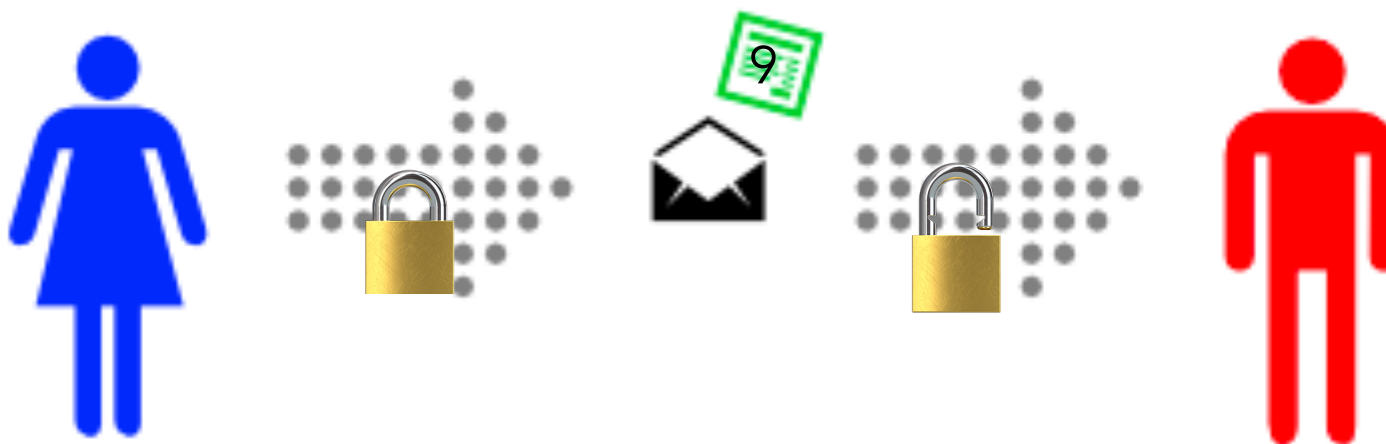


Passo 1: Escolher dois números primos

$$p = 3$$
$$q = 11$$

Criptografia

RSA (Rivest-Shamir-Adleman)



Passo 1: Escolher dois números primos

Passo 2: Calcular o produto dos números

$$n = pq = 33$$

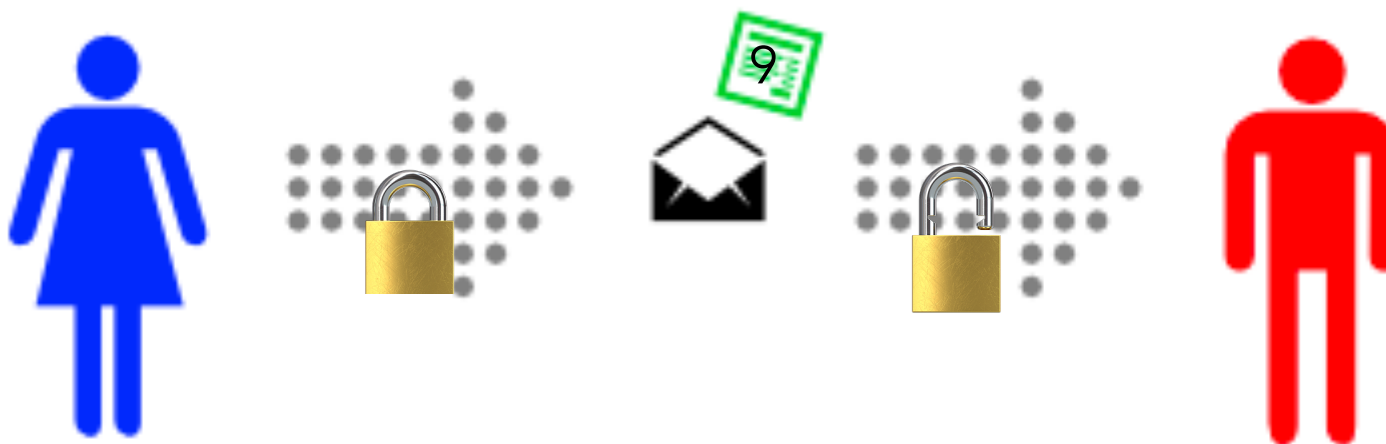
Chave Pública

$n=33$

$e=17$

Criptografia

RSA (Rivest-Shamir-Adleman)



