

Criptografia & caos

Uma introdução a criptografia caótica

Prof. Dr. Odemir Martinez Bruno

Grupo de Computação Interdisciplinar
IFSC - USP

Criptografia

- Criptografia (Do Grego *kryptós*, "escondido", e *gráphein*, "escrita") é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade. (Wikipedia)

Criptografia

- Criptografia é a arte da escrita secreta e sua utilização é tão antiga quanto a própria escrita.
- A criptografia desempenhou um importante papel na história da humanidade, tendo definido a sorte de reis e rainha, batalhas e até mesmo guerras.

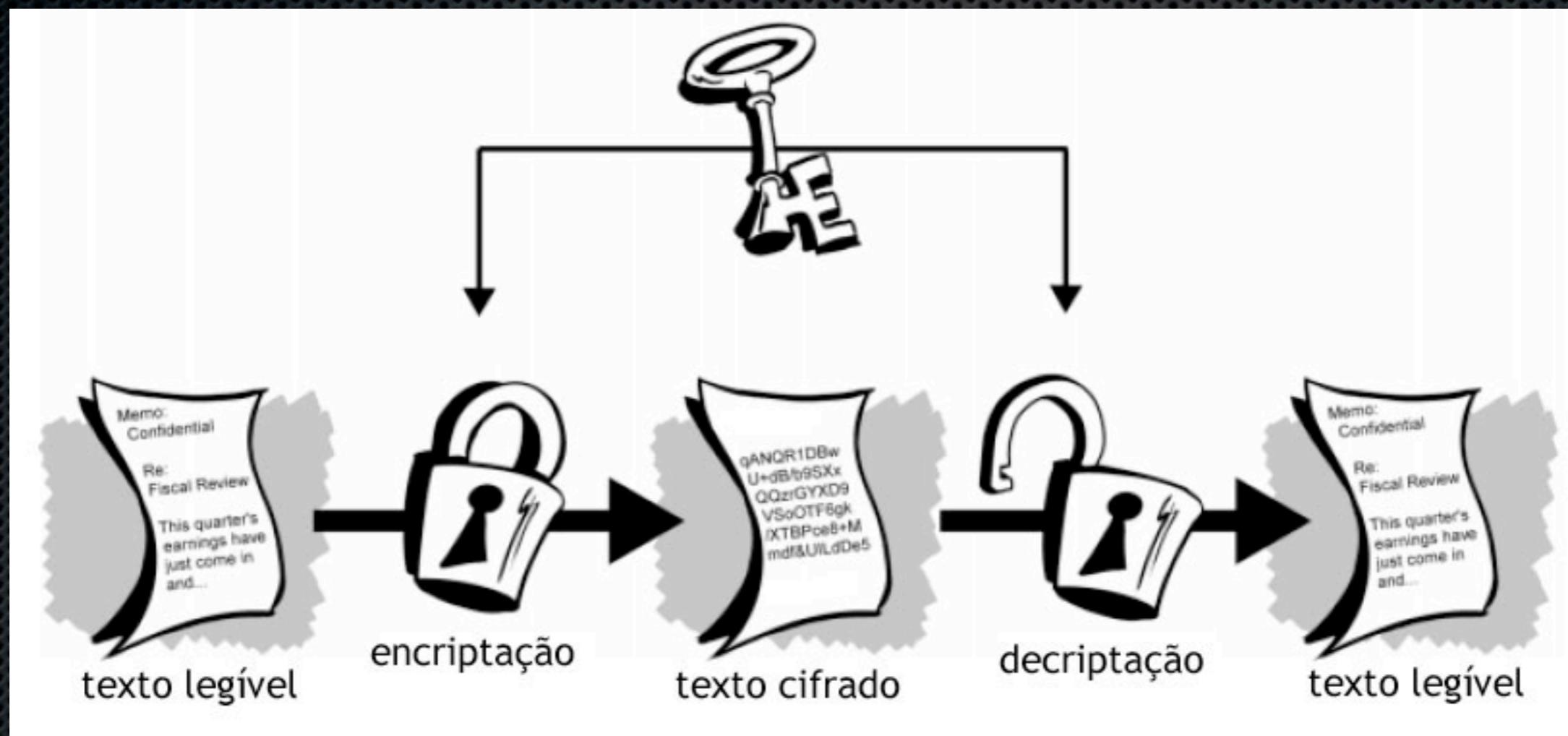
Criptografia hoje

- Comercio eletrônico, comunicação, sistemas financeiros, transações eletrônicas, segurança de computadores, dados sigilosos (por exemplo em hospitais) etc...
- A nossa sociedade é dependente da criptografia

