

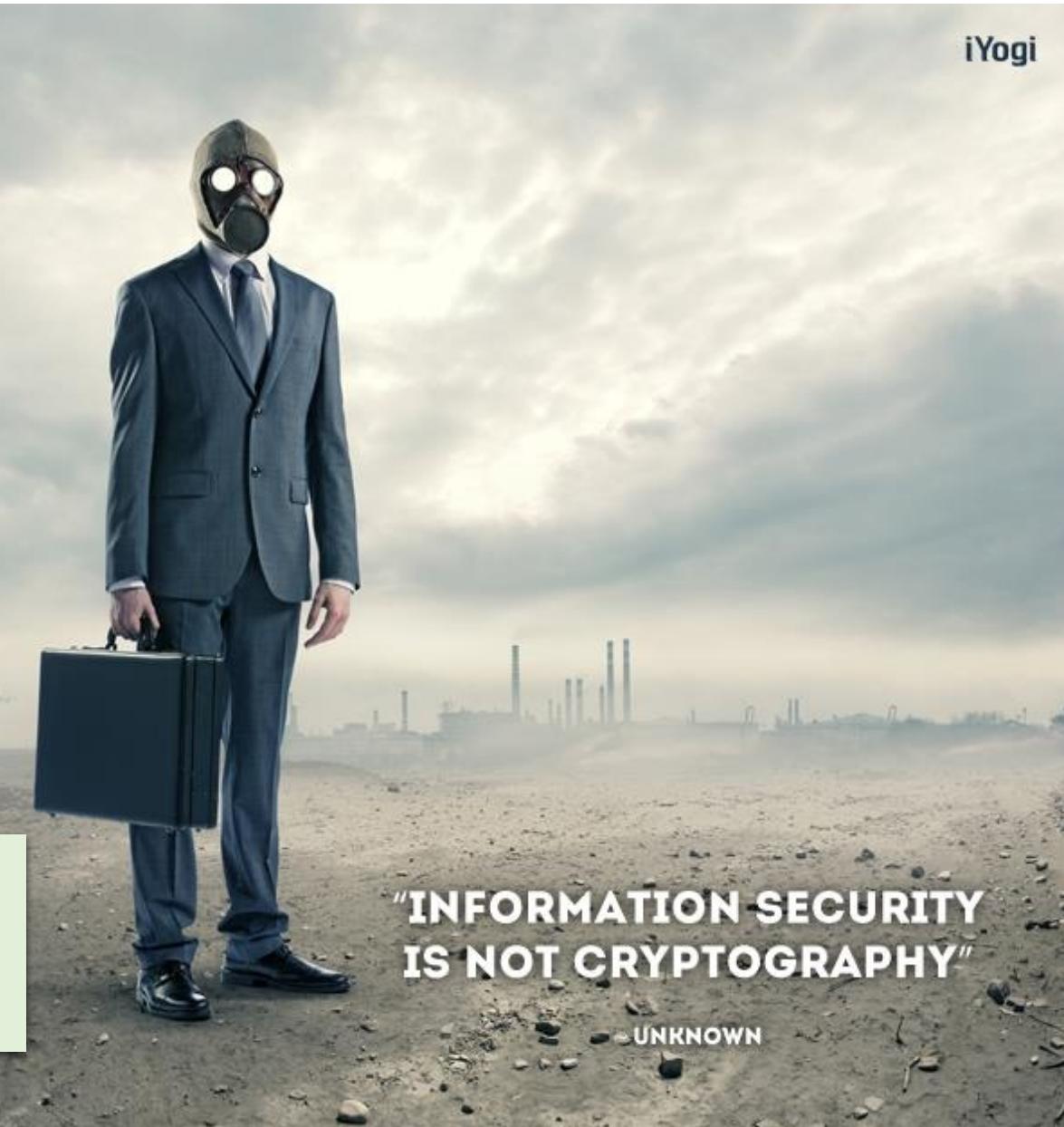
IMD0703 – Segurança de Redes

Introdução à Criptografia. Cifras Tradicionais e Modernas.





**“Segurança da Informação
não é Criptografia”** Desconhecido



Objetivo desta aula

- Geral
 - Contextualizar historicamente o desenvolvimento da criptografia, apresentando algumas das cifras tradicionais mais conhecidas
- Específicos
 - Conhecer os fundamentos da criptografia em um contexto histórico;
 - Entender os principais conceitos relacionados à criptografia tradicional;
 - Conhecer alguns métodos tradicionais de cifragem de mensagens.

Introdução

- A segurança de redes é assegurada, em grande parte, pelo uso de **criptografia**.
- Um Modelo Simplificado de Criptografia Convencional pode ser representado da seguinte forma:



Introdução

- A **Criptografia** é a ciência de escrever mensagens que ninguém deveria poder ler, exceto o remetente e o destinatário.
 - Palavra de origem grega:
 - kryptós= oculto/escondido + gráphei= escrita
 - Criptografia = ciência e arte de escrever oculto, em código
 - Muitas vezes, a criptografia é apresentada como um método de segurança da informação, o que é errado! O método, no caso, é o uso de um algoritmo criptográfico.
- A **Criptologia** é o estudo da escrita cifrada e se ocupa com a CRIPTOGRAFIA, a escrita secreta.