Passo 1: Escolher dois números primos

Passo 2: Calcular o produto dos números

Passo 3: Calcular o produto dos números $p-1$ e $q-1$

$$t = (p-1)(q-1) = 20$$

Criptografia

RSA (Rivest-Shamir-Adleman)



Passo 1: Escolher dois números primos

Passo 2: Calcular o produto dos números

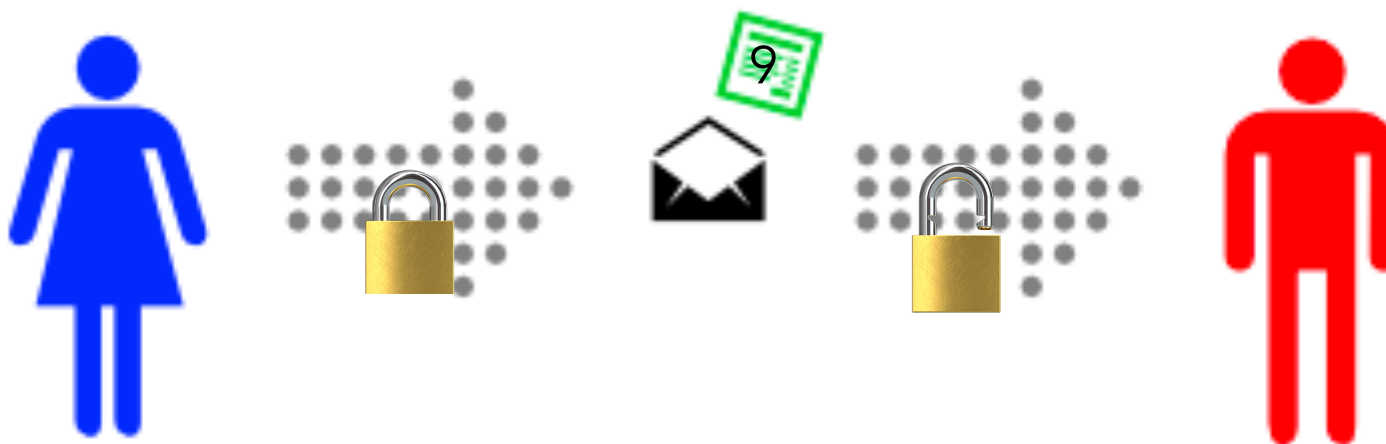
Passo 3: Calcular o produto dos números $p-1$ e $q-1$

Passo 4: Escolher um número que seja primo com t

$$t = (p-1)(q-1) = 20$$

Criptografia

RSA (Rivest-Shamir-Adleman)



Passo 1: Escolher dois números primos

Passo 2: Calcular o produto dos números

Passo 3: Calcular o produto dos números $p-1$ e $q-1$

Passo 4: Escolher um número que seja primo com t

Chave Pública

$n=33$

$e=17$

$e = 17$

Criptografia

RSA (Rivest-Shamir-Adleman)



Passo 1: Escolher dois números primos

Passo 2: Calcular o produto dos números

Passo 3: Calcular o produto dos números $p-1$ e $q-1$

Passo 4: Escolher um número que seja primo com t

Passo 5: Calcular d , de tal forma que $e * d \bmod 20$ precisa ser 1.