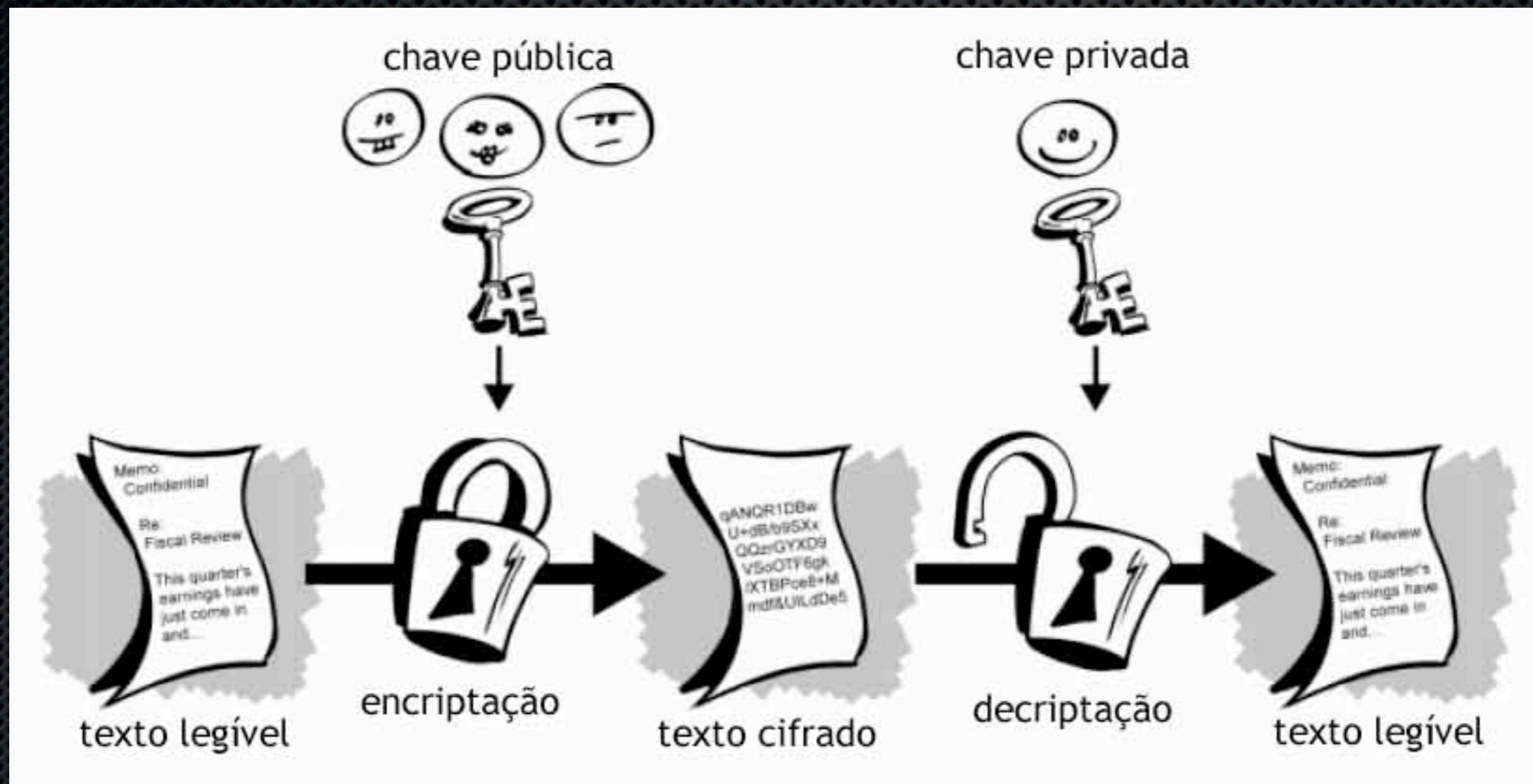
Algumas definições



Criptografia - simétrica



Criptografia - Assimétrica



História da Criptografia

- Grécia
- China
- Roma
- Idade média

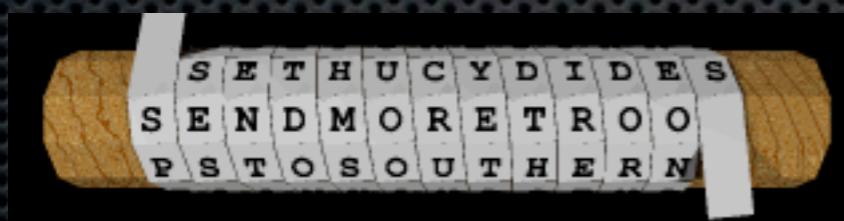
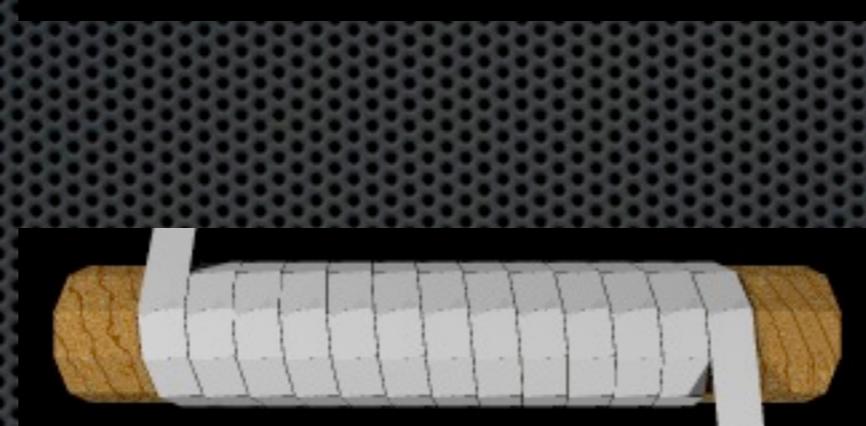
Grécia

- Grande batalha naval entre Atenas e os Persas (Xerxes) Guerras médicas - 23 de Setembro 480AC
- Esteganografia - mensagem oculta - tablete de madeira com mensagem oculta em argila.
- Cinturão espartano

Cinturão Espartano: primeiro dispositivo militar para criptografia



Cinturão Espartano: primeiro dispositivo militar para criptografia



Roma



Bust of Julius Caesar, from
The Art of the Romans
by H.P. Walters (1911),
The British Museum.

