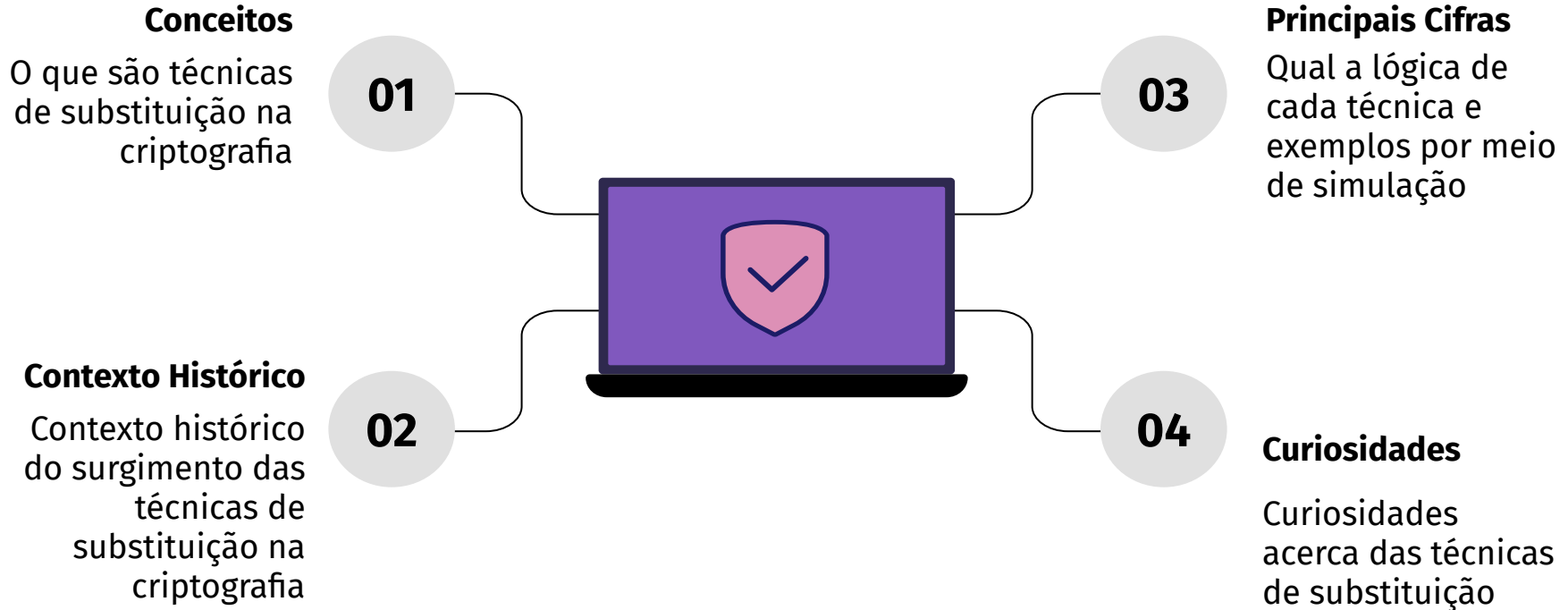




Técnicas de Substituição

Giulia Rossatto Rocha
João Pedro Olimpio
Larissa Mayumi B. Hondo
Rodrigo Cesar B. Rossetti

Apresentação



Conceitos

1

Algoritmo de criptografia é um meio de transformar texto simples em texto cifrado sob o controle de uma chave secreta. Essa chave também é utilizada para decifrá-lo.

2

Na criptografia, pode-se diferenciar o conceito de **código** (semântica) e **cifra** (sintaxe). As técnicas de substituição são cifras de substituição, algoritmos executados individualmente ou em pequenos blocos de letras.

3

Técnicas de substituição consistem em substituir unidades ou blocos de caracteres por outros, de forma coerente. As unidades do texto são mantidas na mesma ordem, mas elas próprias são alteradas.



Conceitos

4

Elas podem se dividir em cifras monoalfabéticas (simples), homófonas, cifras polialfabéticas e cifras poligráficas.

5

Alguns autores as enquadram como cifras pertencentes à categoria de encriptação simétrica (chave única). Outros a enquadram como cifras clássicas.

6

Perderam a força para algoritmos matemáticos de encriptação. E também por conta da sua facilidade de ser quebrada por meio de análise de frequência.



Contexto Histórico



Tornar uma mensagem
incompreensível para
pessoas não autorizadas.

Objetivo

Criptografia e
descriptografia não devia
ser complicada e sim
acessível e apropriada
para as pessoas
envolvidas.

Princípio

Criptografia é uma
técnica milenar. Menções
sobre ter sido usadas em
hieróglifos egípcios.

Há 4000 anos

Contexto Histórico



Associa letras com números ou com outras letras por meio do uso de uma tabela. Algumas mensagens eram transmitidas por tochas de fogo.

Júlio César propõe para proteção de informações governamentais. Três posições consecutivas do alfabeto (cifra monoalfabética).

Uso de diversos alfabetos de substituição e criptografia de cada letra da mensagem original com o uso de um alfabeto diferente (cifra polialfabética)

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

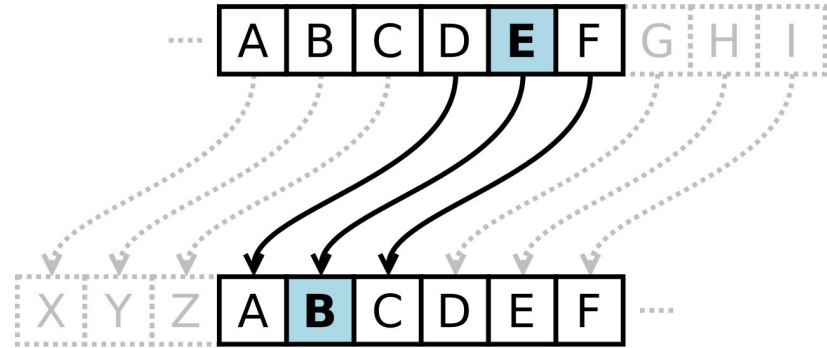
Grécia Antiga: Cifra ou Quadrado de Políbio

Roma Antiga: Cifra de César

Século XIX: Cifra de Vigenère

Cifra de César

- Uma das primeiras cifras utilizadas.
- Nomeada em homenagem a Júlio César, que a usava com uma troca de três posições para proteger mensagens de significado militar.
- Consiste no deslocamento do alfabeto um número de posições para a esquerda ou para a direita.
- Cada letra do texto original é substituída por sua letra correspondente no alfabeto deslocado.



