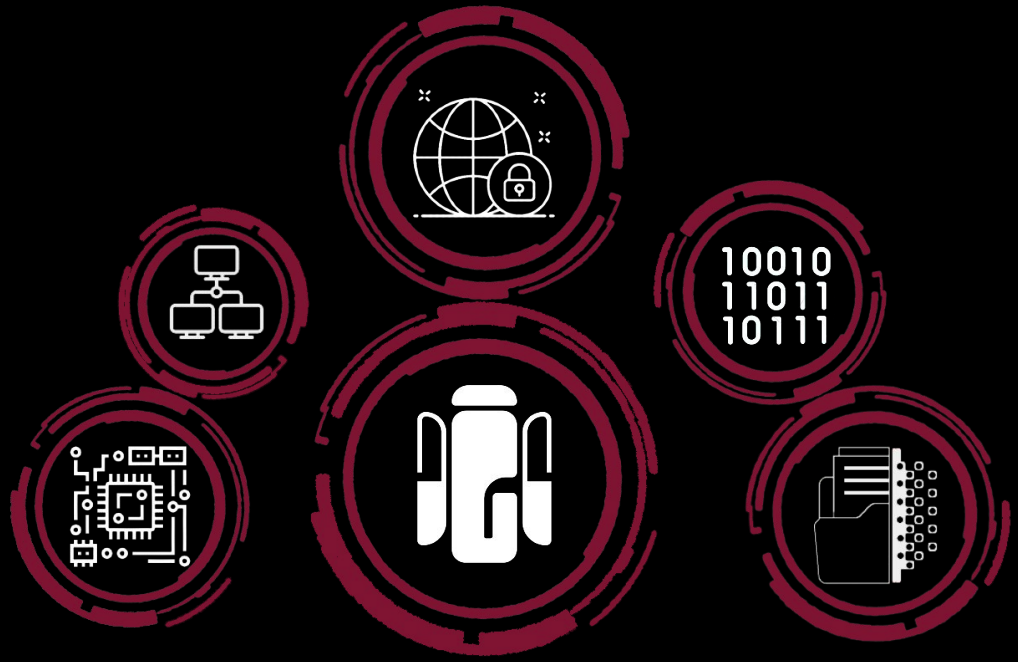
- GANESH -

Criptografia Moderna



- CRIPTO -

CODIFICAÇÃO VS ENCRIPTAÇÃO

Codificação vs Encriptação

Codificação:

- Transformar dados para que estes possam ser própria e convenientemente utilizados por diferentes tipos de sistema.

Encriptação:

- Transformar dados para que estes se tornem secretos. Ninguém consegue entendê-los, a não ser a pessoa para a qual a mensagem foi destinada.

Codificação

- Sistemas de numeração (bases numéricas)

Binário: {0,1}

Decimal: {0,1,2,3,4,5,6,7,8,9}

Hexadecimal: {0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F}

American Standard Code for Information Interchange (ASCII)

- 7-bits (0 a 127)
- Inteligente, mas limitada em vários casos

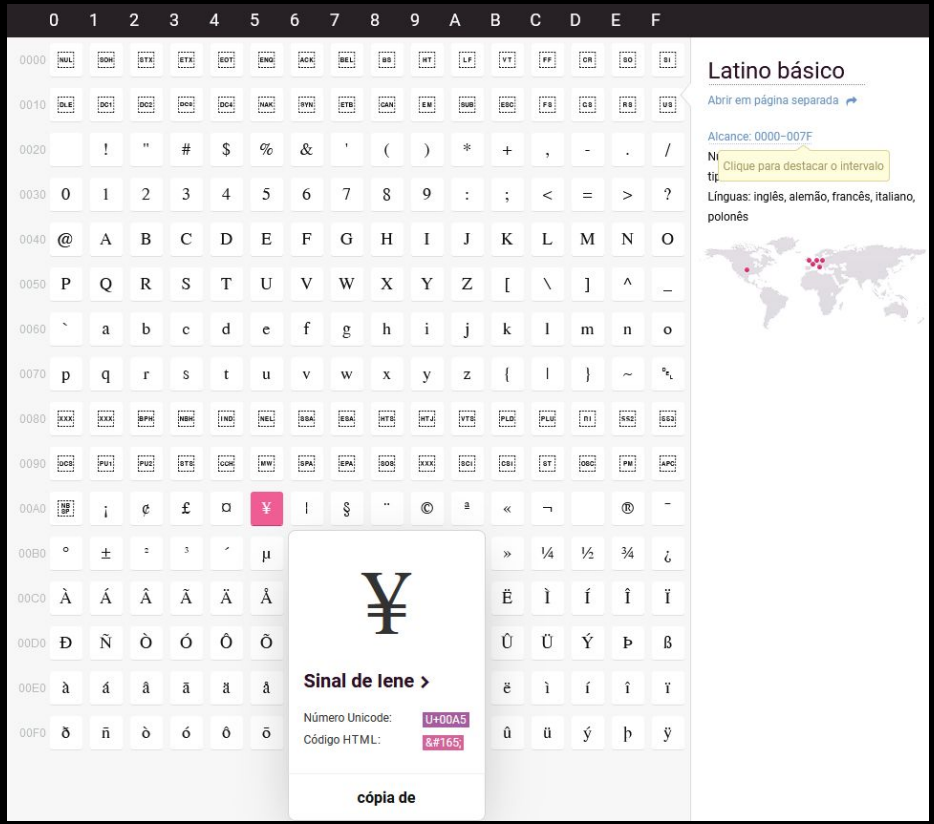
Comando Linux: man ascii

Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Unicode

- Padrão mundial de codificação de caracteres em computadores;
- Mais de 100 mil caracteres associados a números;
- Os símbolos não têm uma representação fixa (apenas 8, 16 ou 32 bits)



UTF-8 (Unicode Transformation Format - 8)

- Código multibyte mais usado
- Cada caractere Unicode é representado por uma sequência de 1 a 4 bytes (8 a 32 bits)
- https://www.ime.usp.br/~pf/algoritmos/apend/unicode.html

Character	Code Point (Unicode designation)	Encoding Form	Code Unit Sequence
M	U+004D	UTF-32	0000004D
		UTF-16	004D
		UTF-8	4D
A	U+0430	UTF-32	00000430
		UTF-16	0430
		UTF-8	D0 B0
	U+4E8C	UTF-32	00004E8C
		UTF-16	4E8C
		UTF-8	E4 BA 8C
	U+10302	UTF-32	00010302
		UTF-16	D800 DF02
		UTF-8	F0 90 8C 82

INTRODUÇÃO À CRIPTOGRAFIA MODERNA

Um pouco sobre Teoria da Informação

- Claude Shannon, 1948;
- *"A Mathematical Theory of Communication"*
- Marco da passagem da Criptografia Clássica para a Criptografia Moderna;
- Algoritmos desenvolvidos para serem utilizados por computadores: a informação é decodificada em cadeias de bits

Motivações para a Criptografia Moderna

Na criptografia clássica...