Number of Lines □ < □ 18 □ >

Plaintext Alphabet	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
Ciphertext Alphabet	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

Keep spaces between words

Slow Encrypt

Fast Encrypt

Plaintext

Mesangem cifrada pela cifra
de Julio Cesar

Ciphertext

EWKSFYWE UAXJSVS HWDS UAXJS
VW BMDAG UWKSJ

Simon Singh - Black Chamber
http://www.simonsingh.net/The_Black_Chamber

Cifra de Pigpen (Maconaria séc. XVIII)



Plaintext

Mensagem cifrada pelo pigpen

Ciphertext

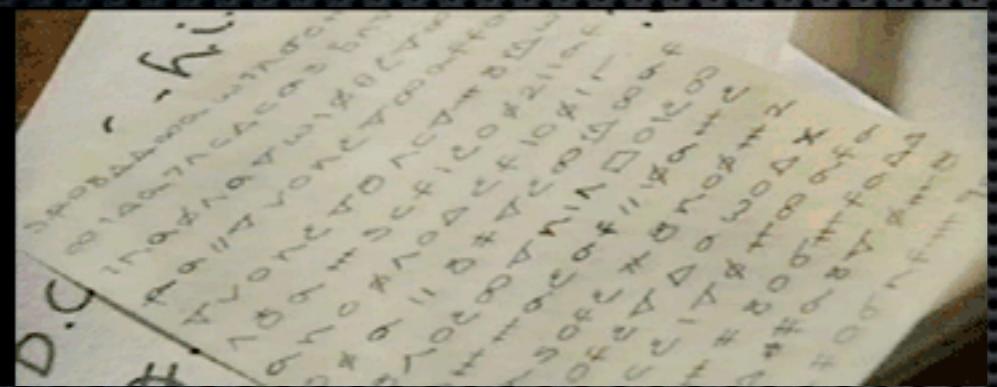


O surgimento da Criptoanálise

- Rainha Maria da Escócia
- Análise de frequência

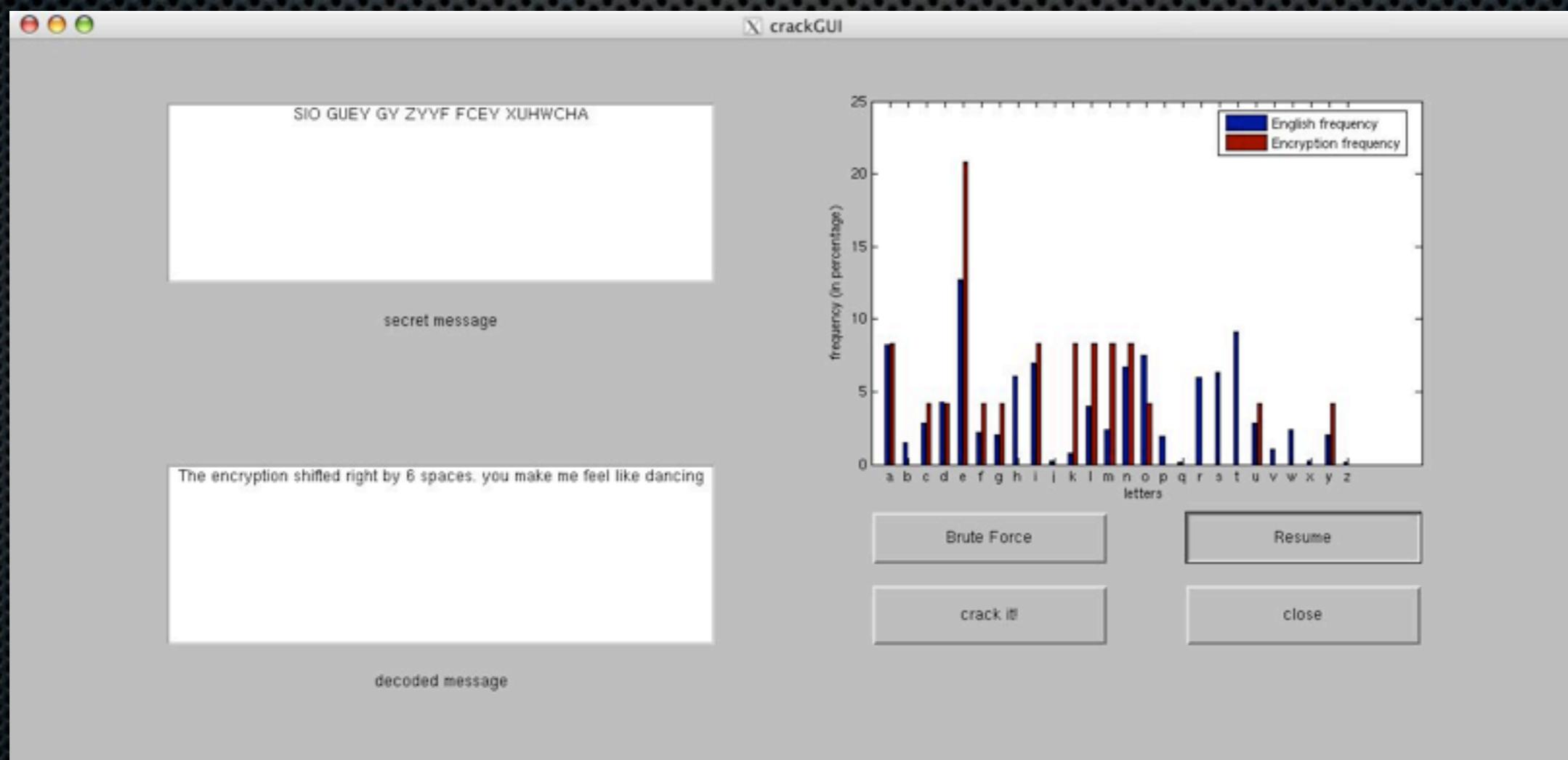
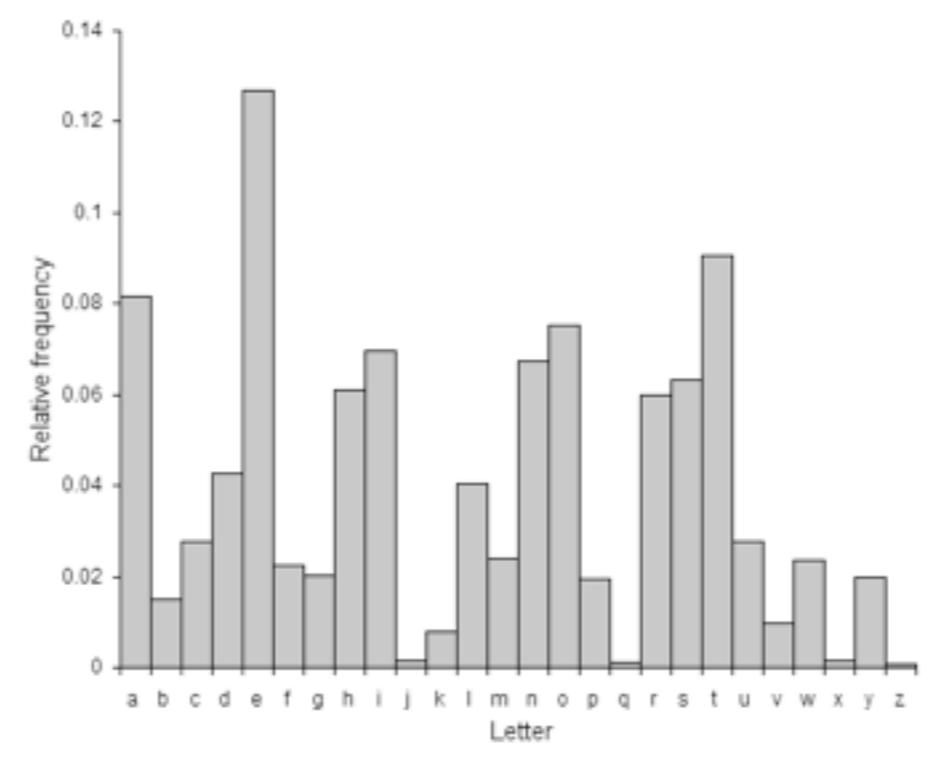
Rainha Maria da Escócia

- Cartas conspirando contra a Rainha Elizabeth da Inglaterra
 - As cartas foram decifradas e a Rainha Maria executada



Análise de freqüência

- Proposto pelos árabes, a análise de freqüência utiliza a estatística para determinar a freqüência comum em que letras e seqüências de letras ocorrem



Criptografia x Cripto-análise

- Duelo permanente. A medida que os cífras são desvendadas, novas e mais bem elaboradas são criadas. A cripto-análise também evolui constantemente ficando cada vez mais elaborada a fim de quebrar as novas cífras

Por que a criptografia é tão importante ?

- A criptografia e a guerra.
- No tempo dos Gregos ou dos Romanos os generais se comunicavam enviando mensageiros.
- A informação é a arma mais poderosa que existe.
- A criptografia atinge seu auge nas guerras do séc XX.