Introdução

- A **Criptoanálise** é a ciência de "quebrar" o método utilizado, decifrar e ler estas mensagens cifradas.
 - Toda cifra pode ser quebrada de alguma forma
 - Matematicamente Possível x Computacionalmente Seguro
 - Meios de criptoanálise
 - Força bruta: tentar todas as possibilidades de chaves ou cífras, seguido de comparações como o texto cifrado.
 - Mensagem conhecida: busca por padrões conhecidos.
 - Análise matemática e estatística.

Filme: "O Jogo da Imitação (The Imitation Game) - 2014"



Criptoanálise: Tipos de ataque sobre mensagens encriptadas

- **Apenas texto cifrado**
 - O criptoanalista deve conhecer a cifra e o texto cifrado.
- **Texto claro conhecido**
 - O criptoanalista deve conhecer a cifra, o texto cifrado e um ou mais pares de [texto claro, texto cifrado] produzidos pela chave secreta.
- **Texto claro escolhido**
 - O criptoanalista deve conhecer cifra, o texto cifrado e uma mensagem de texto claro escolhida pelo criptoanalista (com o respectivo texto cifrado, produzido pela chave secreta).
- **Texto cifrado escolhido**
 - O criptoanalista deve conhecer a cifra, o texto cifrado e um texto cifrado escolhido pelo criptoanalista (com o seu respectivo texto claro decriptado pela chave secreta).
- **Texto escolhido**
 - O criptoanalista deve conhecer a cifra, o texto cifrado, uma mensagem de texto claro escolhida pelo criptoanalista (com o respectivo texto cifrado, produzido pela chave secreta) e um texto cifrado escolhido pelo criptoanalista (com o seu respectivo texto claro decriptado pela chave secreta).

Histórico da Criptografia

- Para alguns autores, a criptografia teve origem com a simples ocultação da mensagem, também conhecida como esteganografia.
 - O termo estenografia tem origem nas palavras gregas *steganos*, que significa coberto, e *graphein*, que significa escrever.
- Um dos primeiros relatos acerca de escrita secreta data de 1900 a.C., e conta a história de Khnumhotep II, arquiteto do faraó Amenemhet II.
 - Os monumentos do faraó necessitavam ser documentados em tabuletas de argila.
 - Substituição de algumas palavras ou trechos de texto (hieróglifos?!).



A	禽	H	禽	N	一一	U	禽
B	口	I	口	O	口	V	口
C	一一	J	一一	P	口	W	禽
D	一一	K	一一	Q	一一	X	一一
E	一一	L	一一	R	一一	Y	一一
F	一一	S	一一	Z			
G	一一	M	一一	T	一一	SH	一一

Histórico da Criptografia

- Outros relatos antigos de escrita secreta são atribuídos a Heródoto, que escreveu as histórias e narrou os conflitos entre Grécia e Pérsia, ocorridos no século V a.C.
 - Uso de tabuletas de madeira cobertas de cera.
 - Mensagem tatuada na cabeça do mensageiro.
- Os antigos chineses escreviam suas mensagens em seda fina que era então amassada para formar uma pequena bola e coberta com cera.
 - Tal bolinha era engolida pelo mensageiro responsável pela entrega da mensagem.
- A esteganografia apresenta uma fraqueza fundamental.
 - O simples fato de a mensagem (ou mensageiro) ser interceptada é suficiente para que o conteúdo da mensagem possa ser obtido.
 - Por apenas ocultar o texto claro, a técnica de esteganografia não é reconhecida como criptografia.