- Padrões na encriptação facilmente descobertos;
- Ataques estatísticos facilmente realizados. Exemplo: Carta do PCC;

Motivações para a Criptografia Moderna

Na criptografia moderna temos...

- Confidencialidade, Integridade, Autenticidade e Não-Repúdio

ONE TIME PAD (OTP)

One Time Pad

- Algoritmo criptográfico
- O funcionamento do algoritmo tem como base a função XOR (ou exclusivo)
- Critérios para a chave: única, randômica e pelo menos do tamanho do plaintext , ou seja, $|k| \geq |m|$.
- Perfect Secrecy

XOR

^, ⊕

Propriedades do XOR (ou exclusivo)

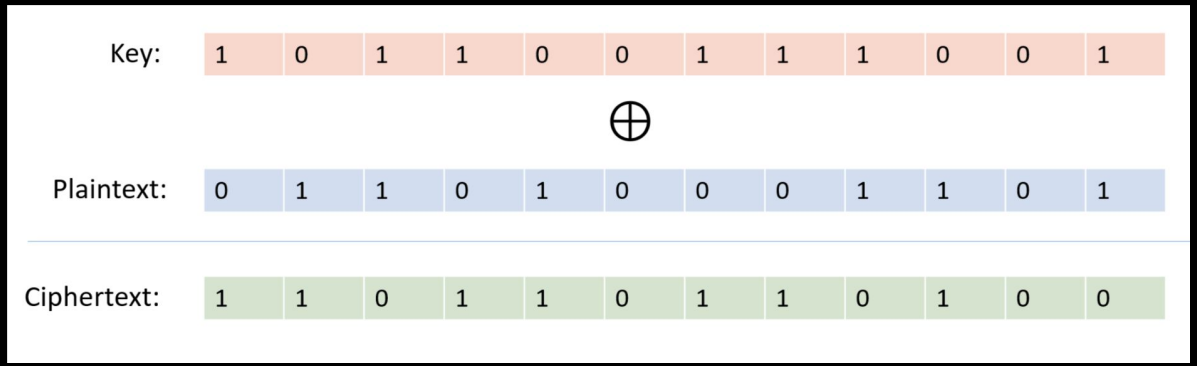
- Comutativa: $A \oplus B = B \oplus A$
- Associativa: $A \oplus (B \oplus C) = (A \oplus B) \oplus C$
- Identidade: $A \oplus 0 = A$
- Auto-inversiva: $A \oplus A = 0$
- $A \oplus B = C \Leftrightarrow C \oplus B = A$ e $C \oplus A = B$

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

One Time Pad

Funcionamento do algoritmo

- Encriptação:
  - $E(k,m) = m \oplus k = c$
- Decriptação:
  - $D(k,c) = c \oplus k = m$
- $E(k,m)$ e $D(k,c)$ são determinísticos



Desvantagens do OTP

- Apesar de ser seguro é impraticável: As chaves são muito grandes
- Solução: Stream Ciphers

Curiosidade

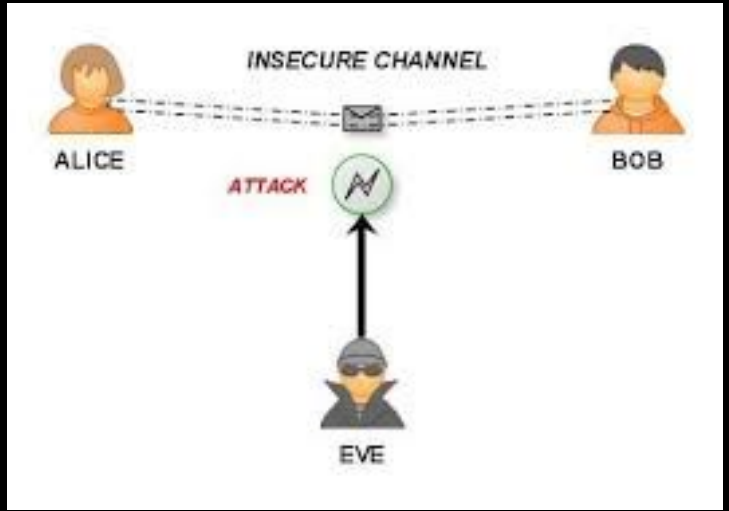
- A cifra OTP foi implementada no *Electronic Teleprinter Cryptographic Regenerative Repeater Mixer II* (ETCRRM II)
- Esse aparelho foi utilizado na comunicação entre os presidentes dos EUA e da Rússia (hotline)

BIT FLIPPING

Bit Flipping

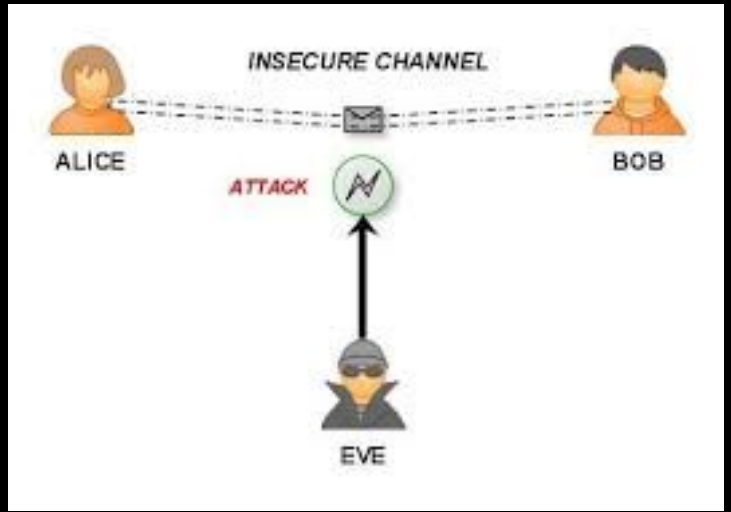
Caso simples

- Consiste em alterar o conteúdo do plaintext sem quebrar a cifra
  - Possuo $\mathbf{c_1 = m_1 \oplus k}$ (Mensagem original)
  - Desejo $\mathbf{c_2 = m_2 \oplus k}$ (Mensagem forjada)



