Introdução à Criptografia

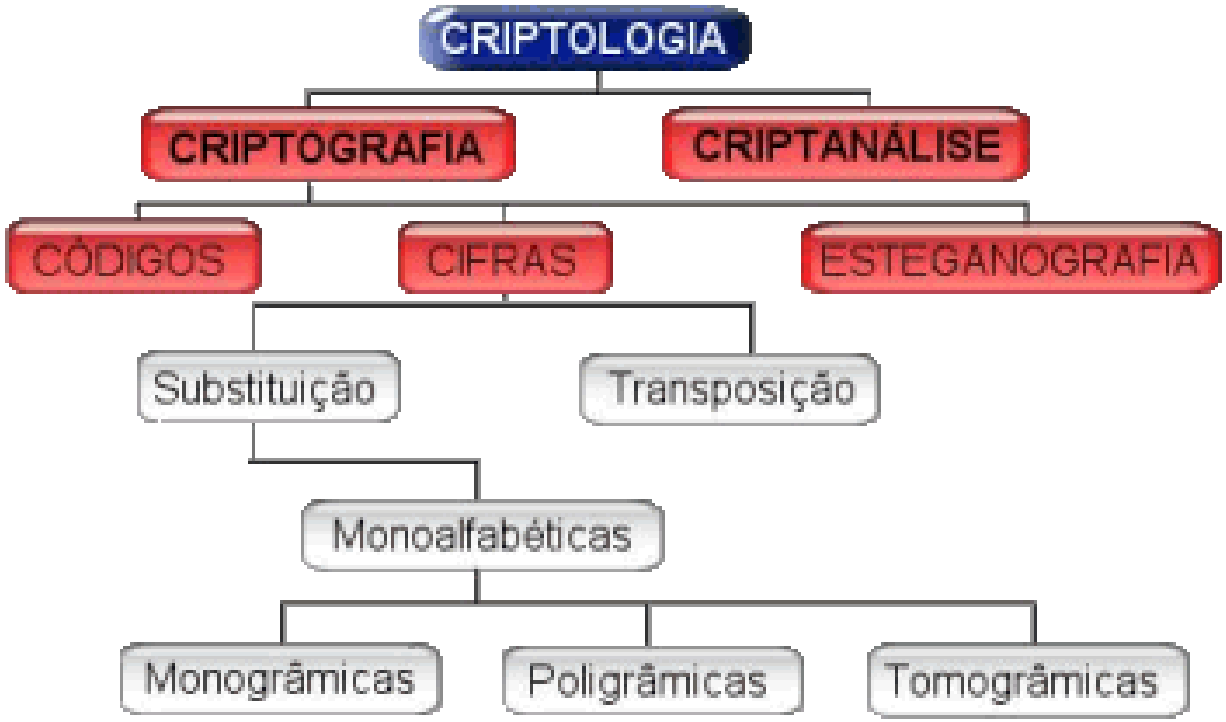
Aspectos Históricos, Cifras Monoalfabéticas e Criptoanálise

Prof. Rodrigo Minetto
rminetto@dainf.ct.utfpr.edu.br
Universidade Tecnológica Federal do Paraná
Material compilado de: O livro dos códigos de Simon Singh.

Sumário

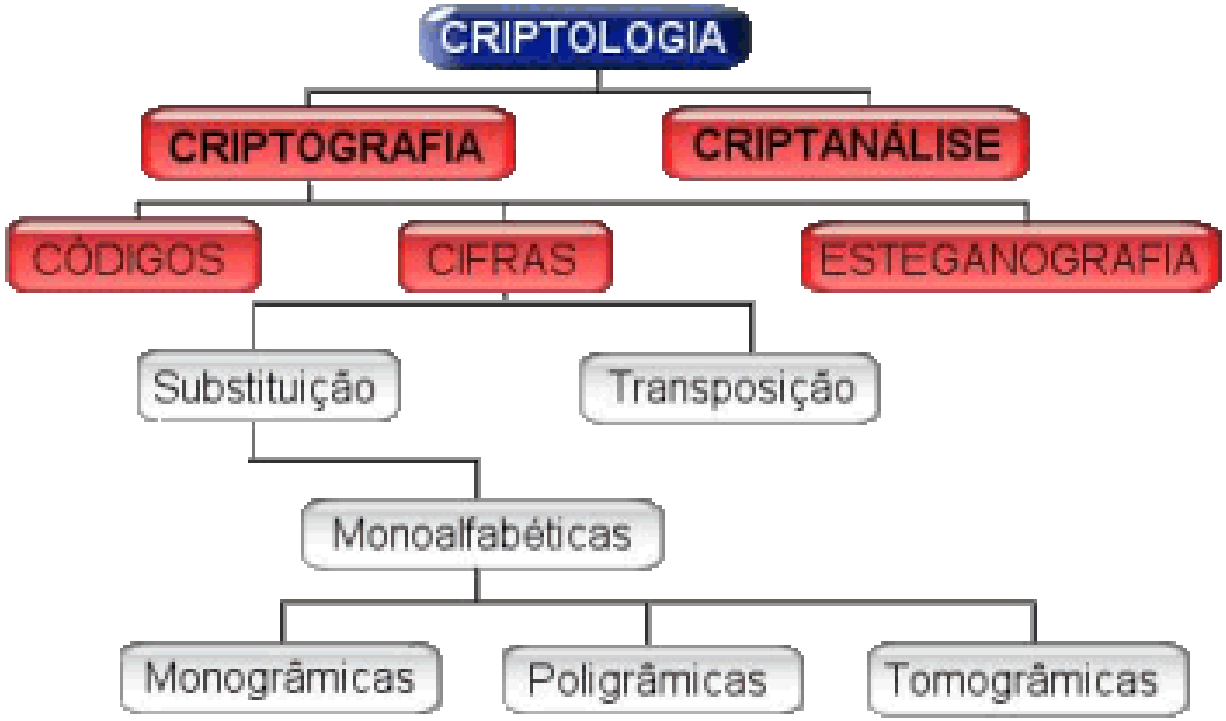
Criptologia

Criptologia: campo científico.



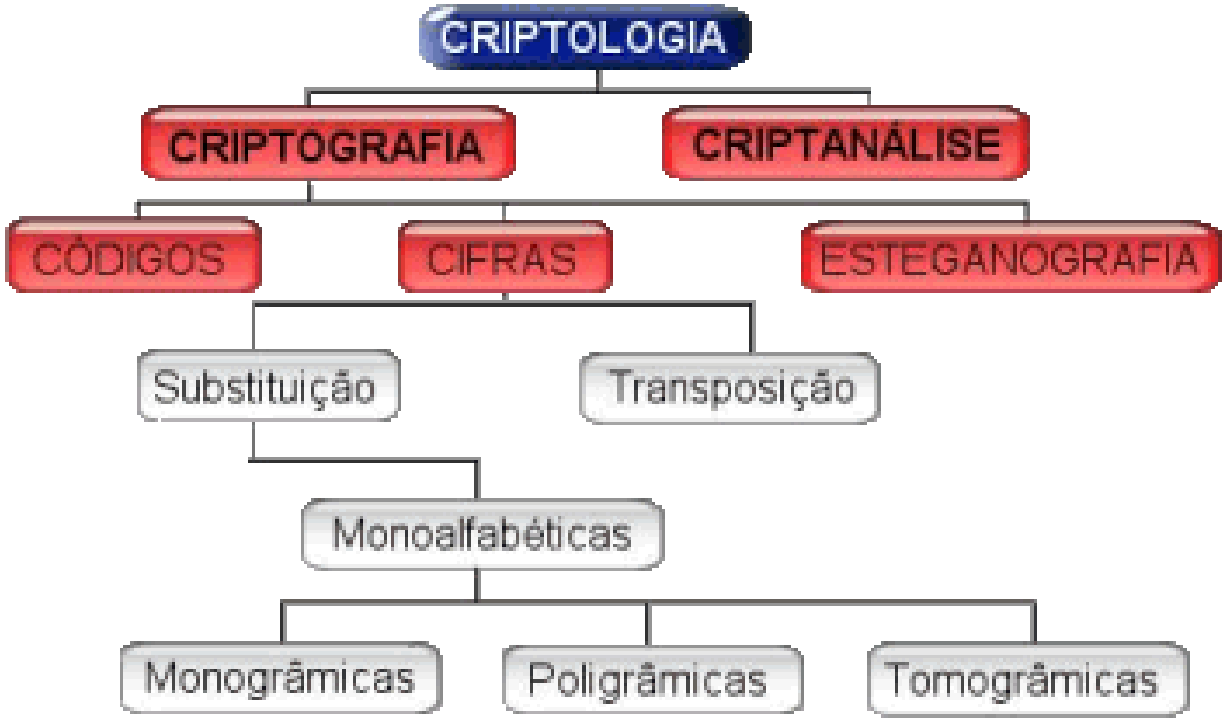
Criptologia

Criptografia: oculta o significado da mensagem, ou seja, a mensagem pode ser vista mas não é possível compreender o seu contéudo. Palavra de origem grega, **kriptos**, "oculto", **graphein**, que significa escrever.