Cifra de César

Exemplo

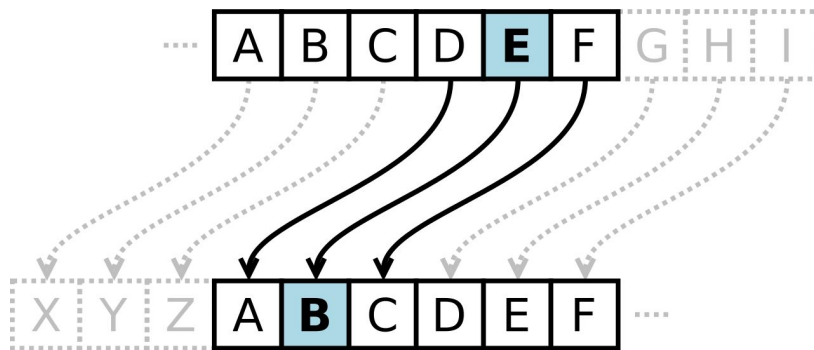
Considerando o alfabeto latino - 26 letras

Texto original: cifra de cesar

Alfabeto original: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Substituição
das letras

Texto cifrado: fliud gh fhvdu



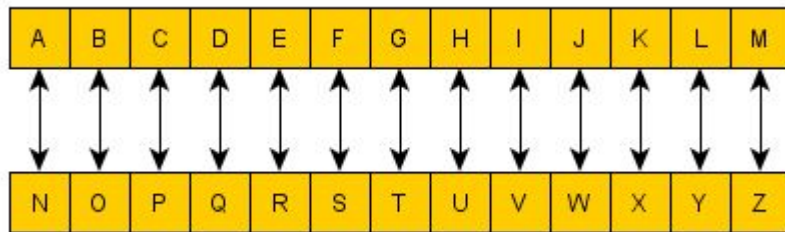
Deslocamento:
3 posições para
a esquerda

Alfabeto deslocado: DEFGHIJKLMNOPQRSTUVWXYZABC

Cifra de César

Casos Especiais

- **Cifra Atbash:** Mapeamento reverso com deslocamento de 25 posições. A primeira letra vira a última, a segunda vira a penúltima, e assim por diante.
- **ROT13:** Rotação de 13 posições. No alfabeto latino é a sua própria inversa, ou seja, o mesmo algoritmo pode ser aplicado para criptografar e descriptografar o texto.



ת
ש
ר
ק
צ
פ
ע
ס
ב
מ
ל
כ
י
ס
ח
ז
ה
ד
ג
ב
א

א
ב
ג
ד
ה
ו
ז
ח
ט
י
כ
ל
מ
נ
ס
ע
פ
צ
ק
ר
ש
ת

Cifra Monoalfabética

- A Cifra de César e suas variações podem ser quebradas por força bruta
 - **25** possibilidades
- A cifra monoalfabética é o caso mais genérico em que cada letra do alfabeto é mapeada a uma outra letra
 - **25!** Possibilidades
 - Inviável quebrar por força bruta, mas ainda pode ser quebrada por análise de frequência
- Exemplo
 - ABCDEFGHIJKLMNOPQRSTUVWXYZ → AZERTYUIOPQSDFGHJKLMWXCVBN
 - Cifra monoalfabetica → eoyka dgfgasyaztmoea

Cifra Afim

- Cada letra é mapeada em seu equivalente numérico, encriptada usando uma função matemática simples e convertida de volta para letra.
- **Função de criptografia:** $E(x) = (ax + b) \bmod m$
- **Função de descriptografia:** $D(x) = a^{-1}(x - b) \bmod m$

Onde:

m é o tamanho do alfabeto

a e b formam a chave

a e m devem ser coprimos

- Dois números são coprimos se o único divisor comum entre eles é 1

Cifra Afim

Exemplo

Vamos considerar:

Alfabeto latino, onde $A = 0$, $B = 1$, ..., $Z = 25$.


$a = 5$ e $b = 8$, sendo que $a = 5$ e $m = 26$ são coprimos


Texto Original	C	I	F	R	A	A	F	I	M
x	2	8	5	17	0	0	5	8	12
$(5x + 8)$	18	48	33	93	8	8	33	48	68
$(5x + 8) \bmod 26$	18	22	7	15	8	8	7	22	16
Texto Cifrado	S	W	H	P	I	I	H	W	Q

Cifra Maçônica

- Cifra antiga, utilizada pela Maçonaria no século 18
- O alfabeto do texto cifrado pode ser diferente do alfabeto do texto original
- Na cifra maçônica usamos símbolos para codificar o texto de acordo com o esquema a seguir

A	B	C	J	K	L
D	E	F	M	N	O
G	H	I	P	Q	R





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				
<	^	∇	>	<	^				

Cifra Maçônica

Exemplo



R E M E M B E R D E A T H

Considerando a variação com 3 grids:

1 ponto

A	B	C
D	E	F
G	H	I

2 pontos

K	L	M
N	O	P
Q	R	S

0 pontos

T	U	V
W	X	Y
Z		

Texto original: Remember death

Cifra Baconiana

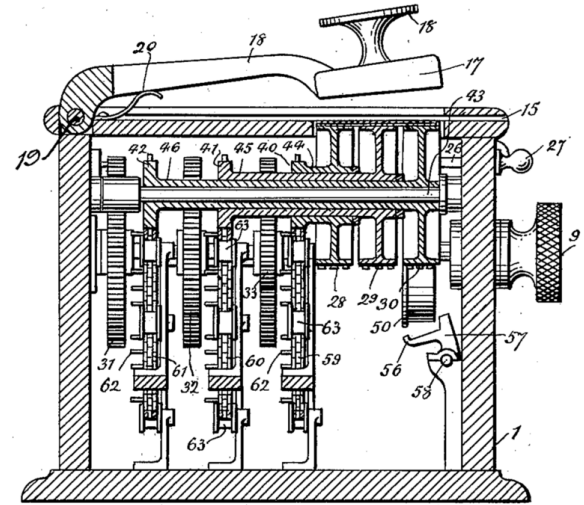
- Cada letra é codificada em uma representação binária usando A e B

A = aaaaa	I/J = abaaa	R = baaaa
B = aaaab	K = abaab	S = baaab
C = aaaba	L = ababa	T = baaba
D = aaabb	M = ababb	U/V = baabb
E = aabaa	N = abbaa	W = babaa
F = aabab	O = abbab	X = babab
G = aabba	P = abbba	Y = babba
H = aabbb	Q = abbbb	Z = babbb

- Na época em que a cifra foi criada, I e J e U e V eram uma única letra
- **Exemplo:** BACON = aaaabaaaaaaaabaabbababbaa

Cifra de Hill

- Quando uma substituição uniforme é aplicada sobre um bloco de texto, a cifra utiliza **substituição poligráfica**
- Na cifra de Hill, cada letra é representada por um número mod 26
- **Criptografia:** Cada bloco de n letras é multiplicado por uma matriz $n \times n$ inversível mod 26
- **Descriptografia:** Cada bloco é multiplicado pela inversa da matriz utilizada para criptografia
- Uma matriz é inversível se o seu determinante for diferente de zero



Cifra de Hill

Exemplo - Criptografia

- **Texto Original:** ACT (n = 3)

Escrito como vetor:

0
2
9

- **Chave:** GYBNQKURP

Escrita como uma matriz 3x3:

6 24 1
13 16 10
20 17 15

- O vetor criptografado é dado:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \times \begin{pmatrix} 0 \\ 2 \\ 9 \end{pmatrix} = \begin{pmatrix} 15 \\ 22 \\ 31 \end{pmatrix}$$

$$\begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

- O que corresponde ao texto criptografado: POH

Cifra de Hill

Exemplo - Descriptografia

- A matriz inversa da chave é:

$$\begin{array}{ccc|ccc} 6 & 24 & 1 & & 8 & 5 & 10 \\ 13 & 16 & 10 & = & 21 & 8 & 21 \pmod{26} \\ 20 & 17 & 15 & & 21 & 12 & 8 \end{array}$$

- O vetor descriptografado é dado:

$$\begin{array}{ccc|cc|cc|cc} 8 & 5 & 10 & & 14 & & 260 & & 0 \\ 21 & 8 & 21 & \times & 15 & = & 574 & = & 2 \pmod{26} \\ 21 & 12 & 8 & & 7 & & 539 & & 19 \end{array}$$

- O que corresponde ao texto original: ACT

Quadrado de Polybius

- É um dispositivo de fragmentação de caracteres de texto
 - Os caracteres podem então ser representados por um conjunto menor de símbolos
 - Isso é útil para a telegrafia, esteganografia e criptografia

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Por exemplo:

GATO

vira

22 11 44 34

Cifra ADFGVX

- Foi utilizada pelo exército da Alemanha durante a Primeira Guerra Mundial para transmitir mensagens secretas via telégrafo.
- A cifra foi nomeada com base nas seis letras possíveis usadas no texto cifrado: A, D, F, G, V e X
- Essas letras foram escolhidas pois são bem diferentes uma da outra em código Morse, o que reduz a possibilidade de erro do operador
- A mensagem é criptografada e descriptografada usando um quadrado de Polybius 6x6 secreto, contendo as 26 letras do alfabeto e os dígitos de 0 a 9

Cifra ADFGVX

Exemplo

Considerando o seguinte
quadrado de Polybius secreto:

	A	D	F	G	V	X
A	N	A	1	C	3	H
D	8	T	B	2	O	M
F	E	5	W	R	P	D
G	4	F	6	G	7	I
V	9	J	0	K	L	Q
X	S	U	V	X	Y	Z

Texto original:

ATAQUE

Texto criptografo:

AD DD AD VX XD FA

Cifras Polialfabéticas

O que é

Qualquer cifra baseada em substituição, usando vários alfabetos.

Proteção

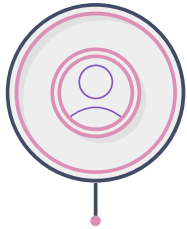
As cifras polialfabéticas são mais fortes que as monoalfabéticas.



1xN

A relação entre um caractere na mensagem original e os caracteres no texto cifrado é de um para muitos.

Cifras Polialfabéticas: Alberti

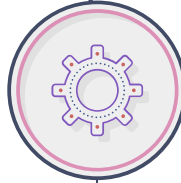


Ano de 1467

Pelo “O Pai da Criptologia Ocidental”, possui alfabetos mistos e períodos variáveis.

Quase Inquebrável

A análise de frequência não funciona



Dois discos de 24 Blocos

O interior para criptografar e o exterior para descriptografar

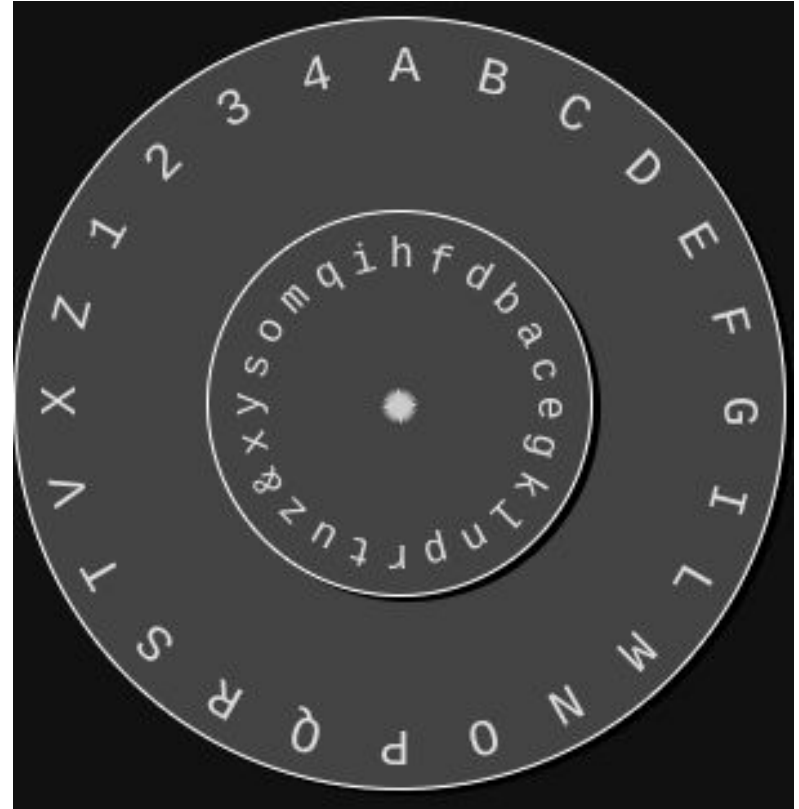


Cifras Polialfabéticas: Alberti - Exemplo

- Há diversas formas de se utilizar o disco;
- Uma delas é escolher um índice inicial para colocar embaixo do A e criptografar a mensagem com as letras correspondentes. Quando houver um número, este deve ser criptografado e o índice mudado para o qual estava no número;
- **Índice:** h
- **Mensagem:** ALBERTI
- **Mensagem para criptografar:** AL1BE3RTI