Bit Flipping

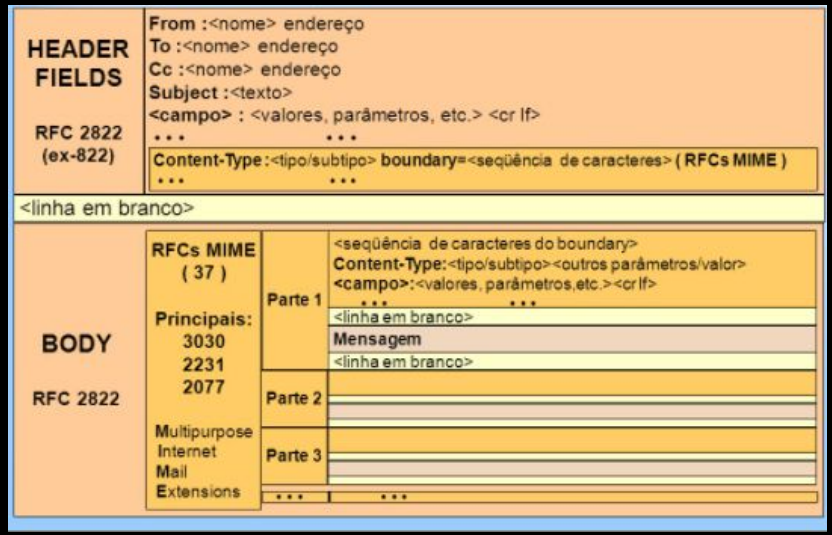
- Caso simples
  - Possuo $\mathbf{c_1 = m_1 \oplus k}$
  - Desejo $\mathbf{c_2 = m_2 \oplus k}$
- Assumindo que sei m_1, consigo achar c_2 fazendo
  - $\mathbf{m_1 \oplus m_2 \oplus c_1}$
- Pois isso é efetivamente
  - $\mathbf{m_1 \oplus m_2 \oplus m_1 \oplus k}$
  - $\mathbf{m_2 \oplus k}$



Bit Flipping

Outro caso

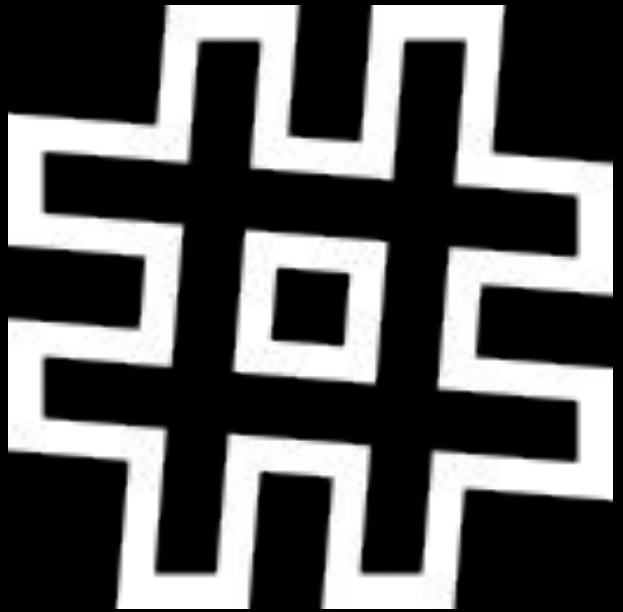
- O bit flipping também pode ocorrer quando sabemos apenas parte da mensagem original
- Isso é útil em mensagens de formato conhecido
  - Exemplo: protocolos públicos



Bit Flipping

Como evitar

- Utilizar mecanismos que assegurem a integridade da mensagem
  - MAC - *Message Authentication Code*
  - Assinaturas digitais



DEMONSTRAÇÃO

Modular conversion, encoding and encryption online


Kahoot!

STREAM CIPHERS

Stream Ciphers

- Visam tratar o problema da chave grande no OTP
- Contam com a função PRNG para gerar bits pseudo-aleatórios
- Úteis para proteger conexão bluetooth, redes móveis, conexões TLS etc

Stream Ciphers

- Entrada:
  - chave/semente (k) secreta
  - nonce (n) não necessariamente secreto
  - o par (k, n) deve ser único
- Saída:
  - Keystream (KS) pelo menos do tamanho da mensagem
  - $|KS| \geq |m|$

Stream Ciphers

Funcionamento do algoritmo

- Encriptação:
  - $E(k,n,m) = m \oplus PRNG(k,n) = c$
- Decriptação:
  - $D(k,n,c) = c \oplus PRNG(k,n) = m$

- $PRNG(k,n) = KS$
- $E(k,n,m)$, $D(k,n,c)$ e $PRNG(k,n)$ são determinísticos

Stream Ciphers modernas

Cifras orientadas a hardware

- Grain-128a
- A5/1(comunicação por voz)

Cifras orientadas a software

- SNOW3G
- ZUC
- RC4
- Salsa20

Stream Ciphers modernas

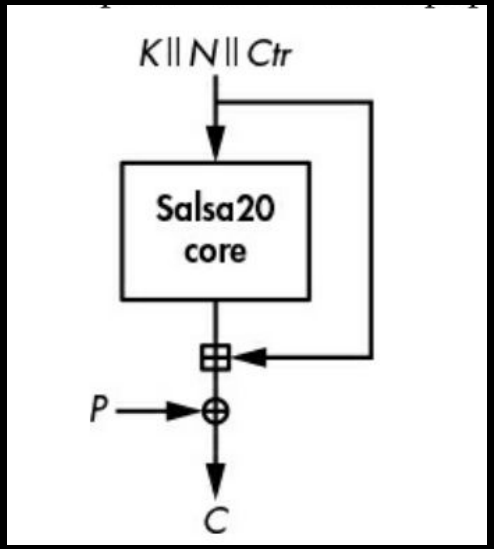
RC4 (Rivest Cipher 4)

- Aplicações mais conhecidas:
  - WEP (Wireless Equivalent Privacy)
  - TLS (Transport Layer Security)
- Não é seguro o suficiente

Stream Ciphers modernas

Salsa20

- Variante mais conhecida: Chacha
- Baseada em contador (Ctr)
- Gera a Keystream processando repetidamente o contador incrementado para cada bloco