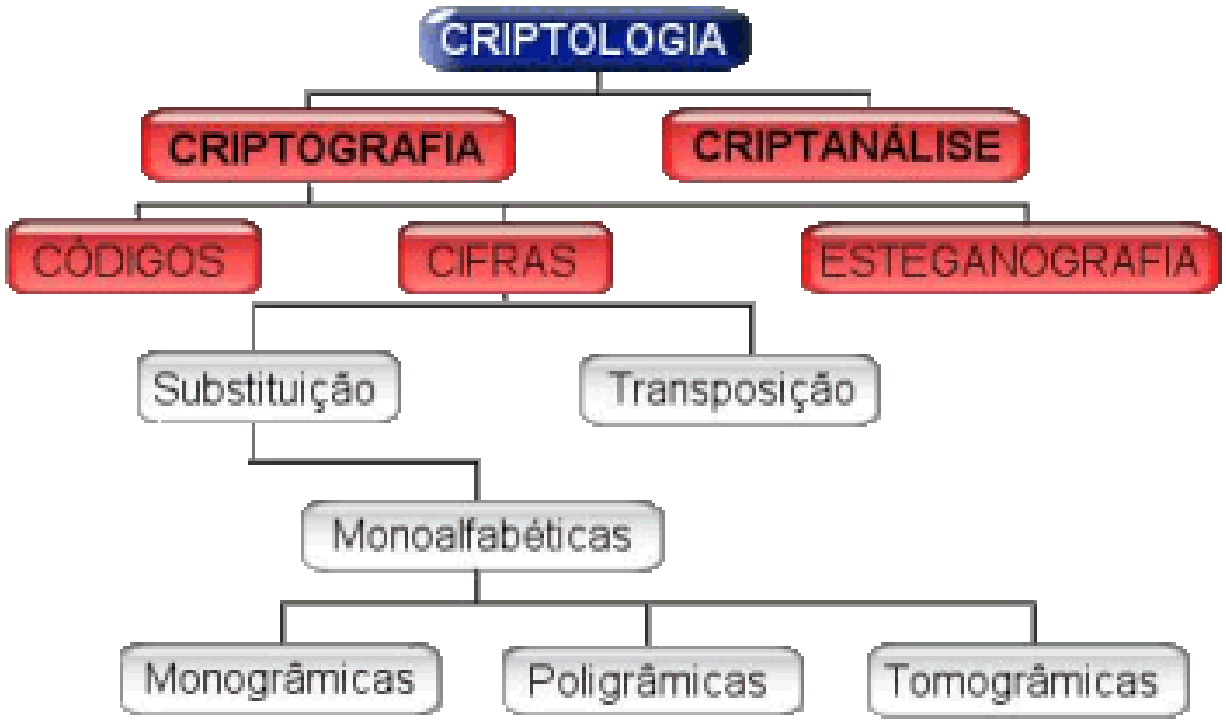
Criptologia

Cripto-análise: é a ciência (arte) de tentar descobrir o texto cifrado e/ou a lógica utilizada em sua encriptação.



Criptologia

Esteganografia: oculta (camufla) a mensagem de forma que sua existência passa despercebida. Palavra de origem grega, **steganos**, que significa coberto e **graphein**, que significa escrever.



Criptografia x Esteganografia

Criptografia	**Esteganografia**
Codifica a mensagem	Não codifica a mensagem
Mensagem segura	Mensagem insegura
Mensagem visível	Mensagem escondida
Prob. maior de ataque	Prob. menor de ataque

Sumário

Esteganografia

Grécia (Atenas e Esparta) x Pérsia (Xerxes) - 480 a.C

Wax table (caderno de cera):

Esteganografia

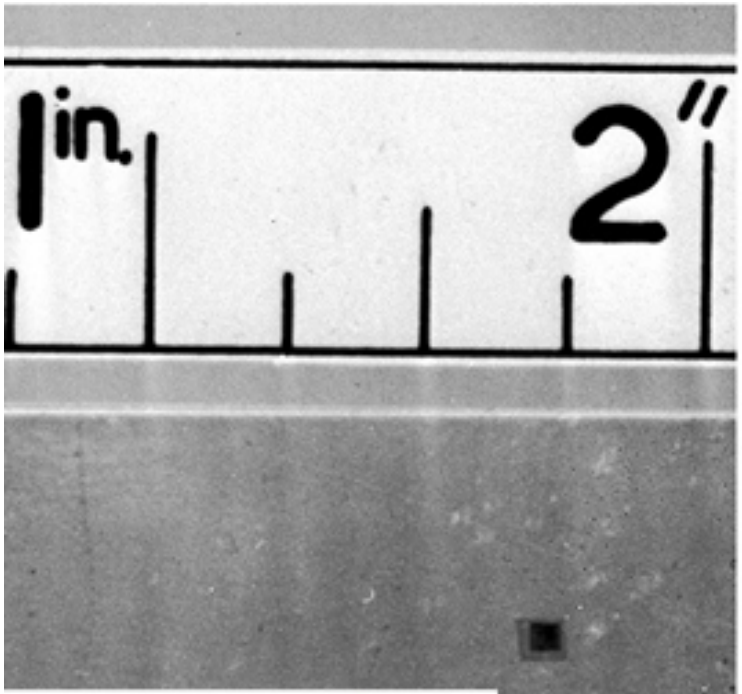
- Escravo com a cabeça raspada, descrito por Heródoto (Grécia).
- Na china antiga escrevia-se mensagem sobre seda fina, que era então amassada até formar uma pequena bolinha e coberta com cera, o mensageiro devia engolir a bolinha.
- No primeiro século d.C Plínio o velho já explicava como o "leite" da planta titímalo podia ser usado como tinta invisível (aquecimento para visualização).

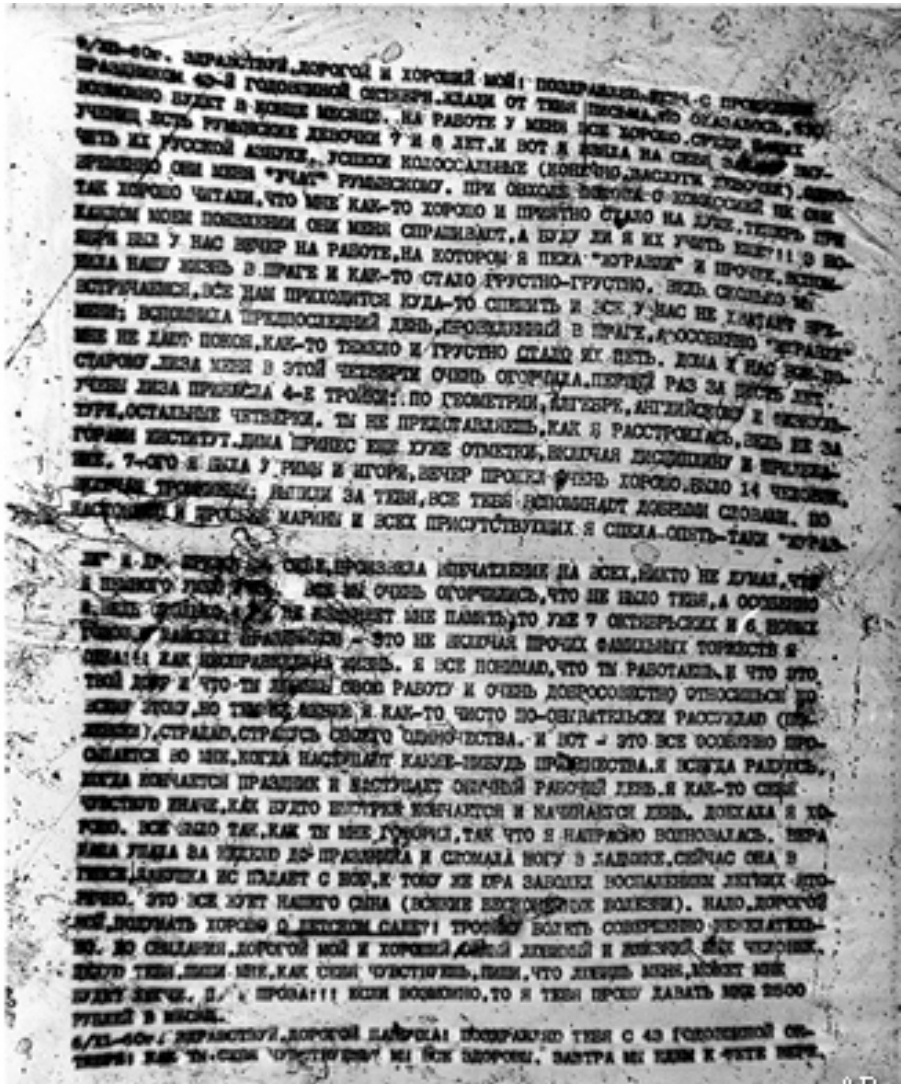
Esteganografia

Giovanni Porta (século XVI): mensagem dentro de um ovo cozido (alume + vinagre).