Grandes Guerras do séc. XX

- Invenção do Rádio.
- Não há fronteiras para as ondas eletromagnéticas.
- As informações transmitidas por rádio podem ser ouvidas pelo inimigo.
- Solução: Criptografia



Guerra, criptografia e computação

- Primeira vez na história em que foi utilizada uma máquina para gerar cífras
- Enigma
- Até o final da guerra outros países possuiriam suas próprias máquinas de cifragem (ex: EUA, Japão, etc)

Enigma

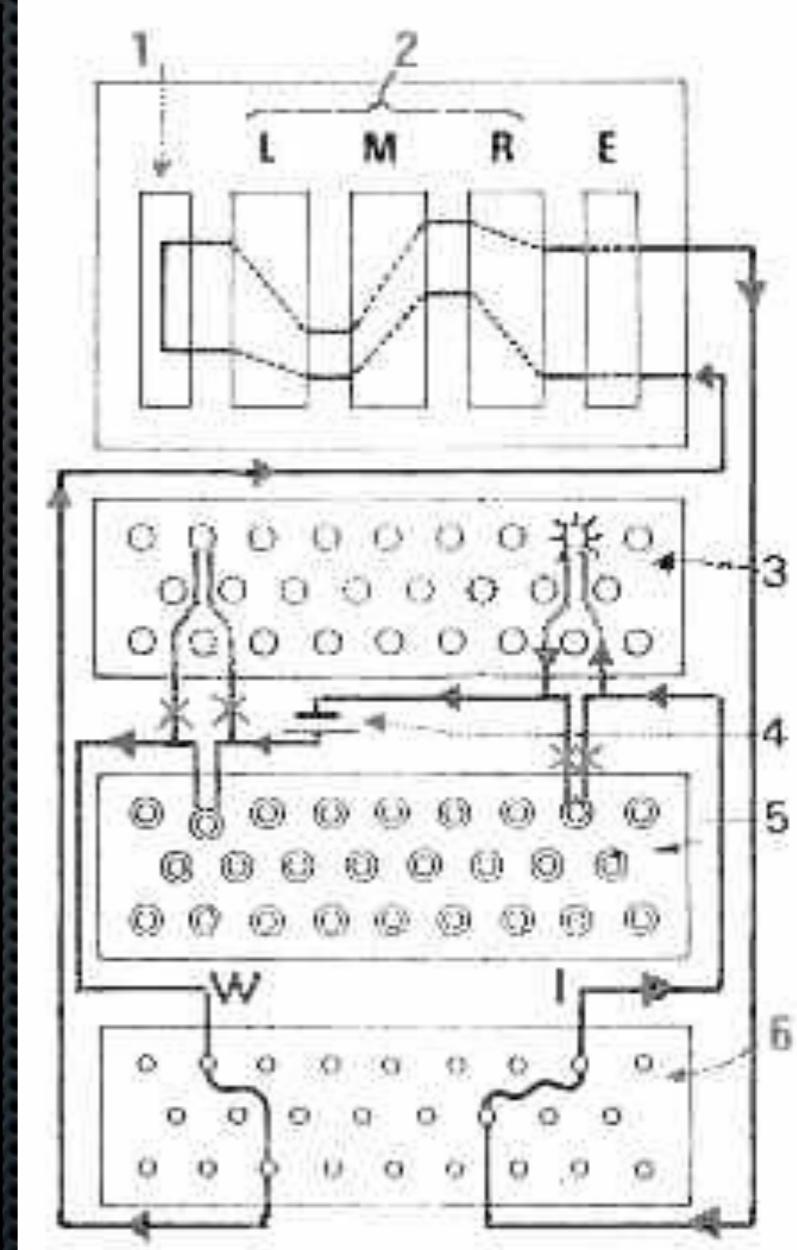


Número de combinações:
15.000.000.000.000.000









Quem decifrou a enigma ?

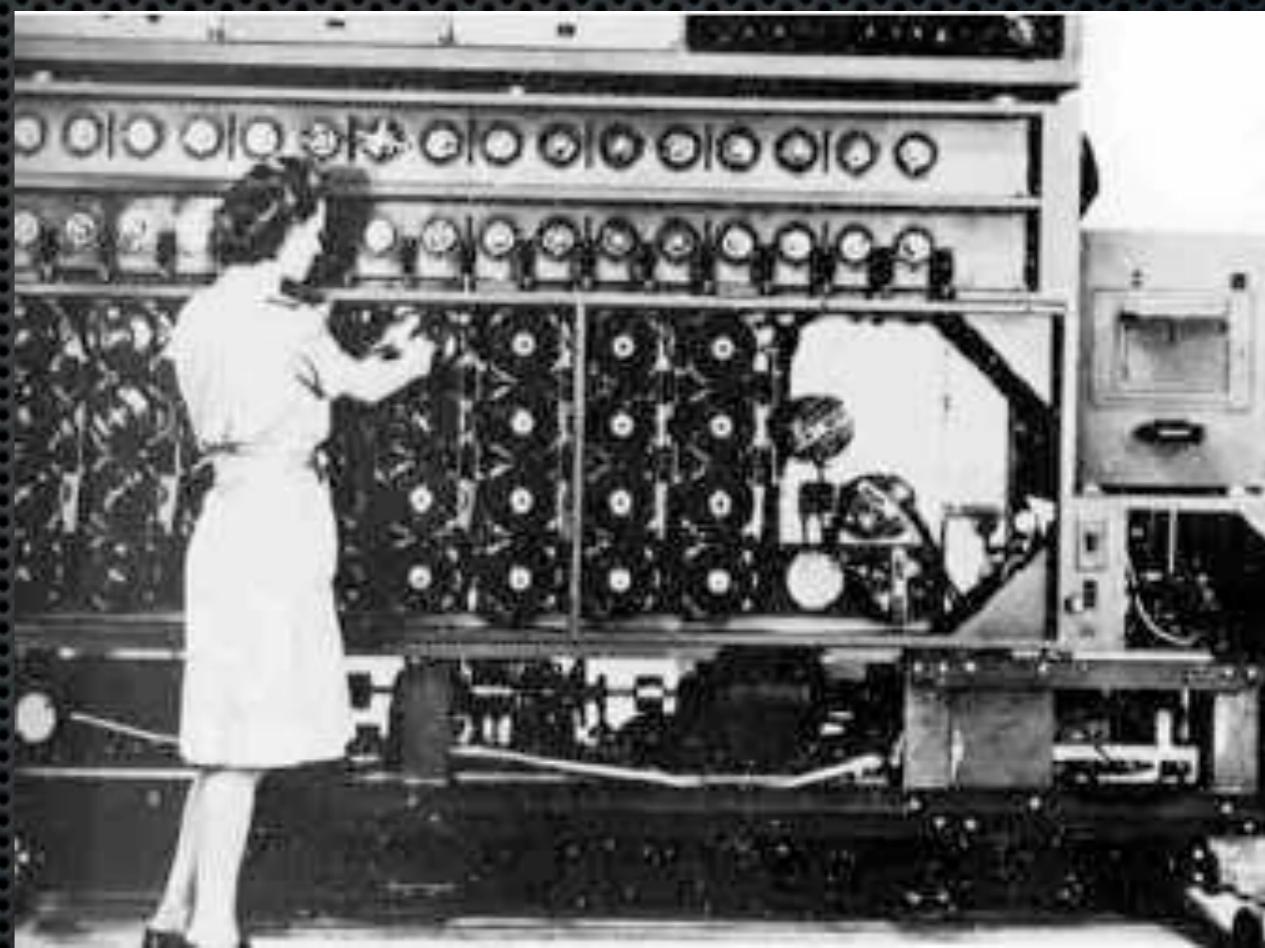
- Matemático polonês
- Marian Rejewski
- Inteligência polonesa - Biuro Szyfrów
- Principais indícios de que a Enigma poderia ser decifrada