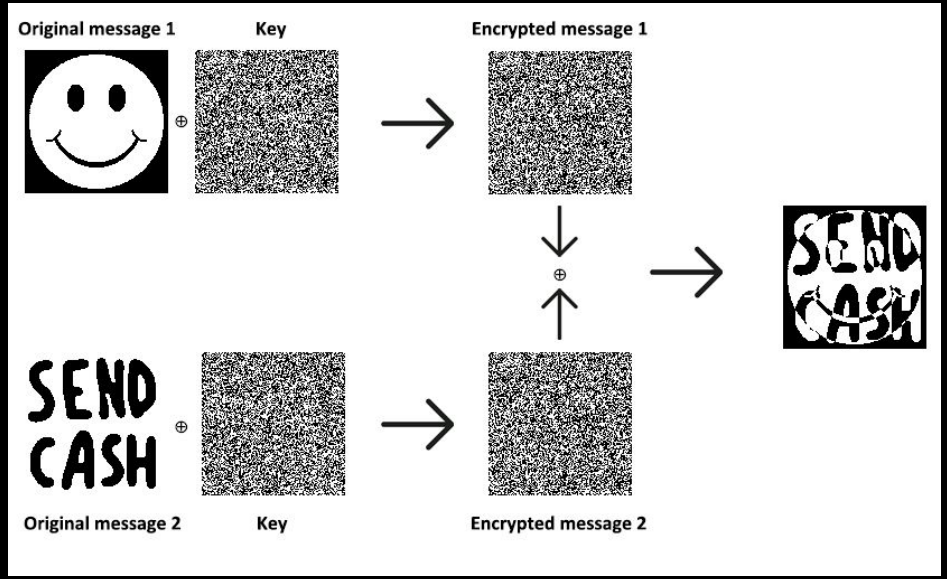
Fonte: Serious Cryptography book

- MANY TIME PAD-

Many Time Pad

Definição

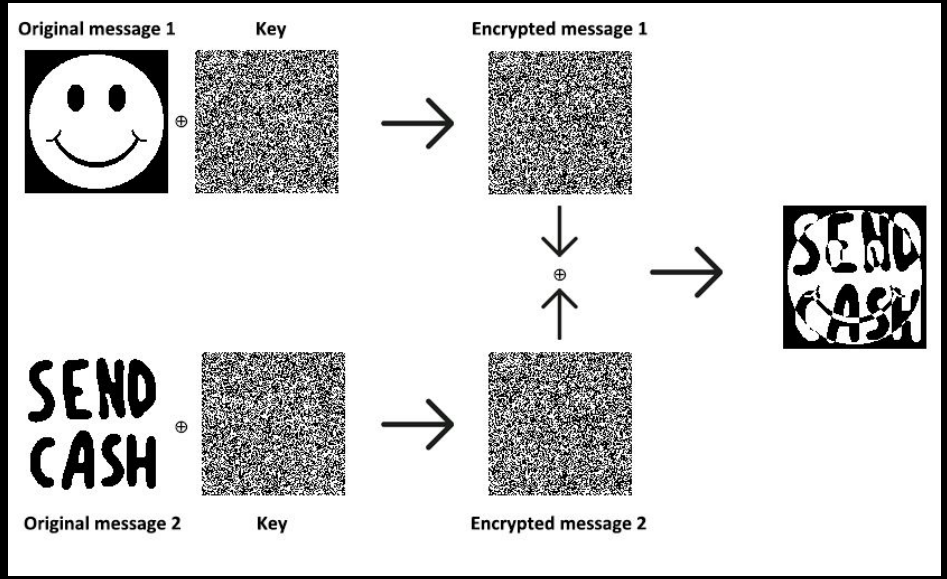
- Many time pad ocorre quando a mesma chave é usada várias vezes
  - $c_1 = m_1 \oplus k$
  - $c_2 = m_2 \oplus k$
  - $c_3 = m_3 \oplus k$ ...



Many Time Pad

Definição

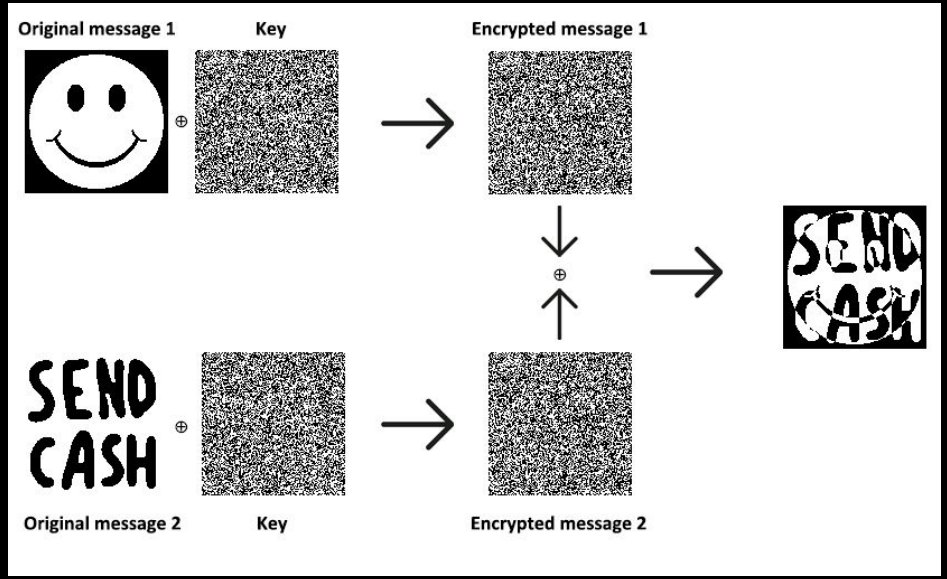
- Many time pad ocorre quando a mesma chave é usada várias vezes
  - $c_1 = m_1 \oplus k$
  - $c_2 = m_2 \oplus k$
  - $c_3 = m_3 \oplus k$ ...
- Permite descobrir coisas sobre o texto ao fazer
  - $c_1 \oplus c_2 = m_1 \oplus m_2$



Many Time Pad

Exemplos

- Esse erro ocorre com mais frequência do que se imagina!
  - Windows NT - protocolo PPTP (comunicação com servidores)
  - WEP (protocolo wireless)
  - Encriptação de arquivos em disco



Many Time Pad - crib

Ataque crib

- Dado duas ou mais mensagens encriptadas com a mesma chave, do tipo $\mathbf{c_1 = m_1 \oplus k}$, $\mathbf{c_2 = m_2 \oplus k}$ ...
- Podemos achar o XOR resultante de duas mensagens fazendo $\mathbf{c_1 \oplus c_2 = m_1 \oplus m_2}$
- Se sabemos uma parte de m_1, podemos achar uma parte correspondente de m_2.

Many Time Pad - crib

Ataque crib

- https://toolbox.lotusfa.com/crib_drag/

Many Time Pad - Spaces

Tabela ASCII

- Espaço = 32 = (0010 0000)
- [A-Z] = [65-90] = (010x xxxx)
- [a-z] = [97-122] = (011x xxxx)