Chave Pública

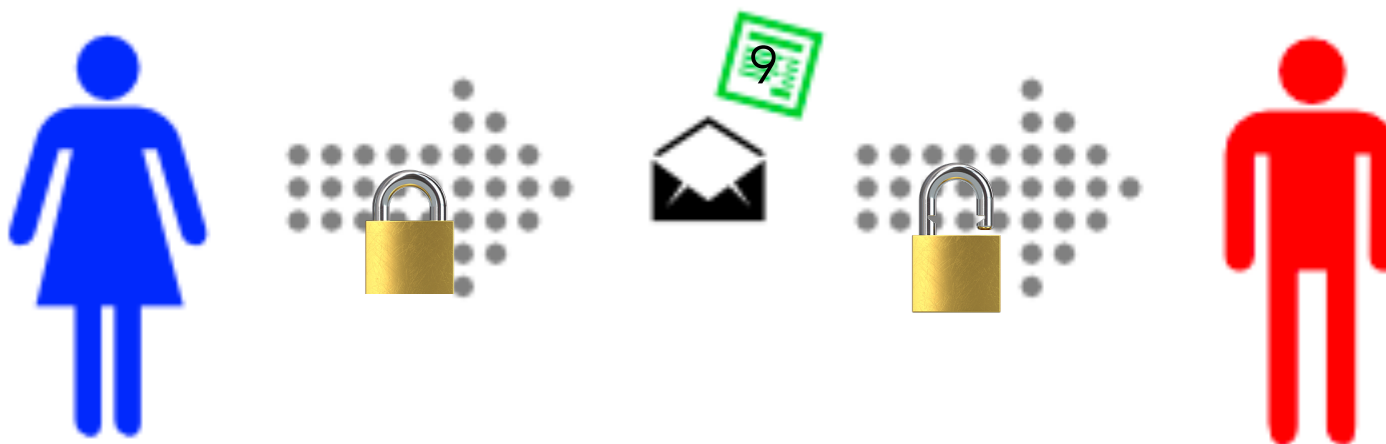
$n=33$

$e=17$

$$e * 17 \bmod 20 = 1 \Rightarrow e=13$$

Criptografia

RSA (Rivest-Shamir-Adleman)



Passo 1: Escolher dois números primos

Passo 2: Calcular o produto dos números

Passo 3: Calcular o produto dos números $p-1$ e $q-1$

Passo 4: Escolher um número que seja primo com t

Passo 5: Calcular d , de tal forma que $e * d \bmod 20$ precisa ser 1.

Chave Pública

$n=33$

$e=17$

Chave Privada

$n=33$

$d=13$

$$e * 17 \bmod 20 = 1 \Rightarrow e=13$$

Criptografia

RSA (Rivest-Shamir-Adleman)

Cifrar:

$$c = m^e \% n$$

Decifrar:

$$c^d \% n$$

Chave Privada

n=33

d=13

Chave Pública

n=33

e=17

Criptografia

RSA (Rivest-Shamir-Adleman)

Cifrar:

$$c = m^e \% n$$

$$c = 9^{17} * 33 = 16677181699666569 \% 33 = 15$$

Decifrar:

$$c^d \% n$$

$$15^{13} \bmod 33 = 1946195068359375 \bmod 33 = 9$$

Criptografia

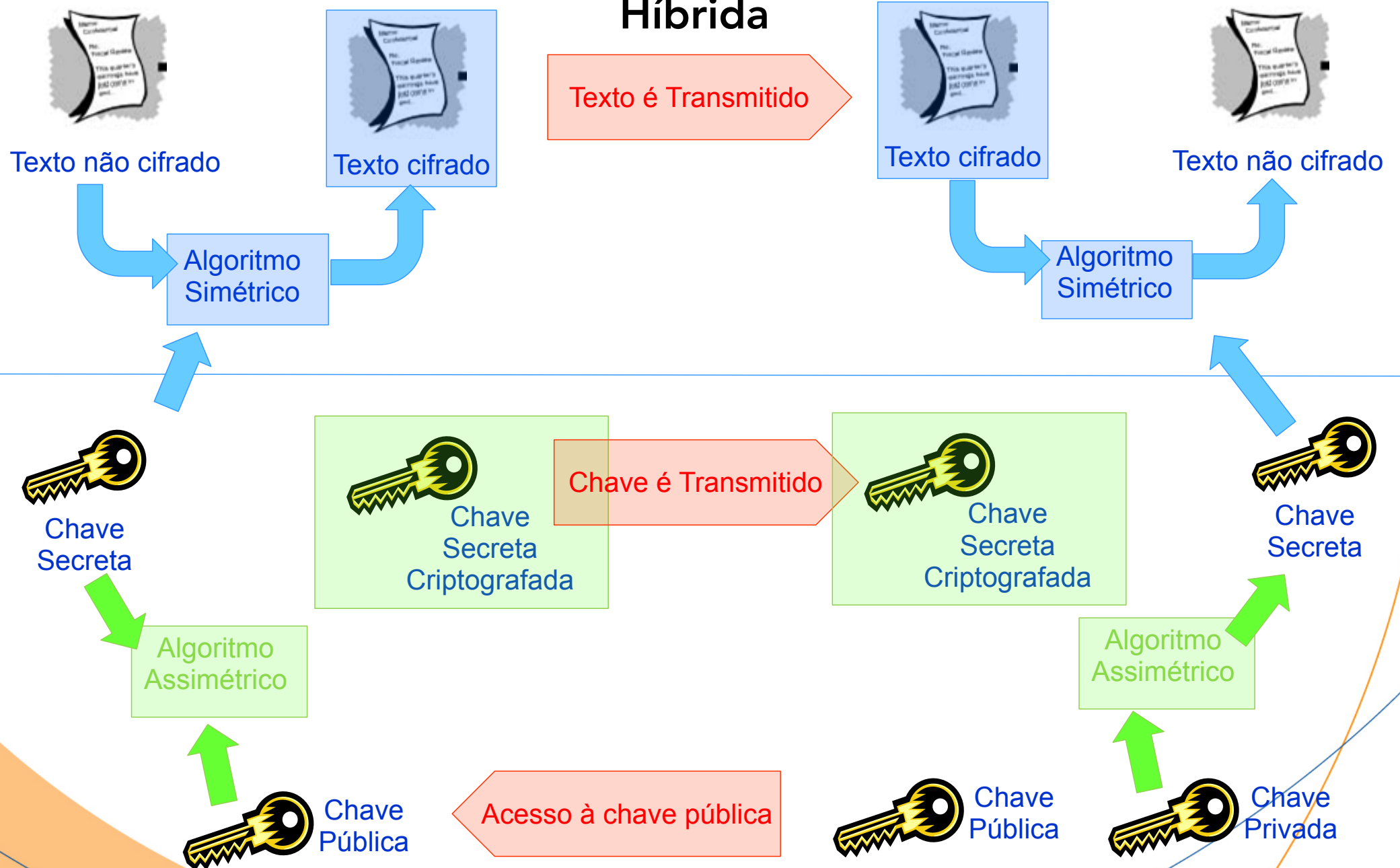
RSA (Rivest-Shamir-Adleman)

Criptografia Híbrida

» Híbrida

- “Meio termo” entre as criptografias
- Aproveita o que tem de bom das duas partes.
- Processo que utiliza a criptografia simétrica para o envio/recebimento de mensagens e a criptografia assimétrica no compartilhamento das chaves secretas