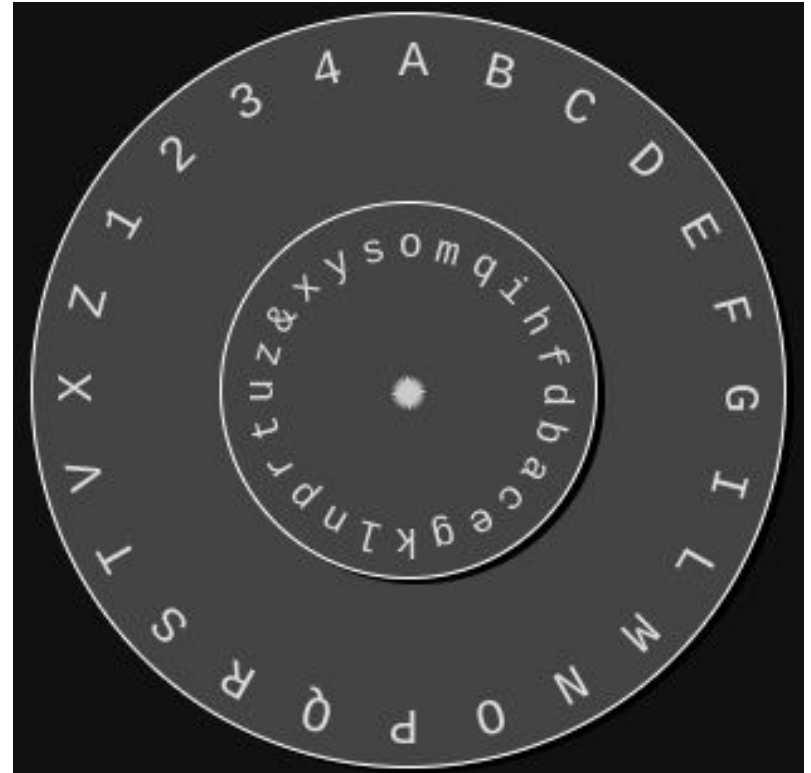
Cifras Polialfabéticas: Alberti - Exemplo

- **Índice:** h
- **Mensagem:** ALBERTI
- **Mensagem para criptografar:**
AL1BE3RTI
- **Texto cifrado:** -> hko
- Depois do 1, colocar 'o' embaixo do 'A'



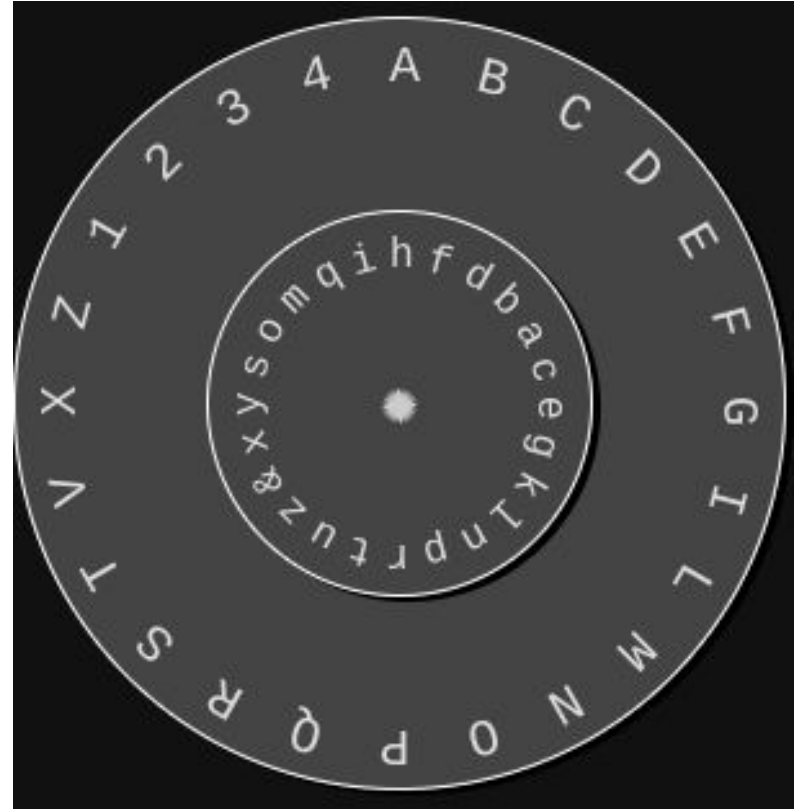
Cifras Polialfabéticas: Alberti - Exemplo

- **Índice:** 0
- **Mensagem:** ALBERTI
- **Mensagem para criptografar:**
AL1BE3RTI
- **Texto cifrado:** -> hkomhy
- Depois do 3, colocar 'y' embaixo do 'A'
- **Texto cifrado:** -> hkomhyknf

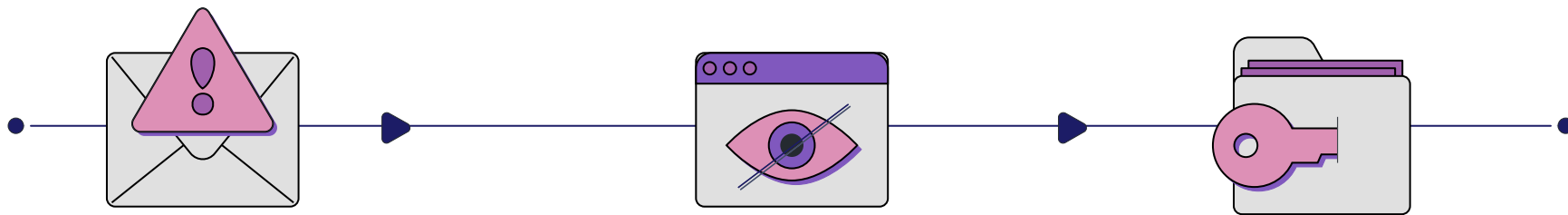


Cifras Polialfabéticas: Alberti - Exemplo

- **Para descriptografar:** mesmo processo com o índice inicial h, mas colocando cada letra no disco interno e checando no disco externo. Se for um número, deve ser rodado.
- **Índice:** h
- **Texto cifrado:** -> hkomhyknf
- **Mensagem obtida:** AL1
- Depois de obtido o 1, colocar 'o' embaixo do 'A'...



Cifras Polialfabéticas: Máquina Enigma



Contexto Histórico

Usado pelo comando militar da Alemanha nazista antes e durante a Segunda Guerra Mundial.

Quebra

Alan Turing desenvolveu uma máquina avançada que decifrava mensagens da Enigma em 1940.

Problema

Nenhuma letra jamais seria codificada como ela mesma, assim, por mensagens como “nada a relatar” e “para o grupo”, foi possível eliminar milhares de posições potenciais do rotor.

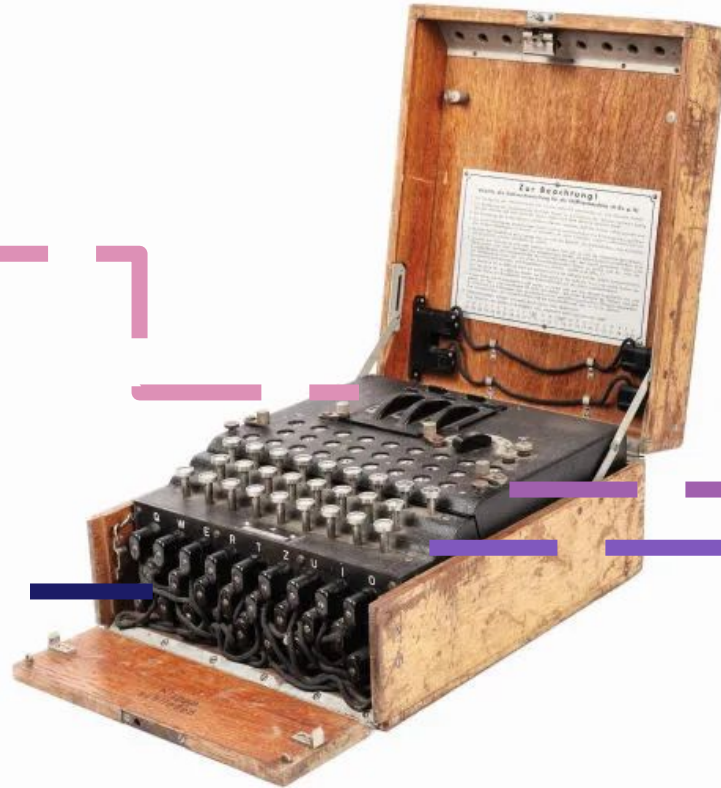
Cifras Polialfabéticas: Máquina Enigma

3 Rotores

A letra pressionada passa por três rotores, cada um a recebe e a envia como uma diferente, bate em um “refletor” no final e passa de volta por todos os três rotores na outra direção.