Many Time Pad - Spaces

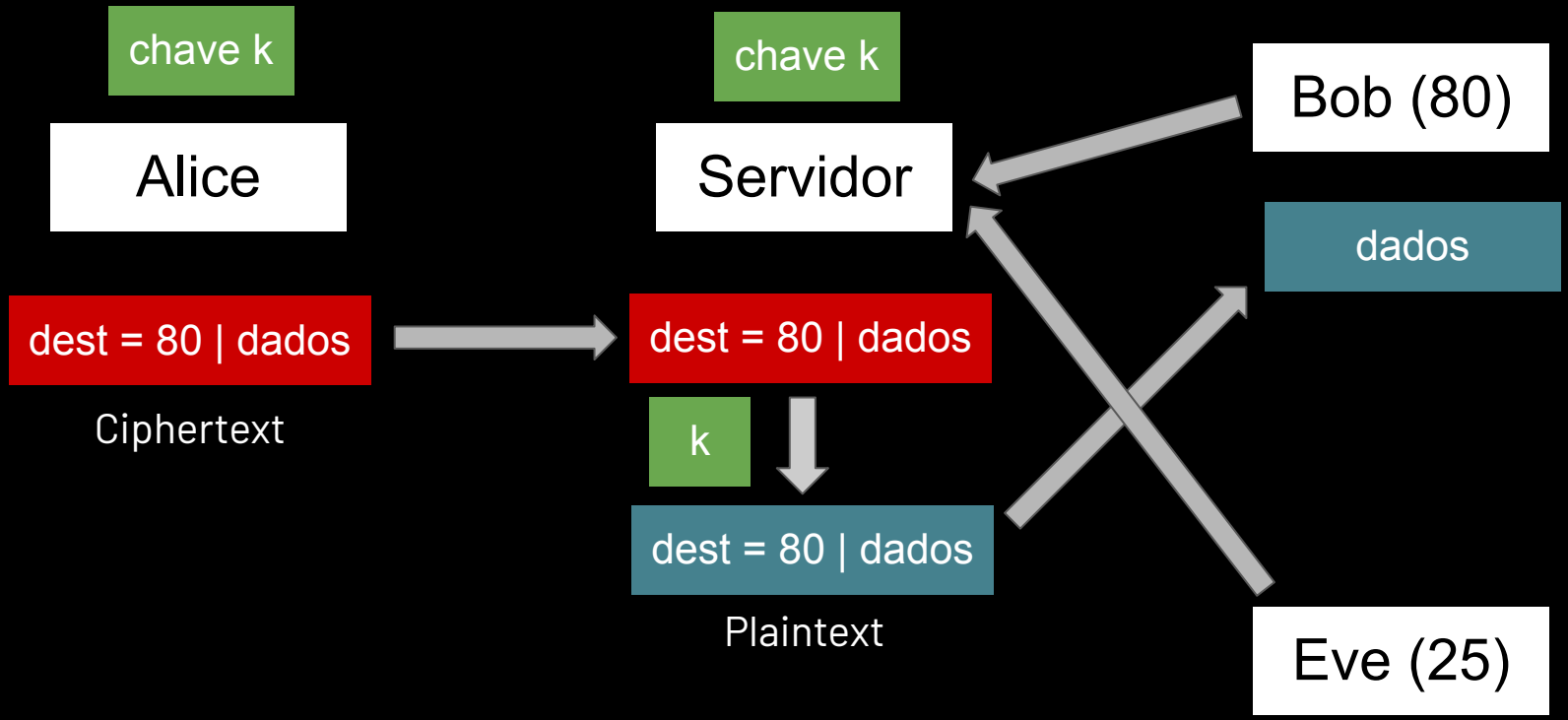
Tabela ASCII

- Ninguem pode ser sabio de estomago vazio.
- Quem eh que quer flores depois de morto?
- Viver eh negocio muito perigoso.
- nao ha regra sem excecao

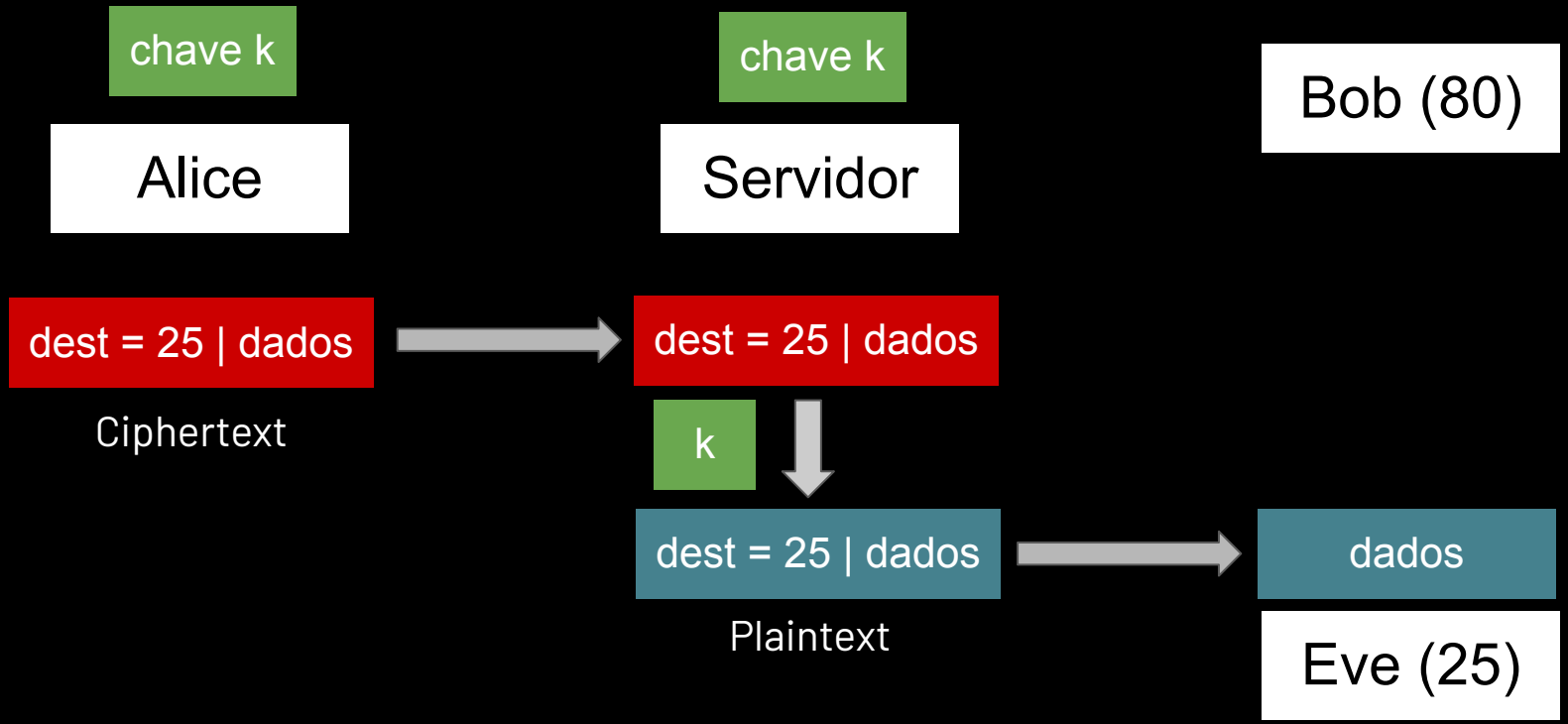

Kahoot!

