

Introdução

1.

- A cifra (encryption) é o processo de codificar uma mensagem de forma a que apenas entidades autorizadas possam ler o conteúdo da mensagem original.
- A história da cifra começou no ano 1900 A.C. com cifras entre sacerdotes egípcios e também na Mesopotâmia.
- 2 Tipos de cifra:
 - Cifra simétrica ou cifra de chave secreta (secret-key encryption): a mesma chave é usada para cifra e decifra.

• Cifra assimétrica ou cifra de
chave pública (public-key encryption):
diferentes chaves são usadas na cifra
e decifra.

Cifra de Substituição

- A cifra é feita substituindo unidades
de texto em claro (plaintext) por
texto cifrado (ciphertext), de acordo
com um sistema fixo.
- unidades podem ser letras isoladas,
pares de letras, triplos, misturas dos
anteriores, etc.
- A decifra realiza a substituição inversa.

- 2 Cifras de substituição:

3.

- Monoalfabética - substituição fixa e usada sobre toda a mensagem.
- Polialfabética - um n° de substituições e usado em diferentes posições da mensagem.

Cifra de César

- cifra de substituição monoalfabética usada pelo imperador Júlio César (100 A.C.)
- cada letra do texto em claro é substituída por outra letra localizada num n° fixo de posições a seguir no alfabeto.

Exemplo

4.

texto em claro:

a	t	t	a	c	k	a	t	o	n	c	e
---	---	---	---	---	---	---	---	---	---	---	---

shift +4

texto cifrado:

e	x	x	e	g	o	e	x	n	g	i
---	---	---	---	---	---	---	---	---	---	---

shift

d	w	w	d	f	n	d	w	n	g	f	h
---	---	---	---	---	---	---	---	---	---	---	---

c	v	v	c	.	.	.
---	---	---	---	---	---	---

b	n	n	b	.	.	.
---	---	---	---	---	---	---

a	t	t	a	c	k	a	t	o	n	c	e
---	---	---	---	---	---	---	---	---	---	---	---

quebram a cifra
por ataque de força bruta
(brute force attack)

Cifra monoalfabética - Exemplo

Letra mais frequente:

- inglês $\rightarrow e$
- criptograma $\rightarrow n$

Bigramas

$t\underline{n} \rightarrow H\underline{E}$

$y\underline{t} \rightarrow T\underline{H}$

$\underline{n}h \rightarrow \underline{E}R$

$\underline{n}q \rightarrow \underline{E}S$

$\underline{v}\underline{\mu} \rightarrow \begin{cases} \underline{ON} \\ \underline{ST} \end{cases} ?$

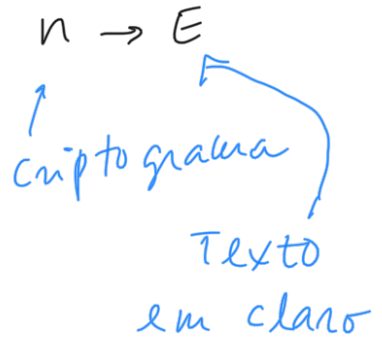
Trigramas

$ytn \rightarrow THE$

$\underline{v}\underline{\mu}p \rightarrow \begin{cases} \underline{AND} \\ \underline{ING} \end{cases} ?$

$\mu \rightarrow N$

Substituições
de decifra:

$n \rightarrow E$


$t \rightarrow H$

$y \rightarrow T$

$h \rightarrow R$

$q \rightarrow S$

$\mu \rightarrow N$

entropy of $E(HTRSN) < \text{ciphertext}$

1^a linha: " v SER m ES x b "

2. \Leftarrow links: "T_x" ... "T_x" "T_x" \rightarrow "T₀"

Substituição:

$$z \rightarrow v$$

2ª linha: "a ENTURd" → "CENTURYy"

4ª linha: "INfENTED"



"ENnINEER"



5ª linha: "FROc"



6ª linha: "ADOATED"



Última linha: "ITAiIAN"



Substituições:

a → C

d → y

f → v

n → G

c → M

e → P

i → L