Esteganografia

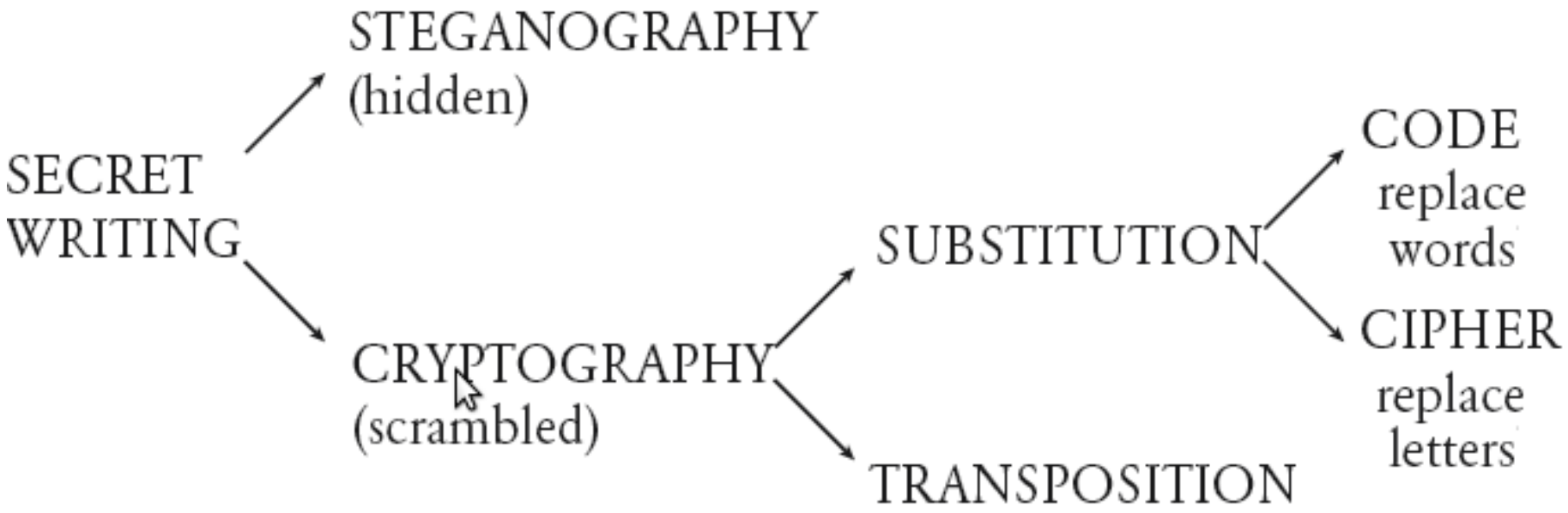
Tecnologia de microdot (muito utilizado na 1 e 2 guerra mundial).





Sumário

Criptografia



The science of secret writing and its main branches.

Criptografia - Cifra de transposição

Criptografia por transposição: as letras da mensagem são rearranjadas, gerando efetivamente um anagrama. Exemplo: transposição por "cerca de ferrovia":

```
TEU SEGREDO É TEU PRISIONEIRO
T U  E R D  É  E  P I I N I O
 E  S G E O  T U  R S O E R
Saída: TUERDÉEPIINIOESGEOTURSOER
```

Criptografia - Cifra de transposição

Citale (bastão de madeira) espartano (404 a.C Lisandro de Esparta)

Criptografia - Cifra de substituição

Uma das primeiras descrições de código por susbtituição aparece no *kama-sutra*, século IV a.C, por Vatsyayana. O livro recomenda que as mulheres devem estudar 64 artes (culinária, vestuário, massagem, . . . , (n. 45) arte da escrita secreta). Uma das técnicas recomendadas envolve o emparelhamento ao acaso das letras do alfabeto.

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

USMQSZLU-CU V CUGD-SQGZU

Criptografia - Cifra de substituição

Cifras bíblicas: o velho testamento continha exemplos óbvios e deliberados de critografia (acrescentar mistério ao texto). Alguns trechos são codificados com o atbash, uma cifra de substituição baseada no alfabeto hebraico (*aleph*, *beth*, . . . , *shin* e *tau*)

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

Criptografia - Códigos

assassinate	= D	general	= Σ	immediately	= 08
blackmail	= P	king	= Ω	today	= 73
capture	= J	minister	= Ψ	tonight	= 28

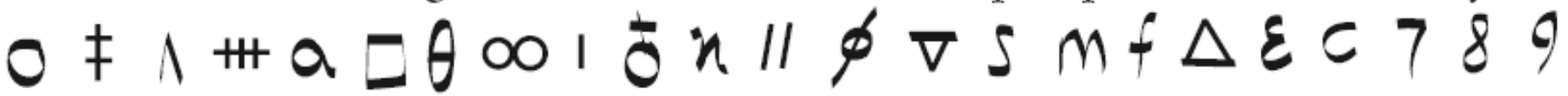
Plain message = assassinate the king tonight
Encoded message = D-Ω-28

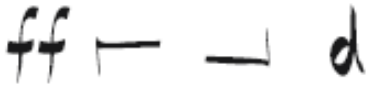
Desvantagens:

- Necessidade de um livro código.
- Transporte e segurança.

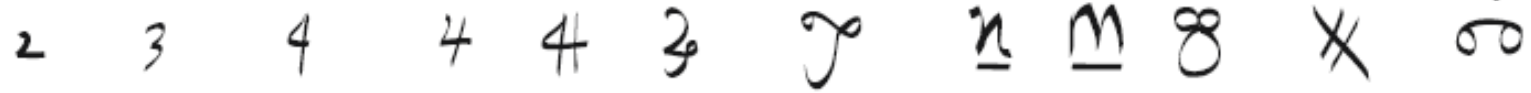
O código de Maria I Stuart (rainha da Escócia)