Painel de Tomadas

Invertia pares de letras.



Painel de Lâmpadas

Acendia letra criptografada correspondente.

Teclado

Para digitar a letra a se criptografar.

Cifras Polialfabéticas: Máquina Enigma - Exemplo

- **Mensagem:** FOLGENDES

0001 F > KGWNT(R)BLQPAHYDVJIFXEZOCSMU

0002 O > UORYTQSLWXZHNM(B)VFCGEAPIJDK

0003 L > HLNRSKJAMGF(B)ICUQPDEYOZXWTV

0004 G > KPTXIG(F)MESAUHYQBOVJCLRZDNW

0005 E > XDYB(P)WOSMUZRIQGENLHVJTFAK

0006 N > DLIAJUOVCEXBN(M)GQPWZYFHRKTS

0007 D > LUS(H)QOXDMZNAIKFREPCYBWVGTJ

0008 E > JKGO(P)TCIHABRNMDEYLZFXWVUQS

0009 S > GCBUZRASYXVMLPQNOF(H)WDKTJIE

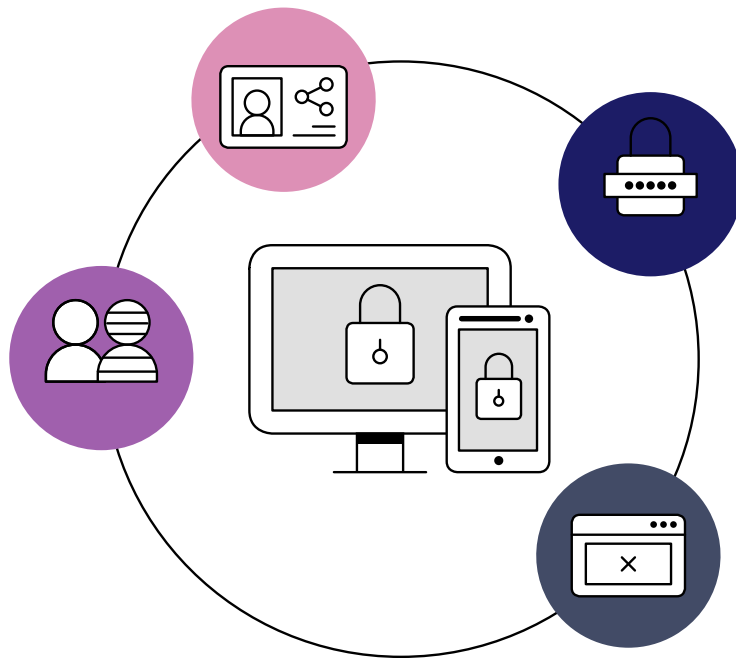
Cifras Polialfabéticas: Vigenère

Ano de 1553

Permaneceu sem ser quebrada por 300 anos.

Famosa

Fácil de colocar em prática.



Funcionamento

Uso de várias cifras de César em sequência.

Primeira Quebra

Percebendo que se a chave é curta e repetida as palavras comuns tendem a aparecer com as mesmas letras.

Cifras Polialfabéticas: Vigenère - Exemplo

- **Primeira forma:** pela Tabula Recta;
- **Segunda forma:** se as letras A–Z forem mapeadas nos números inteiros 0–25, e a adição módulo 26 for aplicada, a criptografia pode ser escrita:

$$x_i = (m_i + c_i)(mod\ 26)$$

- Sendo x_i a letra do texto cifrado, m_i a da mensagem e c_i da chave.

Cifras Polialfabéticas: Vigenère - Exemplo

- **Mensagem:** ATACAR BASE SUL
- **Palavra-chave:** LIMA O
- **Primeira forma:**

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

Cifras Polialfabéticas: Vigenère - Exemplo

- **Mensagem:** ATACAR BASE SUL
- **Palavra-chave:** LIMAO
- **Segunda forma:**

A (0)	T (19)	A (0)	C (2)	A (0)	R (17)	B (1)	A (0)	S (18)	E (4)	S (18)	U (20)	L (11)
L (11)	I (8)	M (12)	A (0)	O (14)	L (11)	I (8)	M (12)	A (0)	O (15)	L (11)	I (8)	M (12)
L (11)	B (1)	M (12)	C (2)	O (14)	C (2)	J (9)	M (12)	S (18)	S (18)	D (3)	C (2)	X (23)

- **Texto cifrado:** LBMCO CJMSSDCX

Cifras Polialfabéticas: Vigenère - Exemplo

- **Para descriptografar:**
 - **Texto cifrado:** LBMCO CJMSSDCX
- **Primeira forma:** ver linha com letra da palavra-chave e checar qual coluna que dá;
- **Segunda forma:** subtrair as letras do texto cifrado com as da palavra-chave. Se der < 0 , subtrair de 26.

L (11)	B (1)	M (12)	C (2)	O (14)	C (2)	J (9)	M (12)	S (18)	S (19)	D (3)	C (2)	X (23)
L (11)	I (8)	M (12)	A (0)	O (14)	L (11)	I (8)	M (12)	A (0)	O (15)	L (11)	I (8)	M (12)
A (0)	T (19)	A (0)	C (2)	A (0)	R (17)	B (1)	A (0)	S (18)	E (4)	S (18)	U (20)	L (11)

- **Mensagem:** ATACARBASESUL

Cifras Polialfabéticas: Trithemius - Exemplo

- Ano de 1518, pode ser considerada como uma cifra de Vigenère com a chave

ABCDEFGHIJKLMNOPQRSTUVWXYZ

- Mensagem:** MACHINE
- Texto cifrado:** MBEKMSK

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

Cifras Polialfabéticas: One-Time Pad



Ano de 1882

Descrita para uso em mensagens telegráficas.



Chave

É uma sequência de caracteres gerada aleatoriamente pelo menos tão longa quanto a mensagem que será enviada.

Cifras Polialfabéticas: One-Time Pad



Uso Único

A chave é usada apenas uma vez na criptografia e descryptografia e nunca mais usada.