A agência de inteligência britânica

- Bletchley Park - 1939
- Sede da agência de inteligência inglesa
- Reunia um equipe “ortodoxa”, matemáticos, lingüistas, jogadores de xadrez e aficionados por palavras cruzadas
- Local de trabalho de Alan Turing

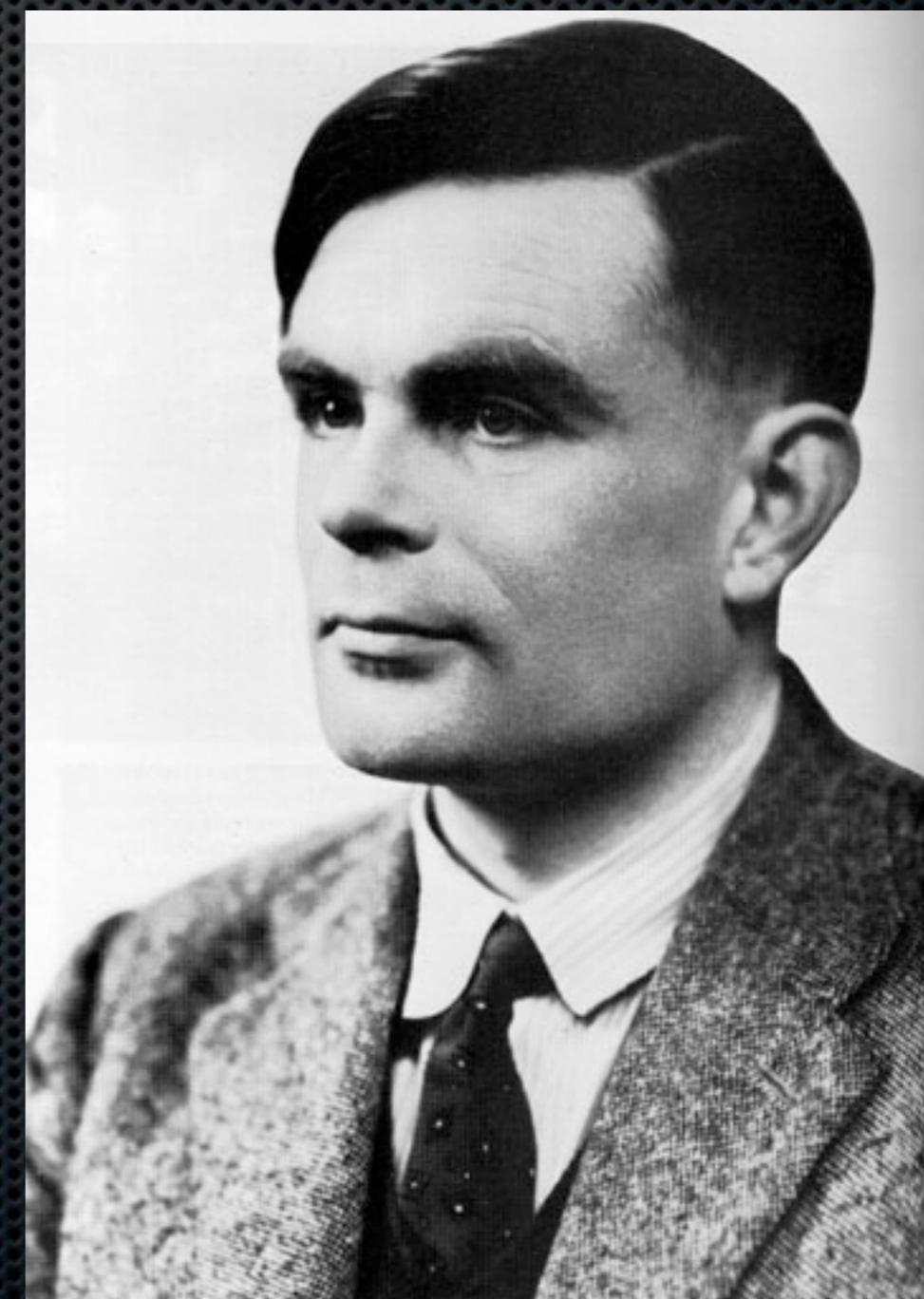


Enigma bombe



Alan Turing (1912-1954)

- Filosofia/Matemática
- Inteligência Artificial
- Criptografia - Enigma
- trabalho militar / participação importante no cenário da segunda guerra mundial
- Base teórica para os computadores



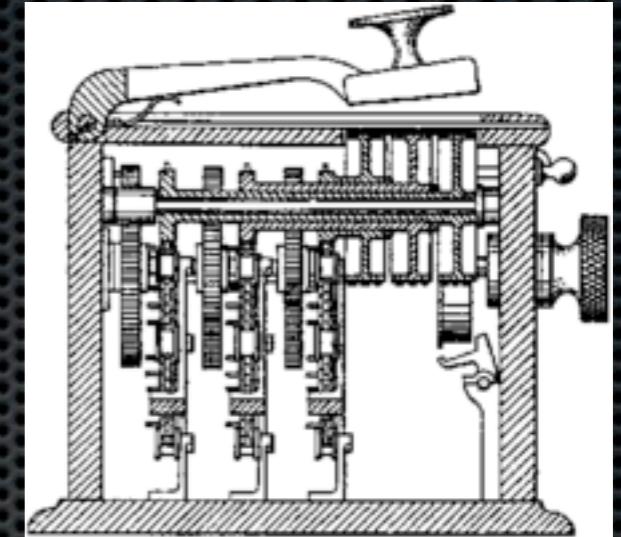
Criptografia em tempos de Paz

- Privacidade da informação
- Segurança em redes e em sistemas operacionais
- Vital para a sociedade moderna: exemplo transações financeiras na internet

Criptografia Moderna

- A criptografia moderna utiliza o embaralhamento bit a bit
- São utilizadas operações, lógicas e aritméticas. Em especial a MOD e XOR
- A grande maioria das cifras atuais podem ser quebradas! Exemplo, MD5, SHA e outras

Cifra de Hill



- Exemplo de cifra baseada em Álgebra Linear
- Idéia de máquina patenteada em 1929 pelo matemático Lester Hill
- Ela utiliza o conceito de criptografia em blocos

Cifra de Hill

- Seja o alfabeto definido por A = 0, B=, ..., Z=25
- Considere a senha $pwd = \text{'elefantes'}$ assim, $pwd = [5 12 5 6 1 14 20 5 19]$