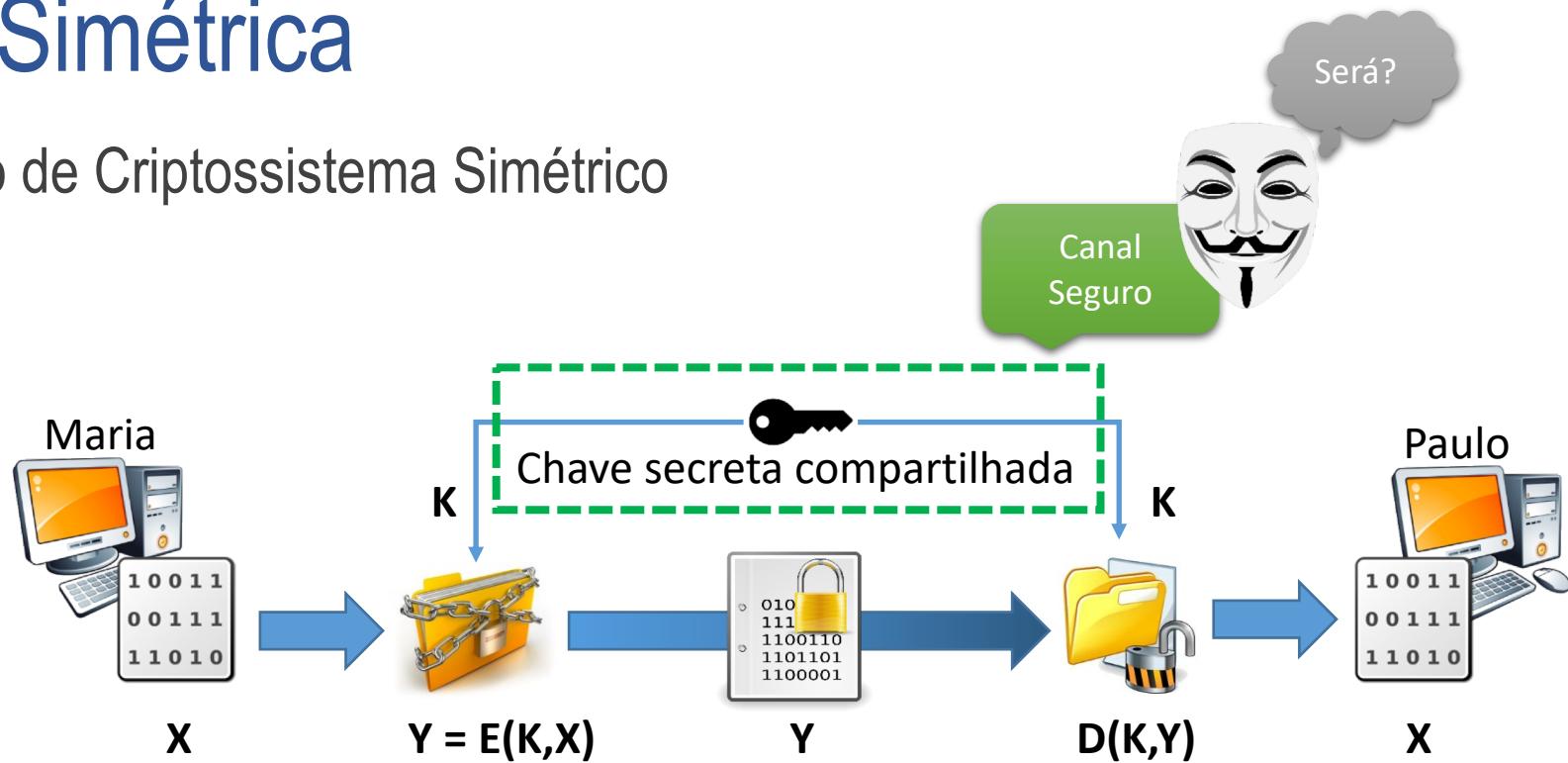


Modelos de Cifra

- Existem dois modelos de cifra
 - Cifra simétrica
 - A criptografia simétrica opera com a premissa de que a chave é de conhecimento unicamente do emissor e do receptor.
 - Cifra assimétrica
 - Na criptografia assimétrica, ou de chave pública, cada um dos usuários do meio criptográfico possui uma chave diferente, dividido em duas porções: a componente pública e a componente privada, cada uma gerando uma respectiva transformação.