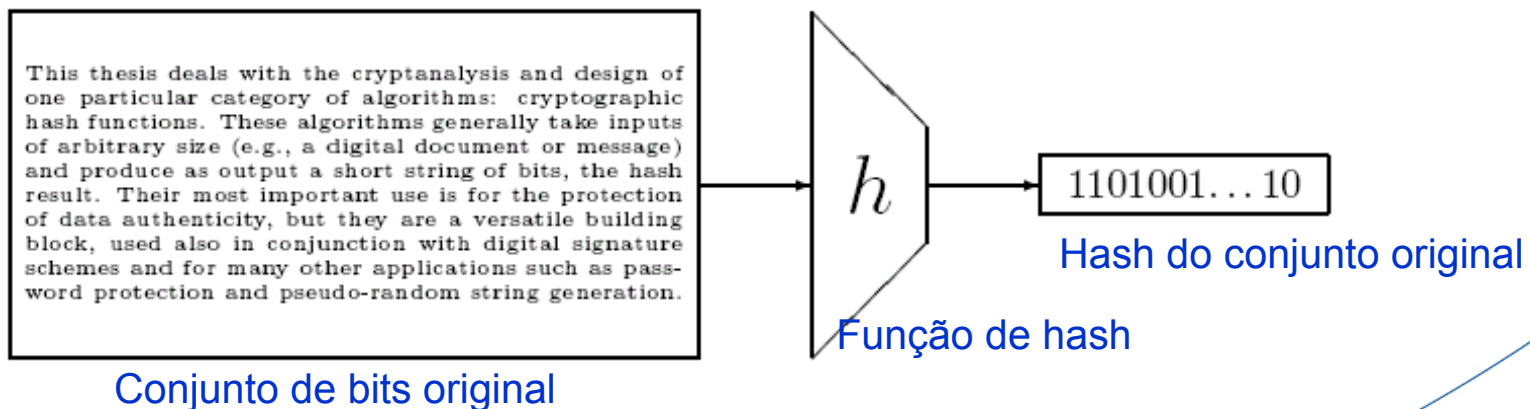
Criptografia Híbrida



Hash

Introdução

- » Também chamada de função de espalhamento, são funções que convertem uma seqüência de bits em um conjunto de strings de tamanho fixo;
- » Embora matematicamente seja possível encontrar o mesmo hash para conjuntos distintos de bits, isso é difícil na prática. Isto é chamado de colisão.
- » Uma boa função *hash* é aquela que: (i) é simples de ser computada e (ii) minimiza o número de colisões, isto é, para cada chave de entrada, qualquer uma das saídas possíveis é igualmente provável de ocorrer.



Hash

Aplicações

- » **Assinatura Digital:** para assegurar que o documento não foi alterado; para verificar a autenticidade de um documento; Distribuição do software;
- » **Digital timestamping:** assegurar a data e hora da criação do documento;
- » **Proteção de senhas:** armazena-se o hash da senha;
- » **Autenticação da mensagem:** assegurar que a mesma não foi alterada.

Hash

MD5: Message Digest

- » Desenvolvidos pela RSA em 1991
- » MD5 proposto em 1991 por Rivest (MD4)
- » Difícil de se provar o nível de segurança
- » MD5 roda 30% mais lento que MD4
- » MD4 e MD5 geram valor *hash* de 128 bits
- » Vulnerabilidade:
 - Como o MD5 faz apenas uma passagem sobre os dados, se dois prefixos com o mesmo hash forem construídos, um sufixo comum pode ser adicionado a ambos para tornar uma colisão mais provável. Deste modo é possível que duas strings diferentes produzam o mesmo hash.
- » Exemplo
 - MD5("The quick brown fox jumps over the lazy dog")
9e107d9d372bb6826bd81d3542a419d6
 - MD5("The quick brown fox jumps over the lazy **c**og") =
1055d3e698d289f2af8663725127bd4b

Hash SHA

- » Surgiu em 1993, considerado sucessor do MD5
- » Grande variedade de aplicações: TLS, SSL, PGP, SSH, IPSec, etc.
- » Também possui vulnerabilidade

Hash

SHA: Variações

Algoritmo	Tamanho de saída (bits)	Tamanho dos blocos (bits)	Comprimento (bits)	Tamanho das palavras (bits)
SHA-0	160	160	64	32
SHA-1	160	160	64	32
SHA-256/224	256/224	512	64	32
SHA-512/384	512/384	1024	128	64

- Exemplos

- SHA1("The quick brown fox jumps over the lazy dog") = 2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12
- SHA1("The quick brown fox jumps over the lazy cog") = de9f2c7f d25e1b3a fad3e85a 0bd17d9b 100db4b3

Hash

Comparação entre MD5 e SHA

- » Pertencem a mesma família de Funções Hash: MDx-class;
- » MD5 é mais vulnerável a ataques de força-bruta devido a sua menor saída: 128 bits contra 160 bits do SHA;
- » O MD5 é mais rápido que o SHA, pois este último possui mais etapas em seu algoritmo (80 contra 64 do MD5) e um buffer maior (160 bits contra 128 bits do MD5);
- » Já foram encontradas colisões para a função de compressão do MD5, enquanto que o SHA permanece inabalável.

Hash

Ataques

» Ataque de inversão: encontrar uma inversão.