a b c d e f g h i k l m n o p q r s t u x y z

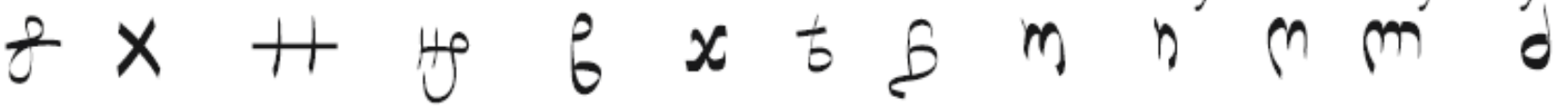


Nulles  Dowbleth

and for with that if but where as of the from by

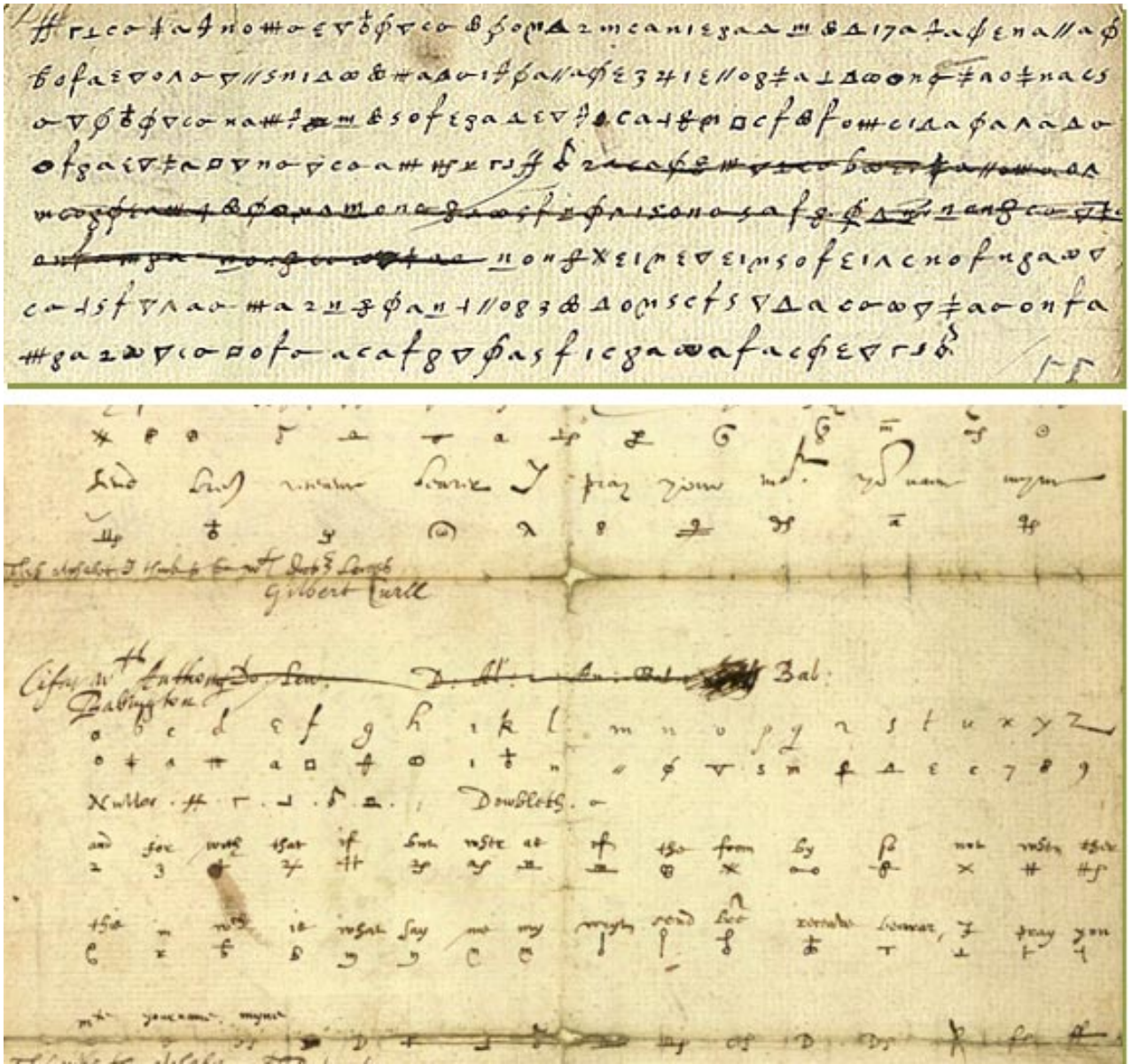


so not when there this in wich is what say me my wyrt



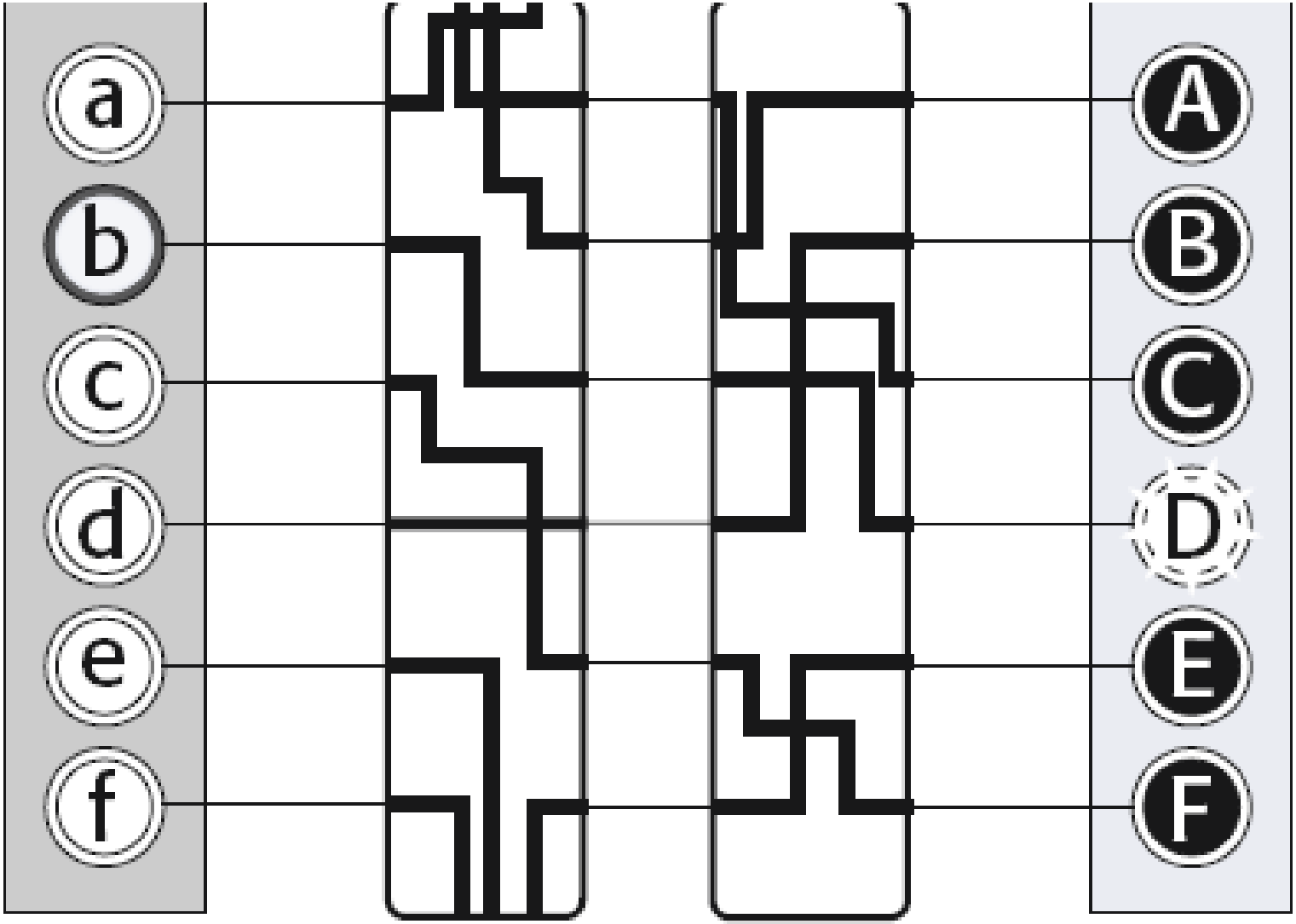
send lr̃e receave bearer I pray you Mte your name myne

O código de Maria I Stuart (rainha da Escócia)

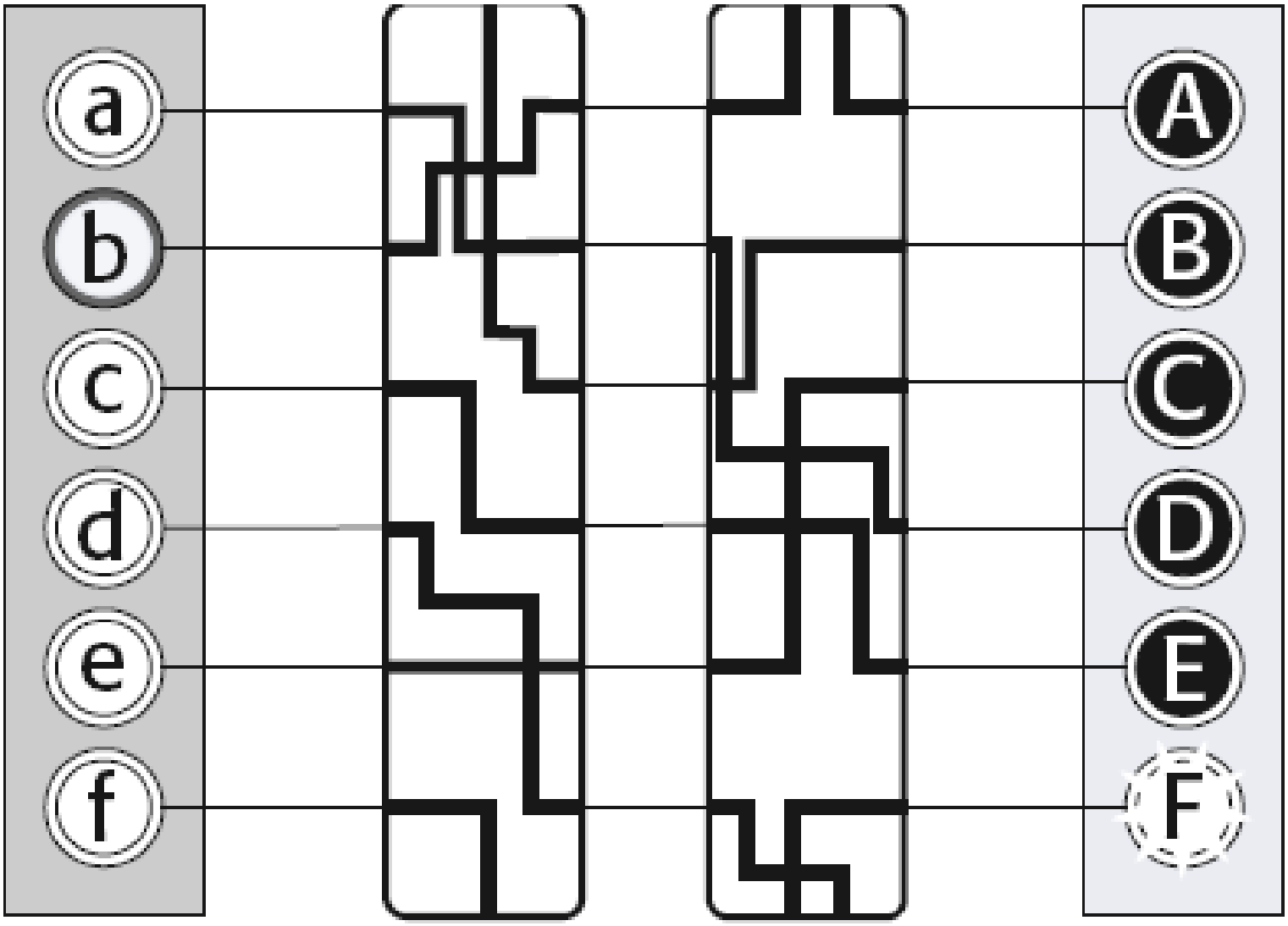


Máquina Enigma (segunda guerra mundial)