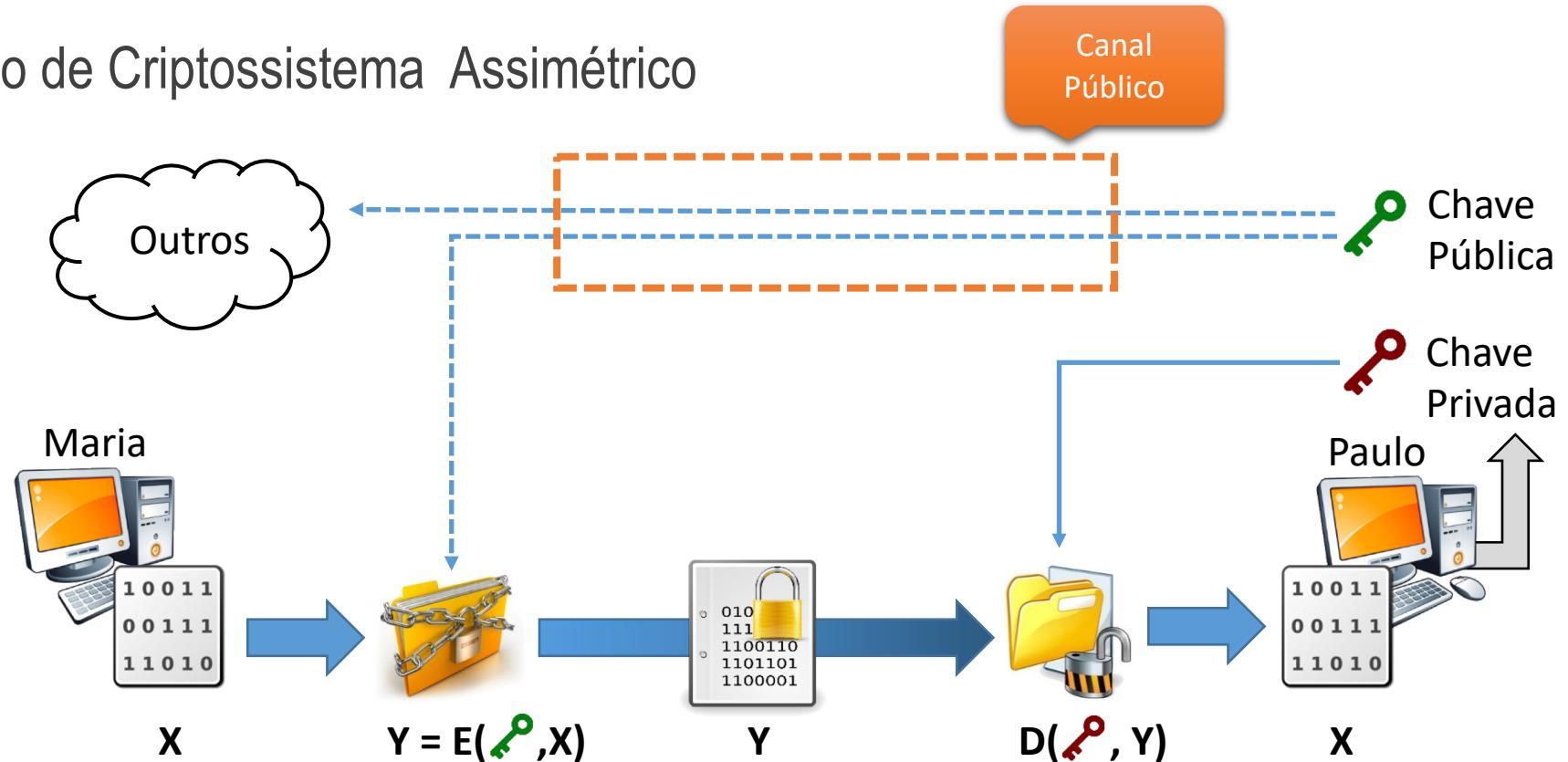
Cifra Simétrica

- Modelo de Criptossistema Simétrico



Cifra Assimétrica

- Modelo de Criptossistema Assimétrico



Modelo de Cifra Simétrica

- **Texto claro**
 - Mensagem original e inteligível.
 - Entrada para a Cifra.
 - **Cifra**
 - Algoritmo usado para encriptar ou decriptar o texto claro.
 - A cifra produzirá uma saída diferente para cada nova chave.
 - **Texto Cifrado**
 - É o texto claro transformado por uma cifra, ou seja, é a mensagem “embaralhada”.
 - Aparentemente aleatório e inteligível.
 - **Chave Secreta**
 - Um valor independente do texto claro e da cifra a ser usado na criptografia.
 - **Emissor e receptor**
-

A chave criptográfica

- O fato de que o número secreto (ou chave secreta) que funcionar da mesma maneira que uma chave convencional, faz aparecer o termo “chave”, para designar esse número secreto.
- Por que não criar um algoritmo que não necessite de uma chave?
 - O que é mais fácil: guardar um algoritmo em segredo ou guardar uma chave?
- A utilização de chaves para proteger segredos (dados), permite utilizar **diferentes chaves** para proteger **diferentes segredos**.
 - Assim, ainda que quebrem uma das chaves, os outros segredos ainda estarão seguros.
 - Sem as chaves, a quebra do algoritmo já revelaria todos os segredos.