Informações Seguras

As mensagens cifradas não fornecem informação sobre a mensagem original, exceto seu tamanho máximo possível



Uso Limitado

Deve-se fazer grandes quantidades de chaves aleatórias e as distribuir ao destinatário.

Cifras Polialfabéticas: One-Time Pad - Exemplo

- **Mensagem:** HELLO
- **Palavra-chave:** XMCKL

+ H (7) E (4) L (11) L (11) O (14)

X (23) M (12) C (2) K (10) L (11)

= 30 16 13 21 25

= E (4) Q (16) N (13) V (21) Z (25)

- **Texto cifrado:** EQNVZ

Cifras Polialfabéticas: One-Time Pad - Exemplo

- **Para descriptografar:** subtrair as letras do texto cifrado com as da palavra-chave. Se der <0 , subtrair de 26;
- **Texto cifrado:** EQNVZ

$$\begin{array}{r} E (4) \quad Q (16) \quad N (13) \quad V (21) \quad Z (25) \\ - X (23) \quad M (12) \quad C (2) \quad K (10) \quad L (11) \\ = 26-19 \quad 4 \quad 11 \quad 11 \quad 14 \\ = H (7) \quad E (4) \quad L (11) \quad L (11) \quad O (14) \end{array}$$

- **Mensagem:** HELLO

Cifras Polialfabéticas: Playfair

Ano de 1854



Vantagens

É fácil de ser implementada e pouco sujeita a erros



Baixa Segurança

A criptoanálise pode ser feita através da análise da frequência de dígrafos, seu interesse é apenas histórico.



Funcionamento

Envolve o uso de uma tabela-chave para organizar as letras alfabéticas em padrões geométricos.

Cifras Polialfabéticas: Playfair - Exemplo

- Primeiro precisa-se criar uma tabela-chave 5x5 sem repetir as letras, por exemplo, com a palavra-chave MONARCHY:

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

- **Obs:** considera-se i/j como uma mesma letra.

Cifras Polialfabéticas: Playfair - Exemplo

- **Mensagem:** INSTRUMENTS
- Precisa-se **separar as letras em pares:**
 - **O par não pode ser feito com a mesma letra:** deve-se adicionar uma letra falsa à letra anterior. Por exemplo: “hello” -> ‘he’ ‘lx’ ‘lo’
 - **Se a letra estiver sozinha no processo de emparelhamento:** precisa-se adicionar uma letra extra falsa com a letra sozinha. “helloe” -> ‘he’ ‘lx’ ‘lo’ ‘ez’
- **Mensagem para criptografar:** IN ST RU ME NT SZ

Cifras Polialfabéticas: Playfair - Exemplo

- Para **criptografar**:
 - **Se ambas as letras estiverem na mesma coluna:** pegue a letra abaixo de cada uma (voltando para a mais ao topo se estiver na parte inferior);
 - **Se ambas as letras estiverem na mesma linha:** pegue a letra à direita de cada uma (voltando para a mais à esquerda se estiver na posição mais à direita);
 - **Se nenhuma das outras regras for verdadeira:** forme um retângulo com as duas letras e pegue as letras no canto oposto horizontal do retângulo.

Cifras Polialfabéticas: Playfair - Exemplo

- Par: **IN** ST RU ME NT SZ

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

- Não estão na mesma linha/coluna -> formar retângulo e pegar letras opostas horizontalmente:
 - I -> G
 - N -> A

Cifras Polialfabéticas: Playfair - Exemplo

- Par: IN **ST** RU ME NT SZ

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

- Estão na mesma linha -> pegar a letra à direita de cada uma (voltando para a mais à esquerda se estiver na posição mais à direita):
 - S -> T
 - T -> L

Cifras Polialfabéticas: Playfair - Exemplo

- Par: IN ST RU **ME** NT SZ

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

- Estão na mesma coluna -> pegar a letra abaixo de cada uma (voltando para a mais ao topo se estiver na parte inferior):
 - M -> C e E -> L
- **Texto cifrado:** GATLMZCLRQTX

Cifras Polialfabéticas: Playfair - Exemplo

- Para **descriptografar**:
 - **Se ambas as letras estiverem na mesma coluna:** pegue a letra acima de cada uma (voltando para a mais embaixo se estiver no topo);
 - **Se ambas as letras estiverem na mesma linha:** Pegue a letra à esquerda de cada uma (voltando para a mais à direita se estiver na posição mais à esquerda);
 - **Se nenhuma das outras regras for verdadeira:** forme um retângulo com as duas letras e pegue as letras no canto oposto horizontal do retângulo.

Cifras Poligráficas

#

A substituição monográfica requer a decomposição do texto plano em caracteres isolados.

pa → l

#

Com a substituição poligráfica, abre-se a possibilidade de uso de conjuntos de caracteres da mensagem.

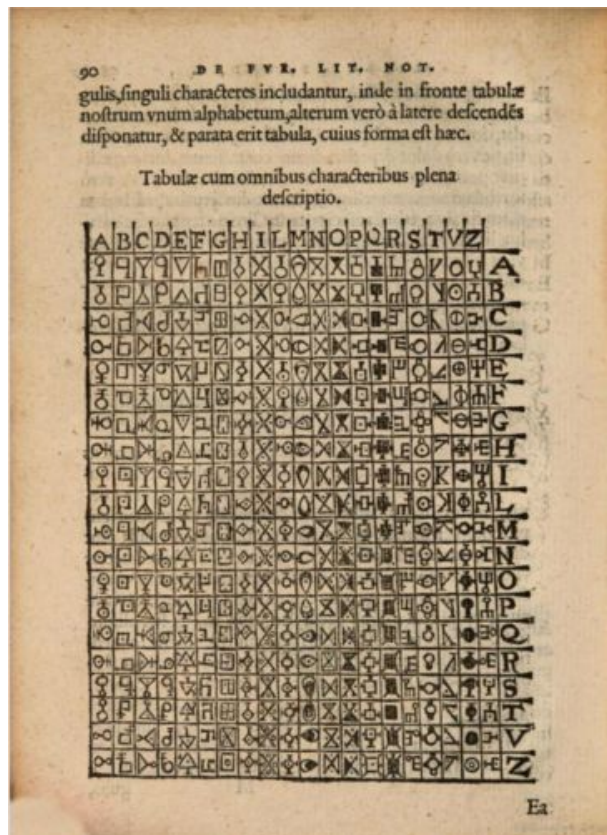
ne → a

#

Os passos de encriptação são da forma $V(n) \rightarrow W(m)$, com $n > 1$.

pane → la

Cifras Poligráficas: Substituição Digráfica ($v^{(2)} \rightarrow w^{(m)}$)



Grafemas

#

O exemplo ao lado foi desenvolvido por Giambattista Della Porta. Para cada grafema, um símbolo/glifo diferente.