- Na forma de matriz $pwd = \begin{pmatrix} 4 & 11 & 4 \\ 5 & 0 & 13 \\ 19 & 4 & 18 \end{pmatrix}$
- Considere que a mensagem é ‘usp’ -> $plain = [20, 18, 15]$
- $plain = \begin{pmatrix} 20 \\ 18 \\ 15 \end{pmatrix}$

Cifra de Hill

$$cypher = pwd * plain \bmod 26$$

$$cypher = \begin{pmatrix} 4 & 11 & 4 \\ 5 & 0 & 13 \\ 19 & 4 & 18 \end{pmatrix} * \begin{pmatrix} 20 \\ 18 \\ 15 \end{pmatrix} = \begin{pmatrix} 338 \\ 295 \\ 722 \end{pmatrix} = \begin{pmatrix} 0 \\ 9 \\ 20 \end{pmatrix} (\bmod 26)$$

cypher = aju

Cifra de Hill

- para a senha elefantes, a cifra do bloco ‘usp’ é ‘aju’
- mudando a ordem do texto plano, para o bloco ‘sup’ a cifra é ‘ozq’
- O que dificulta a análise de frequência

Cifra de Hill

- Para descriptografar a cifra, é necessário:
- $\text{plain} = \text{inv}(\text{pwd}) * \text{cypher}$
- A inversa entretanto deve levar em consideração a operação de módulo

Cifra de Hill

- calculando a inversa:
- Seja a matriz K , sua inversa é determinada por:

$$inv(K) = \frac{1}{det(K)} * adj(K)$$

- Considerando o módulo:

$$inv(K) = x * adj(K) mod 26$$

- onde,

$$x * det(K) mod 26 = 1$$

Cifra de Hill

- Ataque diferencial
- A cifra de Hill parece ser segura, em especial se analisada pela análise de frequência. Entretanto é simples quebrar a cifra por ataque diferencial.