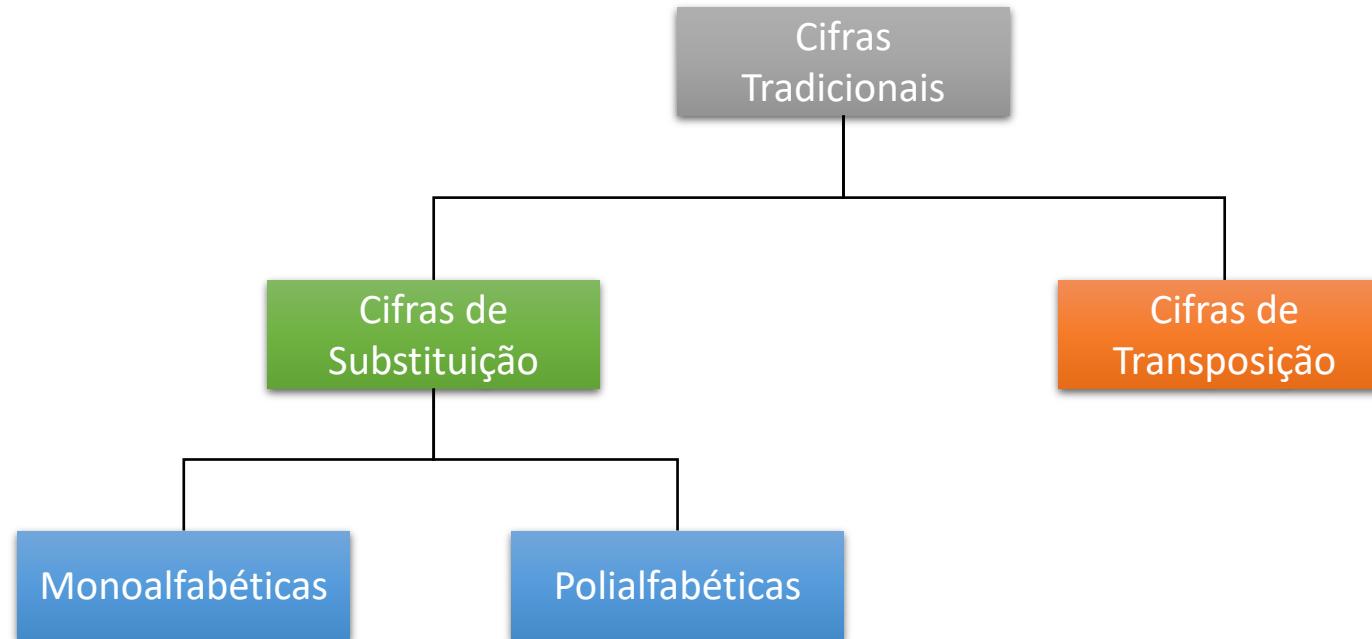
A chave criptográfica

- A idéia de que o criptoanalista conhece o algoritmo e que o segredo deve residir exclusivamente na chave é chamada Princípio de Kerckhoff (1883):
 - “**Todos os algoritmos devem ser públicos; apenas as chaves são secretas.**”
 - Princípios da Criptografia
 - **Princípio Criptográfico #1**
 - “Todas as mensagens criptografadas devem conter alguma redundância, ou seja informações que não são necessárias para a compreensão da mensagem.”
 - **Princípio Criptográfico #2**
- “Assegurar que cada mensagem criptografada recebida, possa ser confirmada como uma mensagem enviada muito recentemente, para evitar ataques de repetição por intrusos ativos que reutilizam mensagens válidas já enviadas.”

Modelo de Cifra Simétrica

- Existem dois requisitos para a utilização segura de encriptação simétrica:
 - Uso de uma **cifra** (algoritmo de encriptação) **forte**.
 - Emissor e receptor precisam ter obtido **cópias da chave secreta** de uma forma **segura** e mantê-la **protegida**.

Cifras Simétricas Tradicionais

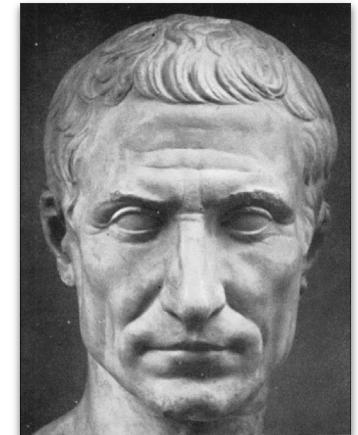
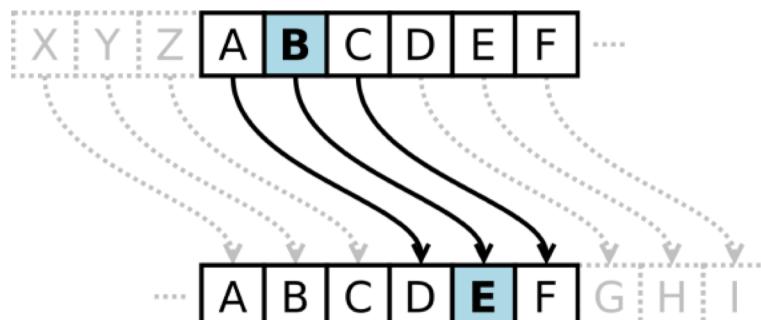


Cifras Tradicionais

- Cifras de Substituição
 - Substitui um símbolo por outro.
 - Monoalfabética: um caractere (ou símbolo) no texto claro sempre é modificado para o mesmo caractere (ou símbolo) no texto cifrado.
 - Facilita a análise estatística (ocorrência de caracteres da língua – quando conhecida).
 - Exemplo:
 - Texto Claro: SILVIO -> Texto Cifrado: WUVOUX
 - Polialfabética: cada ocorrência de um caractere pode ter um substituto diferente, dependendo de sua posição no texto original.
 - Exemplo:
 - Texto Claro: SILVIO -> Texto Cifrado: JBMKUY

Cifra de César

- Também conhecida como Cifra com Deslocamento, é atribuída ao imperador romano Júlio César que teria utilizado esta cifra em suas correspondências pessoais em 50 a.c.
 - Provavelmente, a cifra de substituição monoalfabética mais simples.
 - Os símbolos do alfabeto são deslocados “chave caracteres para cima” para encriptação e “chave caracteres para baixo” na decriptação.



Cifra de César

- Exemplo:
 - Texto Claro: SILVIO
 - Chave: 7 (alega-se que César usou o valor 3)
- Texto Cifrado: ZPSCPV
 - Exercício:
 - Parte 1: Usando a cifra de César com chave 11, cifre o **seu último nome** e entregue a um colega do lado.
 - Parte 2: Usando a mesma cifra de César com chave 11, revele o **último nome de seu colega** (confirme com ele!!!).