#

Os grafemas são as unidades fundamentais dos sistemas de escrita.
No português (ex: *p* e *t* - pato e tato)

Cifras Poligráficas: Substituição Digráfica ($v^{(2)} \rightarrow w^{(m)}$)

Encriptação Digráfica Bipartida

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	...
a	XZ	KJ	YJ	HP	PL	EL	VB	CI	DW	XN	ZL	YP	VN	HH	CC	
b	LP	QT	HE	RS	UR	CR	ZH	GV	WC	HL	YN	KT	WT	MC	KH	
c	DX	MN	AO	NH	SF	GI	WL	MN	AH	GR	BZ	HS	ZU	YM	WU	
d	KM	YZ	RY	FP	TR	CR	XE	JK	NY	PO	GJ	JR	PE	MO	VB	
e	QU	HP	QG	JQ	YQ	OB	SA	NL	PX	OP	VS	AF	XK	XR	UQ	
:																

#

Uma permutação de bigramas recíprocos é semelhante ao que se vê ao lado (Exemplo $V^{(2)} \rightarrow V^{(2)}$).

	a	m	e	r	i	k	b	c	d	f	g	h	j	l	n	...
e	XZ	KJ	YJ	HP	PL	EL	VB	CI	DW	XN	ZL	YP	VN	HH	CC	
q	LP	QT	HE	RS	UR	CR	ZH	GV	WC	HL	YN	KT	WT	MC	KH	
u	DX	MN	AO	NH	SF	GI	WL	MN	AH	GR	BZ	HS	ZU	YM	WU	
a	KM	YZ	RY	FP	TR	CR	XE	JK	NY	PO	GJ	JR	PE	MO	VB	
l	QU	HP	QG	JQ	YQ	OB	SA	NL	PX	OP	VS	AF	XK	XR	UQ	
:																

#

Com o uso de senhas, é possível obter mais etapas de encriptação. No exemplo ao lado, /amerika/ e /equality/.

Cifras Poligráficas: Substituição Digráfica ($v^{(2)} \rightarrow w^{(m)}$)

Encriptação Digráfica Bipartida

K 1 Norw.	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	ca	fn	bl	ou	ih	oo	il	bv	bw	er	rm	qm	mn	ab	zm	ns	wl	yc	zy	tr	du	wo	oa	ho	ic	pu	a
b	sk	wm	dg	ia	cw	pf	if	vd	da	xz	fo	dh	px	rr	iv	gh	mu	ae	qr	tb	og	sr	vu	qg	zt	pm	b
c	hp	no	lj	xp	ji	yf	eo	xh	zu	pl	ft	yv	qw	am	qp	lz	bg	be	lc	nw	ap	vx	rs	yl	wy	gi	c
d	ov	gg	tk	ys	hm	tx	eq	qa	iu	zo	ud	gj	lh	bn	fm	ta	ej	hi	jc	sv	vp	rd	br	rh	kt	tw	d
e	di	wz	qo	pz	ag	wk	fl	uo	ll	oe	ph	jg	gl	vy	lf	af	vt	cj	vq	yz	rz	fc	ps	pq	ro	aq	e
f	cu	rf	nt	xr	ya	tg	xj	db	sc	hg	zr	hs	em	xv	vr	ul	wn	sh	ku	my	va	ad	fg	zp	ut	lb	f
g	sx	hd	vk	st	lk	xf	gn	lv	yr	yd	xg	kr	hc	xl	xw	pa	au	eb	gb	li	id	rj	tz	xq	wd	rn	g
h	bq	oy	sb	mw	qx	zd	ar	po	on	rx	sj	om	as	mb	vs	ke	yy	xy	uj	hb	rc	ig	co	fj	jr	pe	h
i	cb	sl	ri	cf	qt	ek	un	kl	nx	to	hk	ew	yo	wp	kj	kh	su	xi	jo	of	dt	ml	zi	bk	qq	gu	i
j	vv	tf	fi	mp	ky	hl	qc	iq	na	gd	up	tq	hq	xs	xb	wt	ez	mm	hj	vg	eh	dc	qe	ti	uk	cg	j
k	uv	bt	bf	ux	kz	zw	ex	nh	ac	av	tt	aw	ye	dw	dy	nv	wf	dn	sf	eg	lg	wc	kx	ur	pc	od	k
l	ir	ea	kn	le	jb	nu	at	hu	zl	fw	ce	ka	jv	bm	ev	ak	cp	gm	yn	cd	kd	ue	xm	ig	fy	ht	l
m	mv	el	yg	ny	bu	cq	fk	wq	pk	oo	ms	sz	rl	pr	qi	te	qn	kf	gs	uc	kv	kc	dl	kp	cl	lp	m
n	je	sq	gz	ts	dk	vo	xo	ge	mj	qv	mi	dp	vf	rb	yj	bj	mg	vl	qs	uw	rq	pb	mh	lt	oz	qk	n
o	vc	gk	al	vz	np	vm	by	cm	re	wv	uz	yt	ww	gp	js	en	tv	jn	bo	tm	sp	or	fj	ub	ck	td	o
p	hr	ah	ik	xn	mo	zk	ds	in	dz	ym	ci	qu	dv	df	nk	yk	pt	iz	ef	ws	es	ip	fz	ss	jk	ct	p
q	ec	xc	jj	vb	vh	ot	pg	ib	ty	ch	pd	qz	qf	fd	oh	sa	bc	zj	ba	fp	nq	wa	ie	vi	oq	lw	q
r	wi	uq	ln	ja	gq	lo	rp	sd	ko	iy	si	mc	uu	io	yh	ru	xx	qy	fr	hy	ob	ox	nl	uh	fg	ga	r
s	zg	nf	sy	jw	nn	kq	vn	ld	go	mt	pn	jf	he	um	ua	za	xt	bb	op	qh	gf	yl	md	os	ju	ei	s
t	yw	wg	mx	ol	sw	se	rv	yp	us	rk	dx	zs	bz	dj	cn	mf	hx	de	it	ai	ug	mk	ql	cs	ix	pi	t
u	gy	fa	ow	gr	vw	bh	ly	kw	ry	mz	pj	sg	jz	gt	dd	nd	et	az	tp	jh	cx	iw	la	zq	rw	lm	u
v	gv	bi	oi	ii	zb	lj	hz	zh	nb	ks	cy	qj	jx	dq	ma	hf	wr	lq	jp	ng	gw	jl	rg	tl	lr	wh	v
w	aj	gx	nr	qb	uf	ok	rt	xu	bp	wb	qd	jt	mr	aa	pz	yu	nj	xd	eu	mq	hw	nz	ze	km	uy	tn	w
x	kb	yx	ui	pw	we	xk	fe	vj	gc	pp	ep	hh	zn	ha	zf	ax	do	py	nm	xe	ff	so	tc	sm	fb	fx	x
y	fs	ay	ni	wj	wu	fu	ed	an	fv	xa	cv	cz	bs	ve	th	cc	bx	ra	cr	im	ne	hn	zv	oj	yb	tj	y
z	kg	bd	wx	zz	zx	lu	jy	sn	zc	tu	is	ao	dr	ki	ls	ey	qj	ee	lx	hv	nc	dm	jd	me	jm	kk	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	Pr. 0033

Fig. 31a. Bipartite digraphic encryption of the RSHA call signals in Norway

Cifras Poligráficas: Substituição Digráfica ($v^{(2)} \rightarrow w^{(m)}$)

Cifra de Delastelle

#

Nessa cifra, cada caractere está mapeado numa matriz 5x5. As coordenadas das letras são obtidas e combinadas em ordem para gerar novos caracteres.