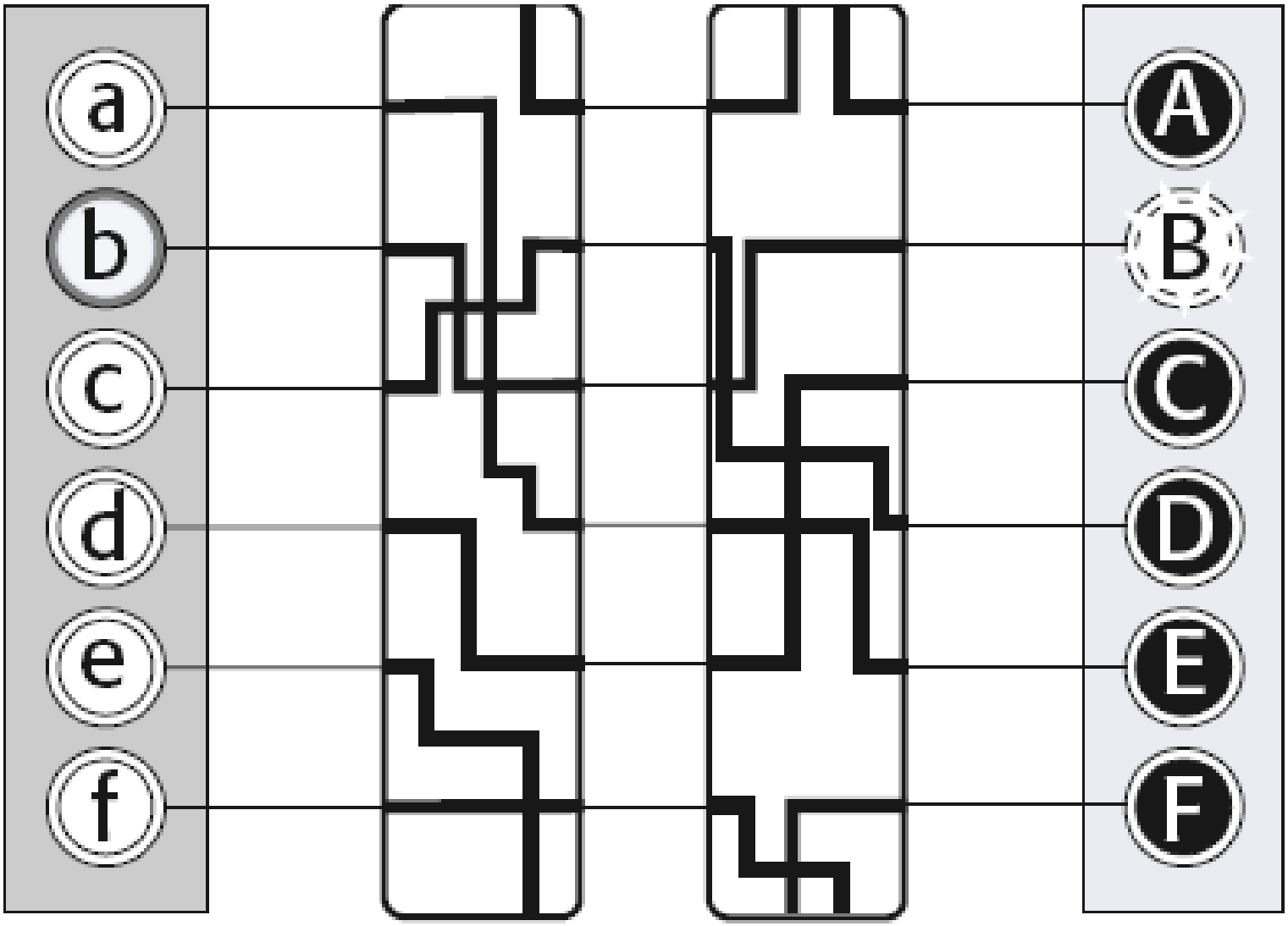
Criptografia - Máquina Enigma



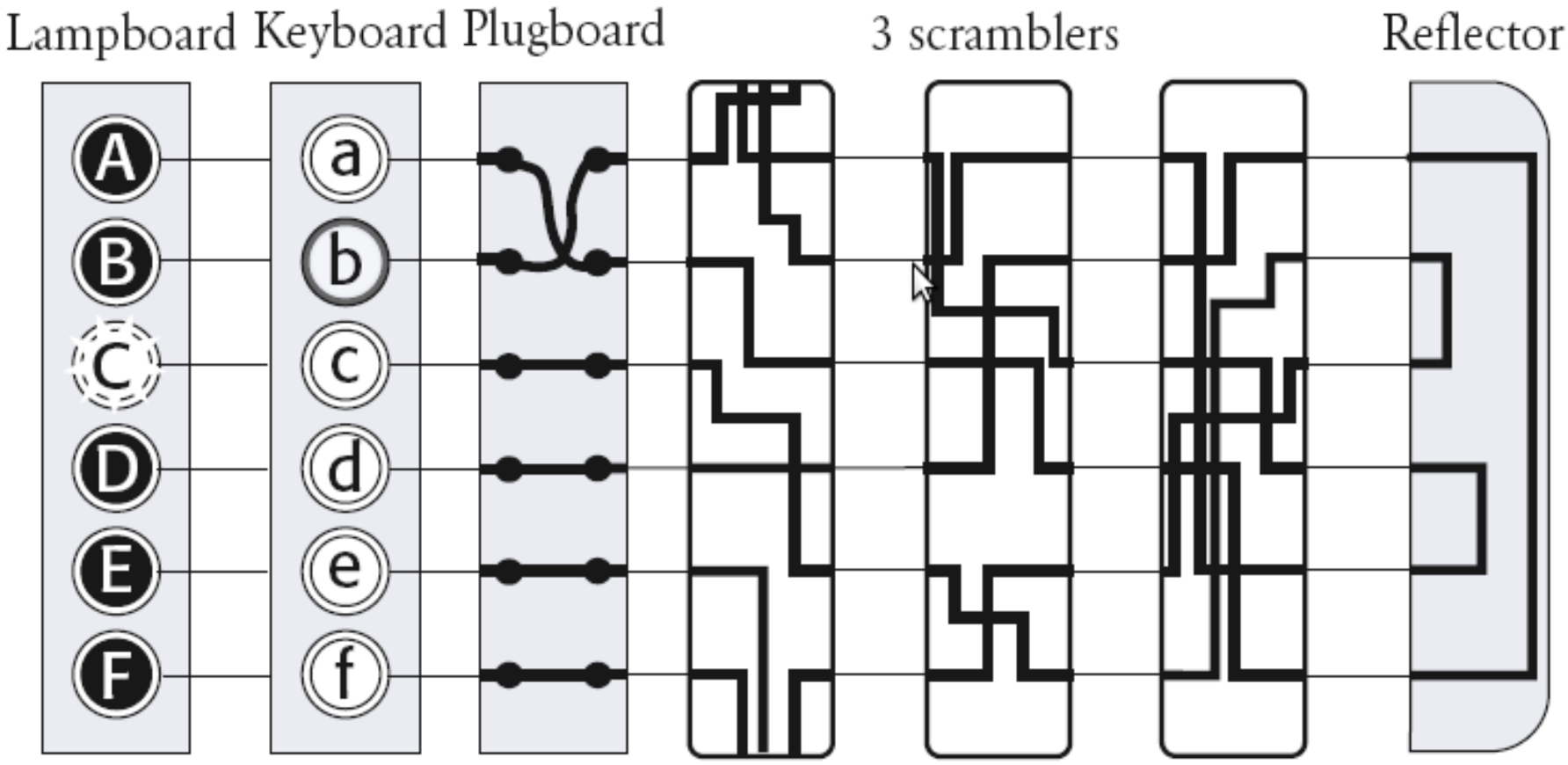
Criptografia - Máquina Enigma



Criptografia - Máquina Enigma



Criptografia - Máquina Enigma



Criptografia - Máquina Enigma

Scrambler orientations. Each of the three scramblers can be set in one of 26 orientations. There are therefore $26 \times 26 \times 26$ settings: 17,576

Scrambler arrangements. The three scramblers (1, 2 and 3) can be positioned in any of the following six orders: 123, 132, 213, 231, 312, 321: 6

Plugboard. The number of ways of connecting, thereby swapping, 6 pairs of letters out of 26 is enormous: 100,391,791,500

Total. The total number of keys is the multiple of these three numbers: $17{,}576 \times 6 \times 100{,}391{,}791{,}500$

≈10,000,000,000,000,000

Criptografia - Definições

Cifrar e decifrar: cifras.