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	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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Cifra de César

- Para cifrar uma mensagem com chave 3:
 - $C = E(3,p) = (p+3) \text{ mod } 26$
- Generalização para qualquer chave k :
 - $C = E(k,p) = (p+k) \text{ mod } 26, k=1..25$
 - $p = D(k,C) = (C-k) \text{ mod } 26, k=1..25$
- Questão: Como realizar a criptoanálise por força bruta na Cifra de César?
 - A cifra é conhecida.
 - O espaço de chaves é pequeno (25 opções).
 - A linguagem do texto claro é conhecida e facilmente reconhecível.

Cifra de Vigenère

- Evolução da cifra de César
 - Provavelmente, a cifra de substituição polialfabética mais conhecida.
 - Usa uma série de cifras de César diferentes, baseado nas letras de uma chave secreta.
 - Originalmente descrita por Giovan Batista Belaso, em 1553.
- Reinventada diversas vezes depois, foi erroneamente atribuída a Blaise de Vigenère, já no século IXX como:
 - Le Chiffre Indéchiffrable

Cifra de Vigenère

- Exemplo:

- Texto Claro: SILVIO
- Chave: SENHA
- Texto cifrado: KMYCIG

- Generalização:

- Texto claro: $P = p_0, p_1, p_2, \dots, p_{n-1}$
- Chave (sequência de letras): $K = k_0, k_1, k_2, \dots, k_m$, $m < n$
- Encriptação: $C_i = (p_i + k_i \bmod m) \bmod 26$, $k=1..25$
- Decriptação: $p_i = (C_i - k_i \bmod m) \bmod 26$, $k=1..25$

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	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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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
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	
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z			
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z				
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z					
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z						
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z							
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z								
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z									
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z										
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z											
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z												
O	O	P	Q	R	S	T	U	V	W	X	Y	Z													
P	P	Q	R	S	T	U	V	W	X	Y	Z														
Q	Q	R	S	T	U	V	W	X	Y	Z															
R	R	S	T	U	V	W	X	Y	Z																
S	S	T	U	V	W	X	Y	Z																	
T	T	U	V	W	X	Y	Z																		
U	U	V	W	X	Y	Z																			
V	V	W	X	Y	Z																				
W	W	X	Y	Z																					
X	X	Y	Z																						
Y	Y	Z																							
Z	Z																								

Cifra de Vernam

- Usa a operação **XOR** (ou exclusivo, bit a bit) entre os bits da chave e do texto claro.
- Exige que o tamanho da chave seja tão longo quanto o texto claro e não deve possuir relação estatística com o mesmo.
 - Isso pode levar a repetições da chave.
 - Caso a chave não seja do mesmo tamanho os caracteres podem ser ciclicamente repetidos, mas isso introduzirá uma fraqueza à cifragem.
- Generalização:
 - Texto claro: P
 - Chave (sequência de letras): K
 - Encriptação: $C = (P \oplus K)$
 - Decriptação: $P = (C \oplus K_i)$

Cifra de Vernam

- Exemplo:

- Texto Claro: SILVIO
- Chave: SEGREDO
- Texto cifrado: AMNEMN

P	10010.01000.01011.10101.01000.01110
K	10010.00100.00110.10001.00100.00011.01110
XOR	-----
C	00000.01100.01101.00100.01100.01101

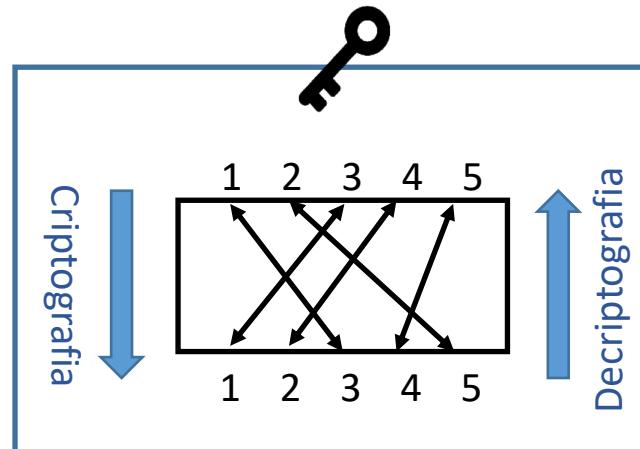
Alfabeto Codificado			
Letter	Bit sequence	Letter	Bit sequence
A	00000	Q	10000
B	00001	R	10001
C	00010	S	10010
D	00011	T	10011
E	00100	U	10100
F	00101	V	10101
G	00110	W	10110
H	00111	X	10111
I	01000	Y	11000
J	01001	Z	11001
K	01010	0	11010
L	01011	1	11011
M	01100	2	11100
N	01101	3	11101
O	01110	4	11110
P	01111	ESPAÇO	11111

One-time pad

- Um oficial do exército, Joseph Mauborgne, propôs uma melhoria na cifra de Vernam.
 - Uso de uma **chave aleatória**, tão grande quanto a mensagem.
 - Além disso, a chave deve ser usada para encriptar e decriptar **apenas uma vez**, e depois descartada
 - Produz uma saída que não possui qualquer relação estatística com o texto claro.
 - Considerável inquebrável (segredo perfeito).
 - Utilidade limitada:
 - Impraticabilidade em criar grandes quantidades de chaves aleatórias.
 - Aumenta o problema de distribuição destas chaves.