INTEGRIDADE E AUTENTICAÇÃO

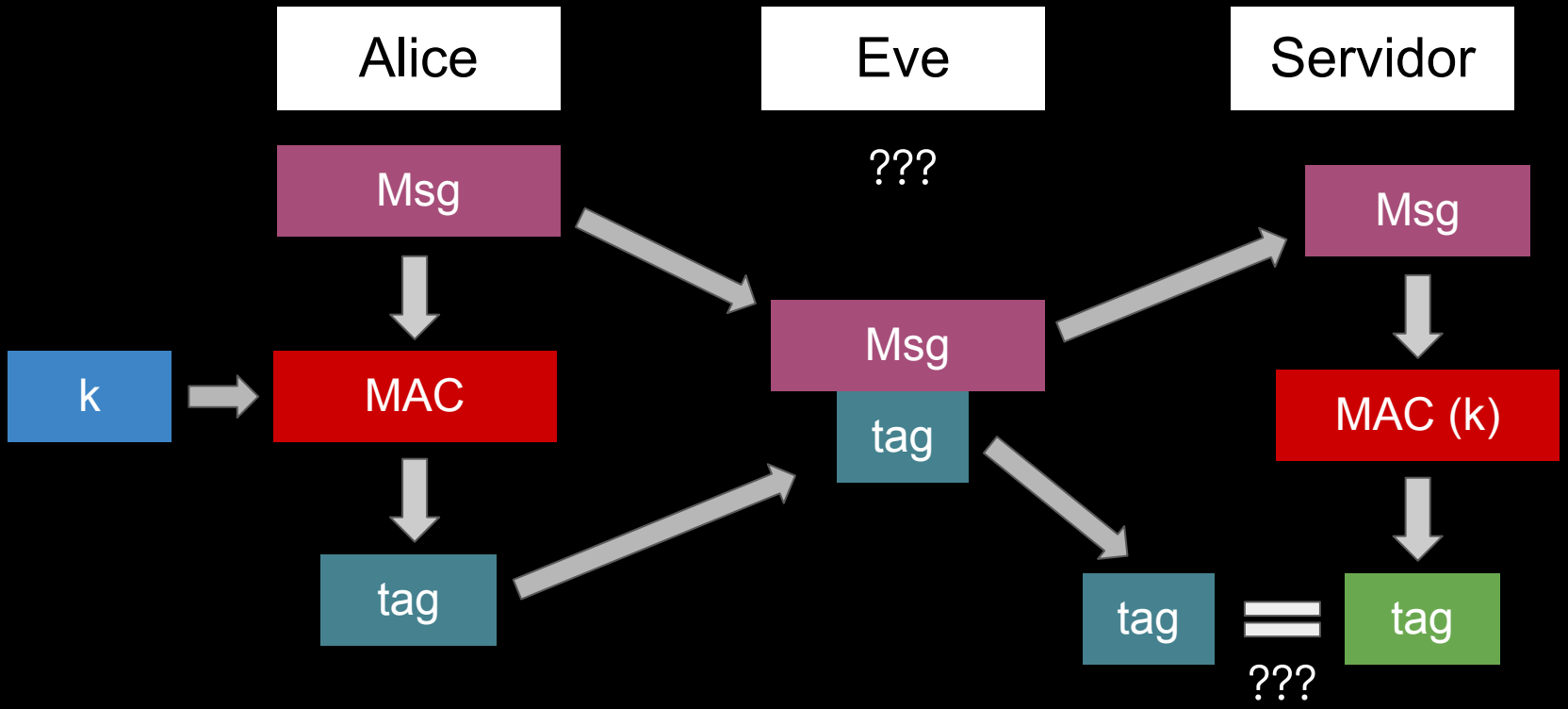
Motivação


chave k
Alice
dest = 80 | dados
Ciphertext
chave k
Servidor
dest = 80 | dados
k
dest = 80 | dados
Plaintext
Bob (80)
dados
Eve (25)

Motivação


chave k
Alice
chave k
Servidor
Bob (80)
dest = 25 | dados
Ciphertext
dest = 25 | dados
k
dest = 25 | dados
Plaintext
dados
Eve (25)

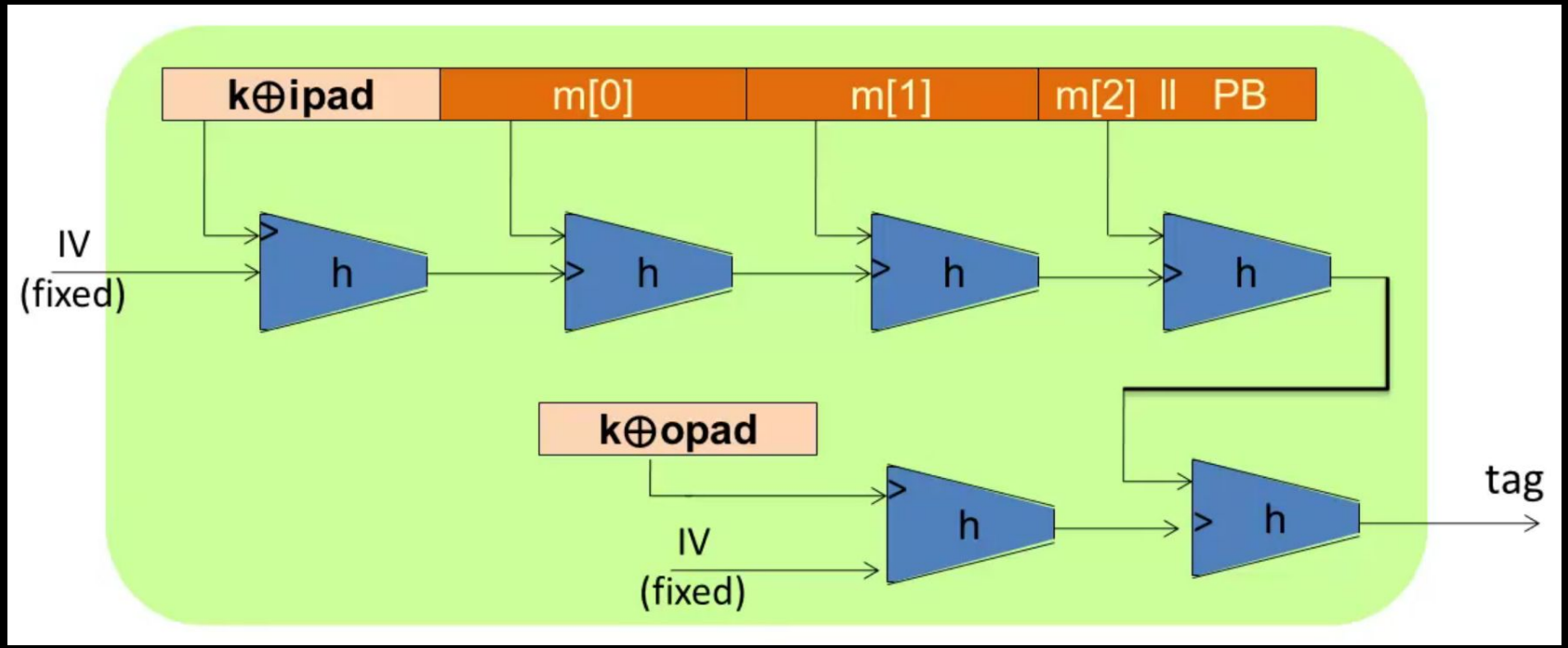
MAC - *Message Authentication Code*



MACs baseados em hash

- Função hash
  - $H: X \longrightarrow T$
  - X tam. variável, T tam. fixo
  - Ex: MD5, SHA128, SHA256...
- Funções resistentes a colisão
  - Inviável encontrar $m_1 \neq m_2 \Rightarrow H(m_1) = H(m_2)$
  - Distribuição uniforme
- MAC: hash + chave ⇒ tag