Codificar e decodificar: códigos.

Encriptar e decriptar: cifras e códigos.

Nomenclator: um sistema que usa um alfabeto cifrado, o qual é usado para cifrar a maior parte da mensagem e uma lista limitada de palavras código.

Sumário

Linguagem

Tribo Navarro (segunda guerra mundial)

Linguagem

Pedra de Roseta (Egito).

Linguagem

Curiosidade: em 1652, o jesuíta alemão Athanasius Kircher, o mais respeitado intelectual da época, publicou um dicionário de interpretações dos hieróglifos e o utilizou para produzir uma série de estranhas e maravilhosas interpretações (com imenso impacto para os decifradores da época). Um punhado de hieróglifos, que agora sabemos ser meramente o nome do faraó Apries, foram traduzidos por Kircher como: "*As benesses do divino Osíris devem ser buscadas por meio de cerimônias sagradas e da corrente do Genii, de modo a que as dádivas do Nilo possam ser obtidas*".
— O livro dos códigos de Simon Singh.

Sumário

Enigmas em aberto - Cifra de Beale

Esconde um tesouro de 60 mi/US em ouro/prata.

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84,
56, 239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554,
122, 106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71,
140, 287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316,
101, 41, 78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371,
59, 196, 81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 6,
191, 122, 43, 234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110,
77, 85, 197, 46, 10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14,
20, 37, 105, 28, 248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62,
51, 220, 37, 113, 140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59,
511, 548, 107, 603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33,
30, 5, 38, 8, 14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239,
540, 52, 53, 79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557,
211, 505, 125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138,
115, 48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37,
121, 12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41,
85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49, 47,
64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2, 270,
20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31, 10, 38,
140, 297, 61, 603, 320, 302, 666, 257, 2, 44, 33, 32, 511, 548, 10, 6, 250, 557, 246,
53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106, 160, 113, 31,

Enigmas em aberto - Cifra de Beale

Carta 2 (decifrada) - Declaração de Indepedência-USA

Eu depositei no condado de Bedford, a seis quilômetros de Bud-ford, em uma escavação ou cripta, carca de 1,80 m abaixo da superfície do solo, o seguinte conteúdo, tudo pertencendo às partes cujos nomes serão dados no texto número 3. O primeiro depósito consiste em mil e quatorze libras de ouro e três mil, oitocentas e doze libras de prata, depositadas em novembro de 1819. O segundo depósito foi feito em dezembro de 1821 e consiste em mil novecentas e sete libras de ouro e mil duzentas e oitenta e oito libras de prata. Também há jóias obtidas em St. Louis em troca da prata, para reduzir o peso do material trans-portado, valendo 13 mil dólares. ... O texto número 1 indica a exata localização da cripta, desse modo não haverá dificuldade em encontrá-la.

Enigmas em aberto - Manuscrito de Voynich

Manuscrito da idade média.

Sumário

Cifras Monoalfabéticas

Em criptografia, uma cifra de substituição monoalfabética é aquela onde cada letra do texto em claro é substituída por uma outra letra no texto cifrado, de forma constante. A **cifra de César** é um exemplo dessa classe de cifras.

Cifras Monoalfabéticas

O primeiro documento que relata o uso de uma cifra de substituição para propósitos militares aparece em *Guerras da Gália* de Júlio César. César enviou uma mensagem para Cícero, que estava cercado e prestes a se render. Ele substituiu as letras do alfabeto romano por letras gregas, tornando a mensagem incompreensível para o inimigo — O livro dos códigos de Simon Singh.

Cifra de (deslocamento de) César: César usava a escrita secreta com tanta frequência, que Valerius Probus escreveu todo um tratado sobre cifras, o qual não sobreviveu até a nossa era. No entanto, em *A vida dos Césares*, do século II, Suetônio detalha que uma das cifras de César consistia em **substituir** cada letra da mensagem por outra que estivesse **três** casas à **frente no alfabeto**.

Cifras Monoalfabéticas

Exemplo:

```
    Alfabeto Original
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

    Alfabeto Cifrado
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

Text original: VENI, VIDI, VICI
Text cifrado:  YHQL, YLGL, YLFL
```

Cifras Monoalfabéticas

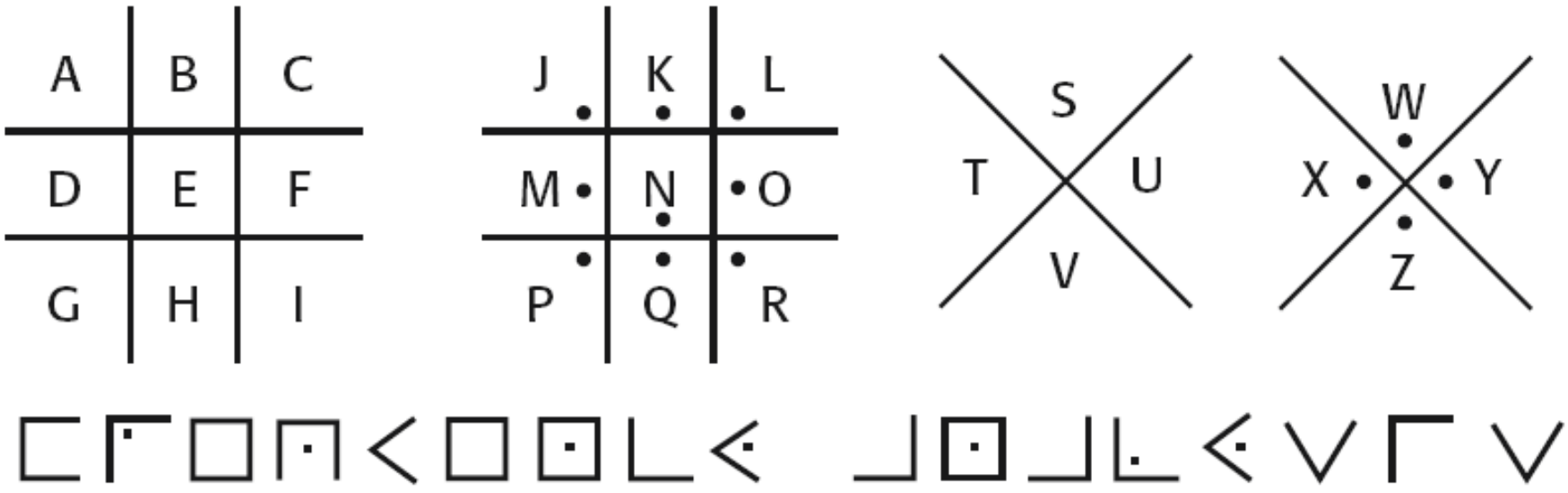
Embora Suetônio só mencione que César deslocava as letras três casas, fica claro que, empregando-se qualquer deslocamento entre 1 e 25 casas, é possível criar 25 códigos diferentes. Augusto, sobrinho de César, também usava a cifra mas deslocando uma casa para à esquerda: B para A, C para B, e assim por diante (que resulta no mesmo número de possibilidades da Cifra de César).

Cifras Monoalfabéticas

É desconhecido o quão efetiva era a cifra de César nesta época, mas é provável que fosse razoavelmente segura, ainda mais porque a maioria dos inimigos de César eram analfabetos e outros presumiam que as mensagens estavam escritas em uma língua estrangeira desconhecida — Josef et.al. Fundamentals of Computer Security. Presumindo que um inimigo pudesse ter acesso a mensagem, não existem registros daquela época de nenhuma técnica para a solução de cifras de substituição simples.

Cifras Monoalfabéticas

A cifra do chiqueiro é outro exemplo de cifra monoalfabética e foi usada pelos maçons em 1700.



Cifras Monoalfabéticas

Se não nos limitarmos a apenas mover as letras do alfabeto, conforme feito na cifra de César, mas permitindo que o alfabeto cifrado seja qualquer rearranjo do alfabeto original, então podemos gerar um número ainda maior de cifras distintas:

$$26 \times 25 \times 24 \times \ldots 2 = 4 \times 10^{26}$$

número equivalente a dez mil vezes o número estimado de estrelas no universo.

Código simples para cifra de substituição

```
int main (int argc, char *argv[]) {
  FILE *ifile = fopen (argv[1], "r"); /*input file!*/
  FILE *ofile = fopen (argv[2], "w"); /*output file!*/
  while (!feof(ifile)) {
    char ch;
    fscanf(ifile,"%c",&ch);
    if (ch == EOF) { break; }
    if (ch == 97)  { ch = 115; } /*a->s*/
    ...
    if (ch == 122)  { ch = 100; } /*z->d*/
    fprintf(ofile,"%c",ch);
  }
  fclose(ifile);
  fclose(ofile);
  return 0;
}
```

Cifras Monoalfabéticas

Nessa codificação mais geral, o ideal é o uso de uma **chave**, que especifica os detalhes exatos de uma codificação em particular. Por exemplo, para usar JULIUS CAESAR como chave, comece removendo qualquer espaço ou letras repetidas **JULISCAER**, assim o alfabeto cifrado poderia ser:

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

Cifras Monoalfabéticas

A importância da chave, em oposição ao algoritmo, é um princípio fundamental da criptografia, conforme definido por Auguste Kerckhoff no livro *La Crytographie Militaire*

Princípio de Kerckhoff

A segurança de um cripto-sistema **não** deve depender da manutenção de um **cripto-algoritmo** em **segredo**. A segurança deve depender apenas em se manter a **chave** em **segredo**.