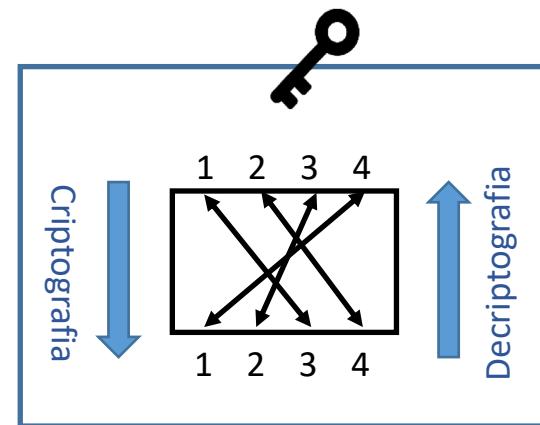
Cifras Tradicionais

- Cifras de Transposição
 - Reordena (permute) símbolos em um bloco de símbolos.
 - Diferente das cifras de substituição, estas cifras permuteam as posições dos símbolos.
 - Neste tipo de cifra a chave é uma associação entre a posição dos símbolos no texto claro e o texto cifrado.
 - A chave é aplicada em blocos de tamanho igual à chave (quanto mais longa a chave, mais eficaz a cifra).



Cifras Tradicionais

- Cifras de Transposição
 - Exemplo:
 - Texto Claro: SAMPAIO
 - Necessário preenchimento (para a aplicação da chave em bloco, o texto claro deve ter um tamanho múltiplo do tamanho da chave). Neste caso usaremos o caractere 9 para preenchimento na encriptação. Na decriptação, o caractere de preenchimento é removido.
 - Texto Claro após preenchimento: SAMPAIO9
 - Texto Cifrado: PMSA9OAI



Esteganografia

- Embora não seja considerado um método de encriptação, a esteganografia tem papel importante na história da ocultação de mensagens.
 - Técnica difundida entre espiões durante o período da Guerra Fria.
- Diversas técnicas podem ser utilizadas:
 - Marcação de caractere.
 - Tinta invisível.
 - Perfurações.
 - Fita corretiva de máquina de datilografar.

Cifras Tradicionais

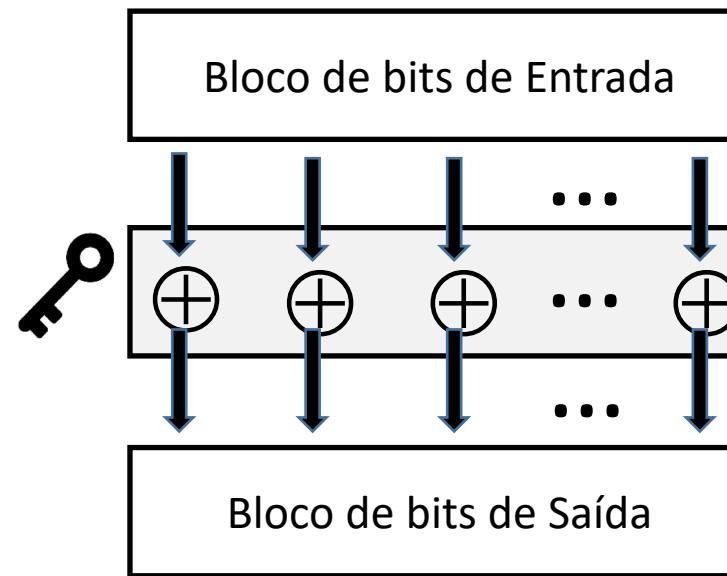
- Máquina de rotor
 - Envolve multiplas etapas de encriptação.
 - Consiste de um conjunto de cilindros rotativos independentes, através do qual pulsos elétricos podem fluir.
 - Cada cilindro possui 26 pinos de entrada e 26 de saída, com fiação interna que conecta cada pino de entrada a um único pino de saída.
 - Combinação para apenas 3 cilindros é de $26 \times 26 \times 26 = 17.576$.
 - A configuração com 5 cilindros é equivalente a uma cifra de Vigenère com um tamanho de chave de 11.881.376.
 - Esta técnica é considerada a inspiração para a cifra mais utilizada de todos os tempos: *Data Encryption Standard (DES)*.

Cifras modernas

- Enquanto as cifras tradicionais são orientadas a caracteres, as cifras modernas são orientadas a bits.
- Mensagens modernas assumem diferentes formatos, além de caracteres (números, imagem, áudio ou vídeo).
- Além disso, mesmo caracteres representados em bits, quando mesclados oferecem maior dificuldade para a criptologia.

Cifra XOR

- O tamanho do bloco de entrada (texto claro), chave e bloco de saída (texto cifrado) são iguais.
- Processos de Encriptação e Decriptação são iguais.