- Probabilidade: $1/2^n$.
- Quantidade de operações: 2^n

» Ataque de aniversário:

- Num grupo de k pessoas, qual o valor mínimo de k para que a probabilidade de que pelos menos duas façam aniversário no mesmo dia seja maior do que 50%?
- $1 - 365 \times 364 \times \dots \times (365 - k + 1) / 365^k > 1/2 \Rightarrow \mathbf{k = 23}$
- - Considerando k entradas e $m = 2^n$ possíveis saídas, qual o valor de k para que a probabilidade de colisão seja maior do que 50%?
- $1 - m! / [(m-k)! m^k] \approx 1 - e^{-k(k-1)/n} > 1/2 \Rightarrow \mathbf{k \approx m^{1/2} = 2^{n/2}}$

Exercícios

Exercícios

No âmbito da criptografia assimétrica, considere a seguinte situação:

João enviou, a partir de uma rede TCP/IP conectada por *HUB*, uma mensagem assinada digitalmente e com criptografia para Maria. Uma determinada estação dessa rede estava com sua interface *Ethernet* em modo promíscuo, tornando possível Luís, detentor da chave pública de Maria, farejar todos os pacotes enviados por João. A partir dessas informações, assinale a afirmação correta.

- (A) Luís pode alterar as mensagens enviadas a Maria, preservando a integridade.
- (B) Luís pode descriptografar a mensagem enviada a Maria.
- (C) João utilizou a chave pública de Maria para criptografar a mensagem.
- (D) João utilizou sua própria chave privada na encriptação da mensagem.
- (E) Maria confirmou a assinatura da mensagem a partir de sua própria chave privada.

Exercícios

No âmbito da criptografia assimétrica, considere a seguinte situação:

João enviou, a partir de uma rede TCP/IP conectada por *HUB*, uma mensagem assinada digitalmente e com criptografia para Maria. Uma determinada estação dessa rede estava com sua interface *Ethernet* em modo promíscuo, tornando possível Luís, detentor da chave pública de Maria, farejar todos os pacotes enviados por João. A partir dessas informações, assinale a afirmação correta.

- (A) Luís pode alterar as mensagens enviadas a Maria, preservando a integridade.
- (B) Luís pode descriptografar a mensagem enviada a Maria.
- (C) João utilizou a chave pública de Maria para criptografar a mensagem.**
- (D) João utilizou sua própria chave privada na encriptação da mensagem.
- (E) Maria confirmou a assinatura da mensagem a partir de sua própria chave privada.

Exercícios

Que algoritmo de criptografia simétrica foi escolhido como padrão AES (Advanced Encryption Standard)?

- (A) RSA
- (B) 3DES
- (C) Rijndael
- (D) Blowfish
- (E) Diffie-Hellman

Exercícios

Que algoritmo de criptografia simétrica foi escolhido como padrão AES (Advanced Encryption Standard)?

- (A) RSA
- (B) 3DES
- (C) Rijndael**
- (D) Blowfish
- (E) Diffie-Hellman

Exercícios

Um conjunto de algoritmos de criptografia simétrica é:

- (A) DSA, MD5, IDEA e SHA-256.
- (B) RSA, SERPENT, DES e RC4.
- (C) RIJNDAEL, IDEA, Blowfish e RC5.
- (D) MD5, DES, RC5 e 3DES.
- (E) Diffie-Hellman, IDEA, Blowfish e RC4.

Exercícios

Um conjunto de algoritmos de criptografia simétrica é:

(A) DSA, MD5, IDEA e SHA-256.

(B) RSA, SERPENT, DES e RC4.

(C) RIJNDAEL, IDEA, Blowfish e RC5.

(D) MD5, DES, RC5 e 3DES.

(E) Diffie-Hellman, IDEA, Blowfish e RC4.

Exercícios

A força do algoritmo RSA é baseada na

- (A) impossibilidade de se quebrar o algoritmo SHA-1 em tempo computacionalmente viável.
- (B) dificuldade de implementação de um algoritmo eficiente para fatoração de números grandes.
- (C) dificuldade de implementação de um algoritmo eficiente para determinar a primalidade de um número.
- (D) obscuridade do algoritmo de geração do par de chaves assimétricas, que varia de acordo com a implementação.
- (E) utilização de números complexos, fortemente aleatórios, na geração da chave simétrica.