Sumário

Criptoanálise

Estudiosos árabes inventaram a **criptoanálise**. **Al-Kindi** no século XI publicou *Um manuscrito sobre como decifrar mensagens criptográficas*: ... "um meio de decifrar uma mensagem decodificada, quando conhecemos o seu idioma, é encontrar um texto diferente, na mesma língua, longo como uma página. Analisa-se em ambos a frequência com que cada letra/símbolo aparece. O símbolo que mais aparecer no criptograma deve ser transformado na letra mais frequente do texto de amostra, e assim por diante".

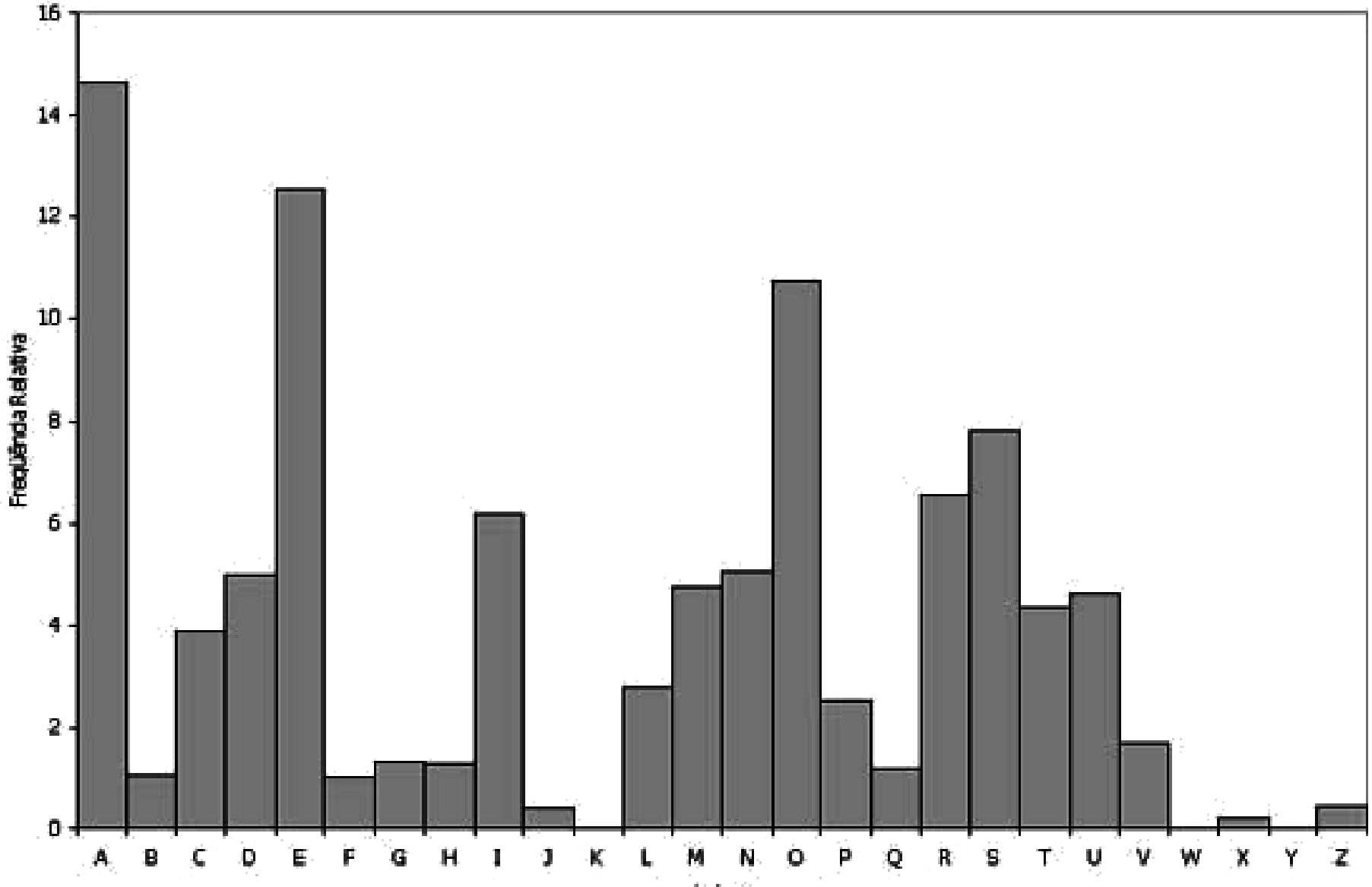
Criptoanálise - Exemplo

```
I ETVYMPKGI JTSTEIXKHI SN MEIZKP T N RIKNE
T RIKZ VNVYPNZN VIKZ SI IRTEKGI PIXKLI T N
QYKLXN RIKNE TR IETI T VNVYPIGIN SN RYLSN
```

I = 18 (17%)	R = 6 (6%)
N = 13 (13%)	Y = 5 (5%)
T = 10 (10%)	S = 5 (5%)
K = 10 (10%)	P = 5 (5%)
E = 7 (10%)	Z = 4 (4%)
V = 6 (6%)	X,L,G = 3 ...

Criptoanálise - Exemplo

Frequência de letras - **Português**



Criptoanálise - Exemplo

LETRAS SOZINHAS	DIGRAMAS COMUNS		TRIGRAMAS COMUNS	
E	DE	UM	QUE	NAO
A	SE	DA	UMA	COM
O	OS	DO	ERA	POR
	AS	EM	MAS	DOS
	NO	NA	LHE	FOI
			ELE	ELA
			DAS	SEU
			SUA	SEM

Criptoanálise - Exemplo

```
I ETVYMPKGI JTSTEIXKHI SN MEIZKP T N RIKNE
T RIKZ VNVYPNZN VIKZ SI IRTEKGI PIXKLI T N
QYKLXN RIKNE TR IETI T VNVYPIGIN SN RYLSN
```

I = 18 (17%)	R = 6 (6%)
N = 13 (13%)	Y = 5 (5%)
T = 10 (10%)	S = 5 (5%)
K = 10 (10%)	P = 5 (5%)
E = 7 (10%)	Z = 4 (4%)
V = 6 (6%)	X,L,G = 3 ...

Criptoanálise - Exemplo

I, N e T devem corresponder a A, E ou O

```
I ETVYMPKGI JTSTEIXKHI SN MEIZKP T N RIKNE
T RIKZ VNVYPNZN VIKZ SI IRTEKGI PIXKLI T N
QYKLXN RIKNE TR IETI T VNVYPIGIN SN RYLSN
```

I = 18 (17%)	R = 6 (6%)
N = 13 (13%)	Y = 5 (5%)
T = 10 (10%)	S = 5 (5%)
K = 10 (10%)	P = 5 (5%)
E = 7 (10%)	Z = 4 (4%)
V = 6 (6%)	X,L,G = 3 ...

Criptoanálise - Exemplo

Substituindo 'I' por 'a' (maior freq.):

```
I ETVYMPKGI JTSTEIXKHI SN MEIZKP T N RIKNE
T RIKZ VNVYPNZN VIKZ SI IRTEKGI PIXKLI T N
QYKLXN RIKNE TR IETI T VNVYPIGIN SN RYLSN
```

I->a	= 18 (17%)	R	= 6 (6%)
N	= 13 (13%)	Y	= 5 (5%)
T	= 10 (10%)	S	= 5 (5%)
K	= 10 (10%)	P	= 5 (5%)
E	= 7 (10%)	Z	= 4 (4%)
V	= 6 (6%)	X,L,G	= 3 ...

Criptoanálise - Exemplo

Substituindo 'I' por 'a' (maior freq.):

```
a ETVYMPKGa JTSTEIXKHa SN MEaZKP T N RaKNE
T RaKZ VNVYPNZN VaKZ Sa aRTEKGa PaXKLa T N
QYKLXN RaKNE TR aETa T VNVYPaGaN SN RYLSN
```

I->a	= 18 (17%)	R	= 6 (6%)
N	= 13 (13%)	Y	= 5 (5%)
T	= 10 (10%)	S	= 5 (5%)
K	= 10 (10%)	P	= 5 (5%)
E	= 7 (10%)	Z	= 4 (4%)
V	= 6 (6%)	X,L,G	= 3 ...