#

A aplicação desse método resulta numa substituição digráfica bipartida.

	1	2	3	4	5
1	B	O	R	D	E
2	A	U	X	C	F
3	G	H	I	J	K
4	L	M	N	P	Q
5	S	T	V	Y	Z

o n
12 43
14 23
D X

or

o n
1 4 D
2 3 X

Cifras Poligráficas: Substituição Digráfica ($v^{(2)} \rightarrow w^{(m)}$)

Encriptação Digráfica Tripartida

#

Nesse método, cada dígrafo da mensagem original torna-se uma tríade na mensagem criptografada.

	a	b	c	d	e	...
a	148	287	089	623	094	
b	243	127	500	321	601	
c	044	237	174	520	441	
d	143	537	188	257	347	
e

Cifras Poligráficas: Substituição Trigráfica ($V^{(3)} \rightarrow W^{(m)}$)

#

Esse método consiste no uso de grupos de 3 letras da mensagem original ($V^{(3)} \rightarrow W^{(m)}$).

#

Para representar, seria necessário uma matriz tridimensional. Surge aqui uma dificuldade, já que o papel é bidimensional. Pensando num sistema de 26 letras, $26^3=17576$ trigramas.

Análise de Frequência



#

Técnica também conhecida como “contagem de letras”.

#

Técnica que visa a inferência de caracteres criptografados, usando como base as estatísticas gerais da linguagem do texto original.

#

Auxilia na quebra de cifras clássicas (César, Vigenère, entre outras), que não conseguem mascarar suficientemente esse padrão.

Análise de Frequência

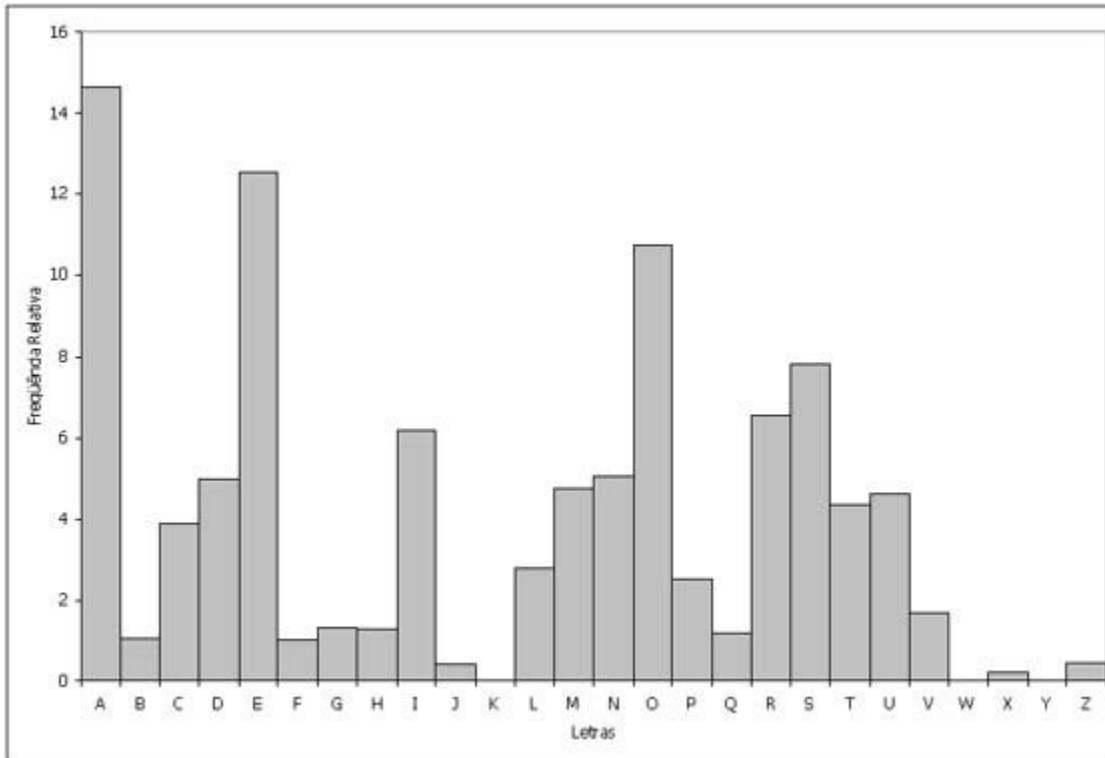


Gráfico de Frequências Relativas para cada letra na Língua Portuguesa.

Fonte:
https://pt.wikipedia.org/wiki/An%C3%A1lise_de_frequ%C3%Aancia

Referências

- BAUER, Friedrich L. **Decrypted Secrets - Methods and Maxims of Cryptology**. Springer, 2000.
- Crypto-IT. Trithemius Cipher. Disponível em:
<https://www.crypto-it.net/eng/simple/trithemius-cipher.html>.
- FIARRESGA, Victor Manuel Calhabrês et al. Criptografia e matemática. 2010. Tese de Doutorado.
- FROEHLICH, Andrew. TechTarget. one-time pad. Disponível em:
<https://www.techtarget.com/searchsecurity/definition/one-time-pad>.
- Geeks for Geeks. Playfair Cipher with Examples. Disponível em:
<https://www.geeksforgeeks.org/playfair-cipher-with-examples/>.

Referências

- Khan Academy. Cifras vs. códigos. Disponível em: <https://pt.khanacademy.org/computing/computer-science/cryptography/ciphers/a/ciphers-vs-codes>.
- SILVA, Willian et al. A Evolução da Criptografia e Suas Técnicas ao Longo da História. 2019.
- SINGH, G. A study of encryption algorithms (rsa, des, 3des and aes) for information security. International Journal of Computer Applications, Foundation of Computer Science, v. 67, n. 19, 2013.
- SMART, Nigel P. **Cryptography made simple**. Springer, 2016.
- TAKATA, Guilherme Ohta. A Criptografia Moderna. Revista Resgates, p. 83.

Referências

- The Guardian. How did the Enigma machine work?. Disponível em: <https://www.theguardian.com/technology/2014/nov/14/how-did-enigma-machine-work-imitation-game>.
- Wiki do Stoa, USP. Criptografia e segurança de rede. Técnicas clássicas de encriptação. Disponível em: <http://wiki.stoa.usp.br/images/c/cf/Stallings-cap2e3.pdf>