Exercícios

A força do algoritmo RSA é baseada na

- (A) impossibilidade de se quebrar o algoritmo SHA-1 em tempo computacionalmente viável.
- (B) dificuldade de implementação de um algoritmo eficiente para fatoração de números grandes.**
- (C) dificuldade de implementação de um algoritmo eficiente para determinar a primalidade de um número.
- (D) obscuridade do algoritmo de geração do par de chaves assimétricas, que varia de acordo com a implementação.
- (E) utilização de números complexos, fortemente aleatórios, na geração da chave simétrica.

Exercícios

Um desenvolvedor deseja utilizar um algoritmo de hash em seu sistema WEB. O algoritmo a ser utilizado será

- (A) Diffie-Hellman
- (B) SHA-256
- (C) telnet
- (D) ICMP
- (E) SSL

Exercícios

Um desenvolvedor deseja utilizar um algoritmo de hash em seu sistema WEB. O algoritmo a ser utilizado será

(A) Diffie-Hellman

(B) SHA-256

(C) telnet

(D) ICMP

(E) SSL

Exercícios

Sejam:

H1 o algoritmo SHA-256

H2 o algoritmo MD5

E1 a *String* "Prova"

E2 a *String* "Cesgranrio"

S1 a saída de **H1** com entrada **E1**

S2 a saída de **H1** com entrada **E2**

M1 a saída de **H2** com entrada **E1**

M2 a saída de **H2** com entrada **E2**

Observe as seguintes afirmativas:

I - **S2** possui 5 bytes a mais do que **S1**;

II - **H1** com entrada **S1** gera **E1**;

III - **M1** e **M2** têm o mesmo tamanho.

Está(ão) correta(s) a(s) afirmativa(s):

(A) I, somente. (B) II, somente.

(C) III, somente. (D) I e III, somente.

(E) II e III, somente.

Exercícios

Sejam:

H1 o algoritmo SHA-256

H2 o algoritmo MD5

E1 a *String* “Prova”

E2 a *String* “Cesgranrio”

S1 a saída de **H1** com entrada **E1**

S2 a saída de **H1** com entrada **E2**

M1 a saída de **H2** com entrada **E1**

M2 a saída de **H2** com entrada **E2**

Observe as seguintes afirmativas:

I - **S2** possui 5 *bytes* a mais do que **S1**;

II - **H1** com entrada **S1** gera **E1**;

III - **M1** e **M2** têm o mesmo tamanho.

Está(ão) correta(s) a(s) afirmativa(s):

(A) I, somente. (B) II, somente.

(C) III, somente. (D) I e III, somente.

(E) II e III, somente.

Exercícios

Em geral, a infra-estrutura de chaves pública e privada (ICP) utiliza algoritmos para colocar uma assinatura em uma mensagem e para criptografar a mensagem. Um algoritmo utilizado para assinar e outro para criptografar uma mensagem, são:

- (A) MD5 e 3DES
- (B) RC4 e SHA-1
- (C) SHA-1 e MD5
- (D) RC4 e 3DES
- (E) 3DES e RC4

Exercícios

Em geral, a infra-estrutura de chaves pública e privada (ICP) utiliza algoritmos para colocar uma assinatura em uma mensagem e para criptografar a mensagem. Um algoritmo utilizado para assinar e outro para criptografar uma mensagem, são:

(A) MD5 e 3DES

(B) RC4 e SHA-1

(C) SHA-1 e MD5

(D) RC4 e 3DES

(E) 3DES e RC4

RSA

Fatores de
sucesso

Exemplos

Simétrica



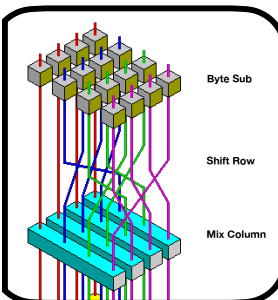
Senac

Híbrida

HELLO
+3 +3 +3 +3
KHOOR

Assimétrica

CRIPTOGRAFIA



Quântica

CRIPTOLOGIA

FORÇA BRUTA

