Criptografia de chave simétrica

...

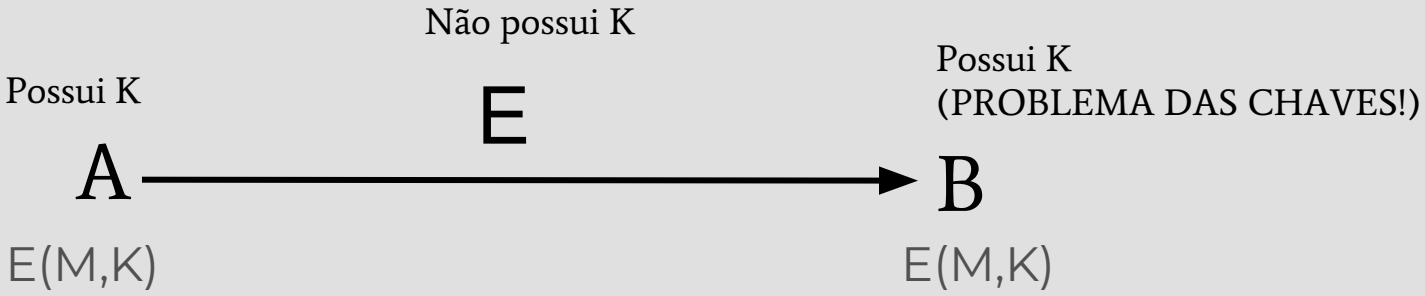
Original: https://enigma.ic.unicamp.br/blog/posts/symmetric-encryption/

O QUE É CRIPTOGRAFIA?

Contar segredos em lugares públicos
Falar coisas sigilosas por meios não confiáveis

- Conjunto de princípios e técnicas utilizados para garantir comunicação segura, ainda que na presença de possíveis atacantes - garantir sigilo da informação e **autenticidade**.

Algoritmo E
Mensagem M
Chave K



PROBLEMA DA DIST. DE CHAVES

Como combinar as chaves?

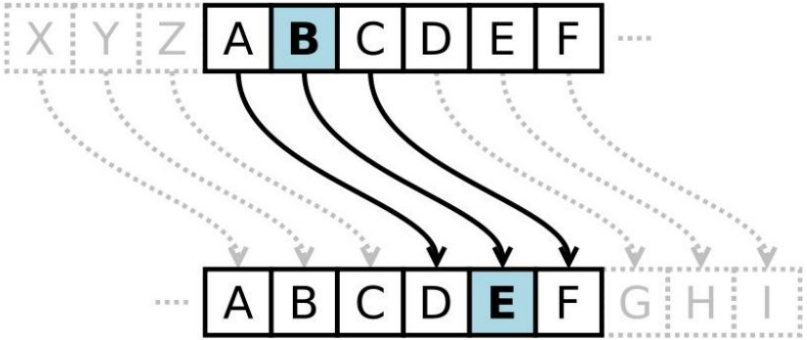
- O **problema da distribuição de chaves** foi uma pulga atrás da orelha por muito tempo. Para isso, foram criados os **algoritmos de chave assimétrica**.

Mas, antes disso...

CIFRA DE CESAR

É uma **Cifra de substituição** em que cada letra é trocada por outra que esta a um número x de posições de distância. A chave é simplesmente esse número

- Se a chave for **K=4**, a letra A será substituída por E. Seguindo essa lógica, o texto **enigma** seria transformado em **IRMKQE**.



Só existem **25** chaves! Ou seja, dá para fazer um algoritmo de força bruta (e **testar todas**)!

SUBSTITUIÇÃO SIMPLES

Agora, vamos gerar um alfabeto novo! Se cada letra receber um novo símbolo (A virar E, E virar Z, etc...), teremos **26!** combinações.

"Os primeiros ativistas no final dos anos 1980, com o embrionario movimento dos Cypherpunks, ja atentavam para falta de seguranca em torno dos dados trocados na internet."

Criando o alfabeto enigmês:

a	b	c	d	e	f	g	h	i	j	k	l	m
P	H	Q	G	I	U	M	E	A	Y	L	N	O

n	o	p	q	r	s	t	u	v	w	x	y	z
F	D	X	J	K	R	C	V	S	T	Z	W	B

DR XKAOIAKDR PCASARCPR FD UAFPN GDR PFDR 1980, QDO D IOHKADFPKAD ODSAOIFCD GDR QWXEIKXVFLR, YP PCIFCPSPO XPKP UPNCP GI RIMVKPFQP IO CDKFD GDR GPGDR CKDQPGDR FP AFCIKFIC.

LEI DE ZIPFT

O problema é que a frequência de caracteres em um texto em uma língua é bem definido. Veja no português:

Letra	Frequência
a	15%
e	13%
o	11%
s	8%
r	7%

Isso já é 54%

do texto!

Digamos que encontramos um texto cifrado com as seguintes frequências:

Letra	Frequência
L	13.55%
G	12.23%
S	8.47%
Z	8%
J	7.81%

Já é possível decifrar sabendo algumas palavras-chave!

CIFRA DE VIGENÈRE

É uma cifra **polialfabética**.

- Digamos que queremos passar a mensagem “cozidomisto” e temos a chave “cab”. Repetimos a chave até ter o tamanho da mensagem e deslocamos as letras do original da seguinte forma:
a primeira letra da mensagem (c) irá virar “e”, pois a primeira letra da chave é c (2), a segunda (o) irá ser o, pois a segunda letra da chave é a (0)

cozidomisto
cabcabcabc
eoakdpoitvo

Estamos seguros???

CIFRA DE VIGENÈRE

Ainda não.

- A Cifra de Vignére possui uma natureza repetitiva. Veja:

A B C D A B C D A B C D A B C D **A B C D** A B C D A B C D
C R Y P T O I S S H O R T F O R **C R Y P** T O G R A P H Y
C S A S T P K V S I Q U T G Q U **C S A S** T P I U A Q J B

- A distância de repetição entre CSAS é 16 caracteres, ou seja, todos os divisores de 16 são candidatos ao **tamanho** chave. Utilizando técnicas estatísticas como o **teste de Friedman** podemos é possível achar K1 K2 K3 K4 da nossa chave (mas o texto precisa ser longo!).

DES E AES

Data Encryption Standard
Advanced Encryption Standard

- Baseados na lógica do **XOR**:

0 XOR 0 = 0
0 XOR 1 = 1
1 XOR 0 = 1
1 XOR 1 = 0

```
0001010101010
1011101010100
1010111111110
```

- Gerar chaves do tamanho da mensagem é custoso, por isso elas são **“reaproveitadas”** (como em vignere), DES utiliza 56 bits e AES 256.
- Em **1999**, conseguiram quebrar o DES em aprox. 22h.