Cifra de Rotação

- Os bits de entrada são deslocados para a esquerda ou para a direita (de forma circular).
 - Com chave: o valor da chave define a quantidade de rotações.
 - Sem chave: o número de rotações é fixo.
- Pode ser considerado um caso especial da cifra com transposição (aplicado a bits em vez de caracteres).
- Por razões óbvias, o número de rotações (ou chave) deve estar entre 1 e $(N-1)$.

S-box e P-box

- S-box
 - Uma S-box (caixa de substituição) é o análogo da cifra de substituição para caracteres.
 - A entrada de uma S-box é um fluxo de bits de comprimento N.
 - A saída é outro fluxo de bits de mesmo tamanho N.
 - S-box não utilizam chave e são utilizados como um estágio intermediário de cifra.
- P-box
 - Uma P-box (caixa de permutação) é o análogo da cifra de transposição para caracteres.
 - Assim como as S-box, não utilizam chave e são utilizados como um estágio intermediário de cifra.

Cifras Cíclicas Modernas

- As cifras modernas são chamadas de cíclicas, pois envolvem vários ciclos
 - Cada ciclo funciona como uma cifra complexa, resultado da combinação das cifras simples descritas anteriormente.
 - A chave usada em cada ciclo é um subconjunto ou variação da chave geral (chave cíclica).
 - Se a cifra usar N ciclos, um gerador de chaves produz N chaves (K_1, K_2, \dots, K_N).
- Exemplos de cifras modernas: DES, 3DES, RC4, RC5, IDEA e AES.

Atividade Prática – Cifra de César

- 1. Implemente um programa de criptoanálise que utilize de força bruta para quebrar uma mensagem encriptada usando uma cifra de César tradicional.
 - A. Teste o seu programa com o algum colega (e vice-versa).
 - B. Utilize o seu programa para ajudar César com a mensagem a seguir (próximo slide).

Cifra de César

sSOHEX?LEJVPZHETHPZESPUKH

qHPZEJOLPHEKLENYHçH

iELSHGETLUPUH

u?LE,LTELEX?LEWHZZH

r?TEKVJLEIHSHUJV

eEJHTPUOVEKVETHY

qVçHEKVEJVYVWEKV?YHKV

hVEZVSEKLEMWHULTH

SEZL?EIHSUçHKVEéETHPZEX?LE?TEWLTH

ÉEHEJVPZHETHPZESPUKHEX?LEL?EQHE,PEWHZZHY

eOGEWVYEX?LELZ V?E HVEZVdPUOVF

eOGEWVYEX?LE ?KVELE HVE YPZ LF

eOGEHEILSLdHEX?LELbPZ L

eEILSLdHEX?LEUHVELEZVETPUOH

u?LE HTILTEWHZZHEZVdPUOH

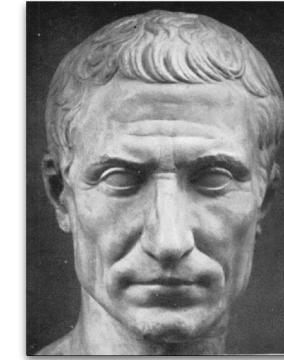
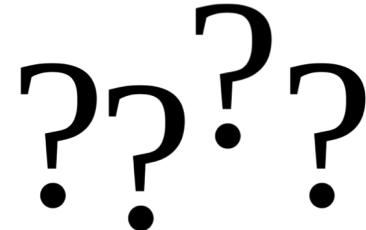
eOGEZLELSHEZV?ILZZL

u?LEX?HUKVELSHEWHZZH

SET?UKVEPU LPYPUOVEZLELUJOLEKLENYHJH

iEMPJHETHPZESPUKV

tVYEJH?ZHEKVEHTVY



Sabe-se apenas que foi utilizado o seguinte alfabeto:
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ ?,

Atividade Prática - Vigenère

- 2. Qual é a mensagem?

W gags domj a esgpi so eiu dm goze qnyjaaxa hikinq frmh tvkdea irvwfea eaee frmh peefoa se gvugw

Sabe-se que foi utilizado o alfabeto:

abcdefghijklmnopqrstuvwxyz

E uma senha/chave relacionada com o segredo que César descobriu.

Atividade Prática - Esteganografia

- 3. Escreva um programa que lê uma mensagem e a esconde em um arquivo de imagem no formato Bitmap (um dos formatos mais utilizados na esteganografia pelo fato de não possuir compactação) e outro que permita extrair a mensagem do arquivo novamente.
 - Técnica de ocultação: A cada 3 pixels da imagem, composto por 3 bytes cada (RGB), têm-se 9 bytes
 - Desses 9 bytes, pegar o bit menos significativo dos 8 primeiros e ocultar os bits de caractere da mensagem (char = 8 bits).
 - Testar se a imagem comporta a mensagem!
 - Detalhes do formato Bitmap pode ser aprendido em <http://tipsandtricks.runicsoft.com/Cpp/BitmapTutorial.html> ou numa simples consulta ao Google!
 - Teste o seu programa com o algum colega (e vice-versa).
 - Sugestão: Se funcionou, melhore o programa para ocultar um arquivo texto inteiro, passado por parâmetro.

Alguma Questão?