HMAC

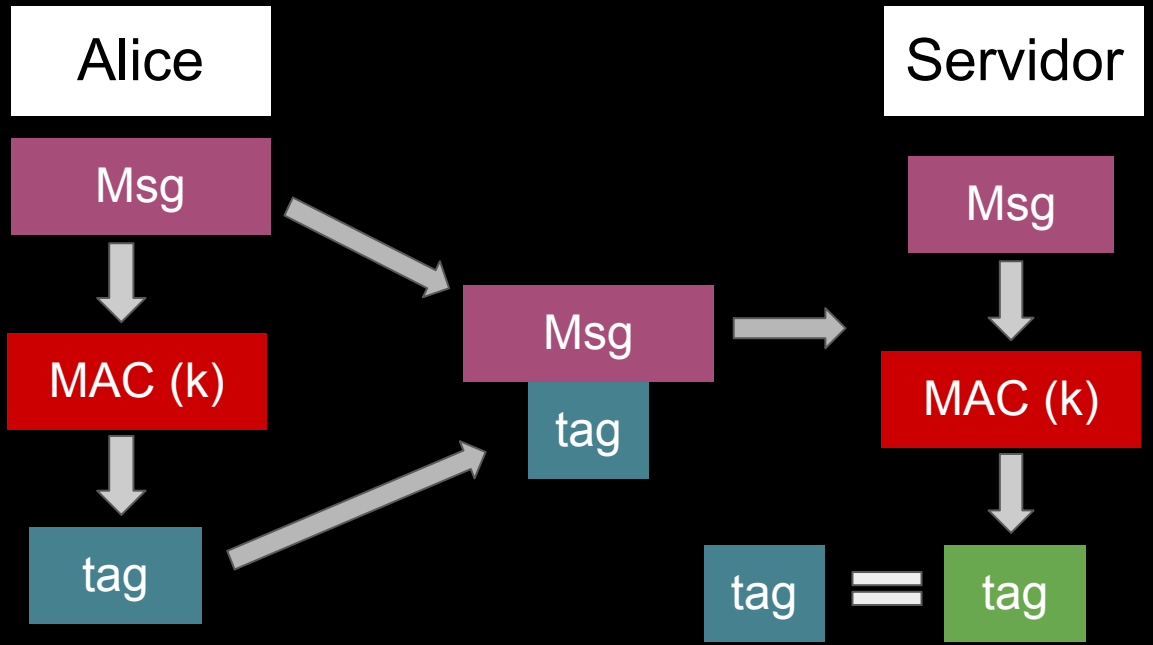


Fonte: https://www.coursera.org/learn/crypto

MACs

Garantias

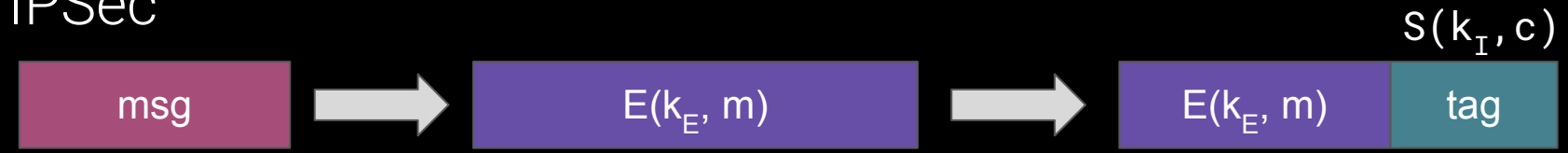
- Confidencialidade?
  - Não
- Integridade?
  - Sim
- Autenticidade?
  - Sim
- Não-repúdio?
  - Não



Encriptação Autenticada

k_I = chave mac k_E = chave enc.

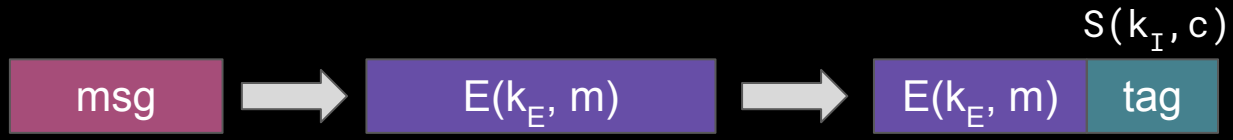
IPSec



Encriptação Autenticada

Garantias

- Confidencialidade?
  - Sim
- Integridade?
  - Sim
- Autenticidade?
  - Sim
- Não-repúdio?
  - Não
    - Assinaturas digitais



CRIPTOGRAFIA ASSIMÉTRICA

Criptografia Assimétrica

Motivação

- Compartilhamento de chaves secretas através de um canal inseguro
- Não-repúdio

Criptografia Assimétrica

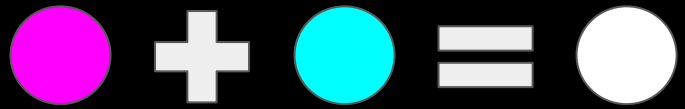
Conceitos

- Chave pública
  - É literalmente pública, todos têm acesso
- Chave privada
  - Somente o “dono” possui acesso
- Chaves diferentes ⇨ assimétricas!