Ataque Diferencial

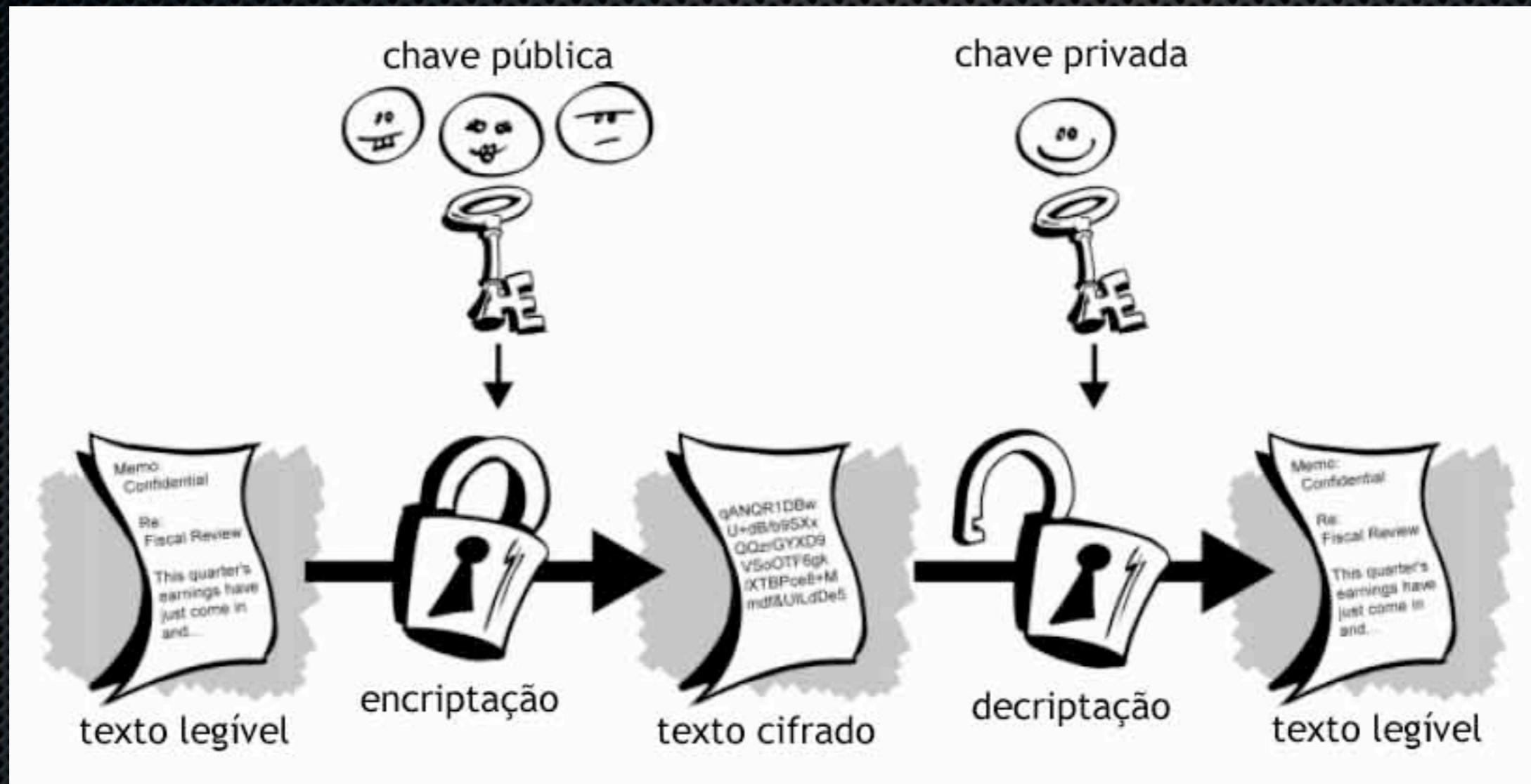
- » [http://www.public.iastate.edu/~roettger/307/matlab/
crypto.html](http://www.public.iastate.edu/~roettger/307/matlab/crypto.html)

Modo de operação

$$C_i = E_{\vec{\pi}}(P_i \oplus C_{i-1})$$

$$P_i = D_{\vec{\pi}}(C_i \oplus C_{i-1})$$

Criptografia Assimétrica



Algoritmo de Diffie-Hellman

- Alice e Bob querem estabelecer um chave pública e privada
- Alice e Bob combinam os parâmetros $K = 7$ e $Z = 11$ (números primos)
- Alice escolhe a sua senha como $S_a = 6$ e Bob $S_b = 3$
- Alice envia para Bob sua chave pública $R_a = 4$ [$R_a = (7^{^6}) \text{ mod } 11 = 4$]
- Bob envia para Alice sua chave pública $R_b = 2$ [$R_b = (7^{^3}) \text{ mod } 11 = 2$]
- A chave privada PSK é calculada:
 - Para Alice -> $\text{PSK} = 9$ [$\text{PSK} = (2^{^6}) \text{ mod } 11 = 9$]
 - Para Bob -> $\text{PSK} = 9$ [$\text{PSK} = (4^{^3}) \text{ mod } 11 = 9$]
- PSK é utilizada com senha para uma algoritmo simétrico. Com base neste modelo, o algoritmo simétrico, pode ser utilizado com assimétrico

Caos: em busca da cifra invencível