Criptografia Assimétrica

Conceitos

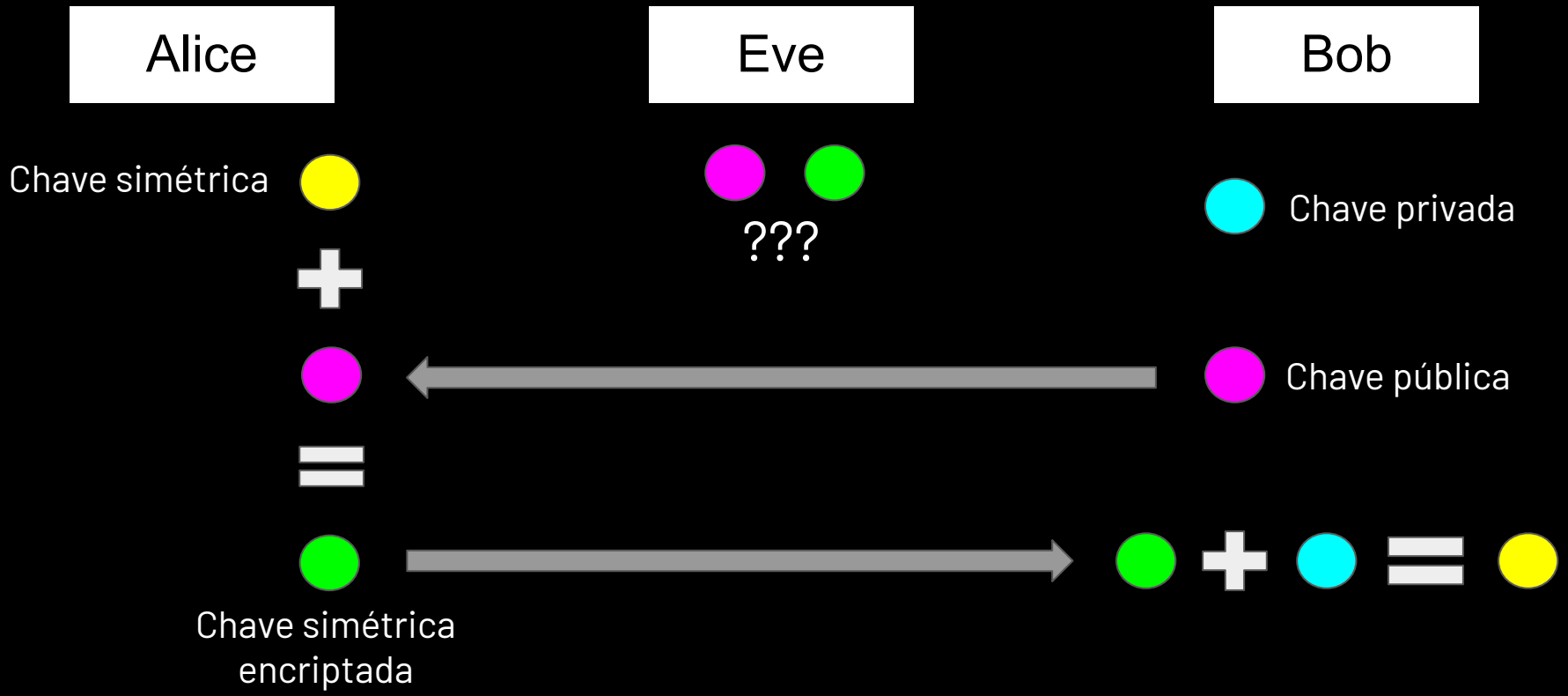
- Chave pública
- Chave privada



Plaintext + Chave pública = Ciphertext

Ciphertext + Chave privada = Plaintext

Troca de chaves

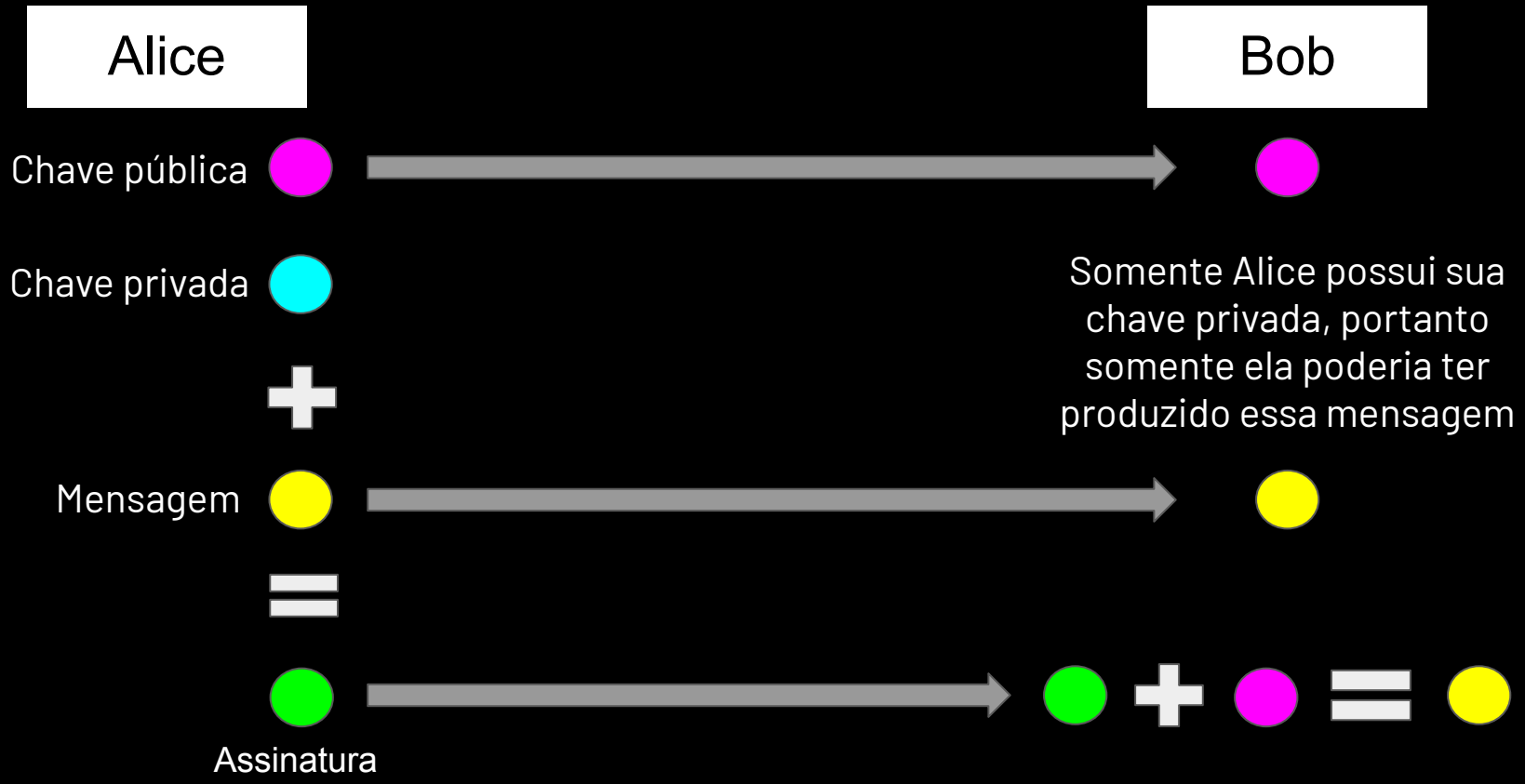


Criptografia Assimétrica

Simétrica vs Assimétrica

- Simétricas são mais rápidas e mais simples
  - Utilizamos assimétricas somente para troca de chaves
- Assimétricas permitem a construção de Assinaturas Digitais
  - Garantia de não-repúdio

Não-repúdio


Alice
Bob
Chave pública
Chave privada
Somente Alice possui sua chave privada, portanto somente ela poderia ter produzido essa mensagem
Mensagem
Assinatura


Kahoot!

CONTATO:

- ganesh.icmc.usp.br
- ganesh@icmc.usp.br

REDES SOCIAIS:

@ganeshICMC @ganeshicmc

GANESH

USP

ICMC USP SÃO CARLOS