Criptoanálise - Exemplo

Substituindo 'N' por 'o' (devido a T N):

```
a ETVYMPKGa JTSTEIXKHa SN MEaZKP T N RaKNE
T RaKZ VNVYPNZN VaKZ Sa aRTEKGa PaXKLa T N
QYKLXN RaKNE TR aETa T VNVYPaGaN SN RYLSN
```

I->a	= 18 (17%)	R	= 6 (6%)
N->o	= 13 (13%)	Y	= 5 (5%)
T	= 10 (10%)	S	= 5 (5%)
K	= 10 (10%)	P	= 5 (5%)
E	= 7 (10%)	Z	= 4 (4%)
V	= 6 (6%)	X,L,G	= 3 ...

Criptoanálise - Exemplo

Substituindo 'N' por 'o' (devido a T N):

```
a ETVYMPKGa JTSTEIXKHa So MEaZKP T o RaKoE
T RaKZ VoVYPoZo VaKZ Sa aRTEKGa PaXKLa T o
QYKLXo RaKoE TR aETa T VoVYPaGao So RYLSo
```

I->a	= 18 (17%)	R	= 6 (6%)
N->o	= 13 (13%)	Y	= 5 (5%)
T	= 10 (10%)	S	= 5 (5%)
K	= 10 (10%)	P	= 5 (5%)
E	= 7 (10%)	Z	= 4 (4%)
V	= 6 (6%)	X,L,G	= 3 ...

Criptoanálise - Exemplo

Substituindo 'T' por 'e' (devido a T o):

```
a ETVYMPKGa JTSTEIXKHa So MEaZKP T o RaKoE
T RaKZ VoVYPoZo VaKZ Sa aRTEKGa PaXKLa T o
QYKLXo RaKoE TR aETa T VoVYPaGao So RYLSo
```

I->a	= 18 (17%)	R	= 6 (6%)
N->o	= 13 (13%)	Y	= 5 (5%)
T	= 10 (10%)	S	= 5 (5%)
K	= 10 (10%)	P	= 5 (5%)
E	= 7 (10%)	Z	= 4 (4%)
V	= 6 (6%)	X,L,G	= 3 ...

Criptoanálise - Exemplo

Substituindo 'T' por 'e' (devido a T o):

```
a EeVYMPKGa JeSeEIXKHa So MEaZKP e o RaKoE
e RaKZ VoVYPoZo VaKZ Sa aReEKGa PaXKLa e o
QYKLXo RaKoE eR aEea e VoVYPaGao So RYLSo
```

I->a = 18 (17%)	R = 6 (6%)
N->o = 13 (13%)	Y = 5 (5%)
T->e = 10 (10%)	S = 5 (5%)
K = 10 (10%)	P = 5 (5%)
E = 7 (10%)	Z = 4 (4%)
V = 6 (6%)	X,L,G = 3 ...

Criptoanálise - Exemplo

Substituindo 'S' por 'd' (devido a So, Sa e So):

```
a EeVYMPKGa JeSeEIXKHa So MEaZKP e o RaKoE
e RaKZ VoVYPoZo VaKZ Sa aReEKGa PaXKLa e o
QYKLXo RaKoE eR aEea e VoVYPaGao So RYLSo
```

I->a	= 18 (17%)	R	= 6 (6%)
N->o	= 13 (13%)	Y	= 5 (5%)
T->e	= 10 (10%)	S->d	= 5 (5%)
K	= 10 (10%)	P	= 5 (5%)
E	= 7 (10%)	Z	= 4 (4%)
V	= 6 (6%)	X,L,G	= 3 ...

Criptoanálise - Exemplo

Substituindo 'S' por 'd' (devido a So, Sa e So):

```
a EeVYMPKGa JedeEIXKHa do MEaZKP e o RaKoE
e RaKZ VoVYPoZo VaKZ da aReEKGa PaXKLa e o
QYKLXo RaKoE eR aEea e VoVYPaGao do RYLdo
```

I->a	18 (17%)	R	6 (6%)
N->o	13 (13%)	Y	5 (5%)
T->e	10 (10%)	S->d	5 (5%)
K	10 (10%)	P	5 (5%)
E	7 (10%)	Z	4 (4%)
V	6 (6%)	X,L,G	3 ...

Criptoanálise - Exemplo

Substituindo 'E' por 'r' (devido a aEea):

```
a EeVYMPKGa JedeEIXKHa do MEaZKP e o RaKoE
e RaKZ VoVYPoZo VaKZ da aReEKGa PaXKLa e o
QYKLXo RaKoE eR aEea e VoVYPaGao do RYLdo
```

I->a	18 (17%)	R	6 (6%)
N->o	13 (13%)	Y	5 (5%)
T->e	10 (10%)	S->d	5 (5%)
K	10 (10%)	P	5 (5%)
E->r	7 (10%)	Z	4 (4%)
V	6 (6%)	X,L,G	3 ...

Criptoanálise - Exemplo

Substituindo 'E' por 'r' (devido a aEea):

```
a reVYMPKGa JederIXKHa do MraZKP e o RaKor
e RaKZ VoVYPoZo VaKZ da aRerKGa PaXKLa e o
QYKLXo RaKor eR area e VoVYPaGao do RYLdo
```

I->a	18 (17%)	R	6 (6%)
N->o	13 (13%)	Y	5 (5%)
T->e	10 (10%)	S->d	5 (5%)
K	10 (10%)	P	5 (5%)
E->r	7 (10%)	Z	4 (4%)
V	6 (6%)	X,L,G	3 ...

Criptoanálise - Exemplo

Substituindo 'K' por 's' (4 maior freq. - português)

```
a reVYMPKGa JederIXKHa do MraZKP e o RaKor
e RaKZ VoVYPoZo VaKZ da aRerKGa PaXKLa e o
QYKLXo RaKor eR area e VoVYPaGao do RYLdo
```

I->a	18 (17%)	R	6 (6%)
N->o	13 (13%)	Y	5 (5%)
T->e	10 (10%)	S->d	5 (5%)
K->s	10 (10%)	P	5 (5%)
E->r	7 (10%)	Z	4 (4%)
V	6 (6%)	X,L,G	3 ...

Criptoanálise - Exemplo

Substituindo 'K' por 's' (4 maior freq. - português)

```
a reVYMPsGa JederIXsHa do MraZsP e o Rasor
e RasZ VoVYPoZo VasZ da aRersGa PaXsLa e o
QYsLXo Rasor eR area e VoVYPaGao do RYLdo
```

I->a	18 (17%)	R	6 (6%)
N->o	13 (13%)	Y	5 (5%)
T->e	10 (10%)	S->d	5 (5%)
K->s	10 (10%)	P	5 (5%)
E->r	7 (10%)	Z	4 (4%)
V	6 (6%)	X,L,G	3 ...

Criptoanálise - Exemplo

Substituindo 'R' por 'm' (devido a eR)

```
a reVYMPsGa JederIXsHa do MraZsP e o Rasor
e RasZ VoVYPoZo VasZ da aRersGa PaXsLa e o
QYsLXo Rasor eR area e VoVYPaGao do RYLdo
```

I->a	18 (17%)	R->m	6 (6%)
N->o	13 (13%)	Y	5 (5%)
T->e	10 (10%)	S->d	5 (5%)
K->s	10 (10%)	P	5 (5%)
E->r	7 (10%)	Z	4 (4%)
V	6 (6%)	X,L,G	3 ...

Criptoanálise - Exemplo

Substituindo 'R' por 'm' (devido a eR)

```
a reVYMPsGa JederIXsHa do MraZsP e o masor
e masZ VoVYPoZo VasZ da amersGa PaXsLa e o
QYsLXo masor em area e VoVYPaGao do mYLdo
```

I->a	18 (17%)	R->m	6 (6%)
N->o	13 (13%)	Y	5 (5%)
T->e	10 (10%)	S->d	5 (5%)
K->s	10 (10%)	P	5 (5%)
E->r	7 (10%)	Z	4 (4%)
V	6 (6%)	X,L,G	3 ...

Criptoanálise - Exemplo

'masor' não existe no português!

```
a reVYMPsGa JederIXsHa do MraZsP e o masor
e masZ VoVYPoZo VasZ da amersGa PaXsLa e o
QYsLXo masor em area e VoVYPaGao do mYLdo
```

I->a	18 (17%)	R->m	6 (6%)
N->o	13 (13%)	Y	5 (5%)
T->e	10 (10%)	S->d	5 (5%)
K->s	10 (10%)	P	5 (5%)
E->r	7 (10%)	Z	4 (4%)
V	6 (6%)	X,L,G	3 ...

Criptoanálise - Exemplo

Substituindo ‘s’ por ‘i’ (devido a masor)

```
a reVYMPsGa JederIXsHa do MraZsP e o masor
e masZ VoVYPoZo VasZ da amersGa PaXsLa e o
QYsLXo masor em area e VoVYPaGao do mYLdo
```

I->a	18 (17%)	R->m	6 (6%)
N->o	13 (13%)	Y	5 (5%)
T->e	10 (10%)	S->d	5 (5%)
K->i	10 (10%)	P	5 (5%)
E->r	7 (10%)	Z	4 (4%)
V	6 (6%)	X,L,G	3 ...

Criptoanálise - Exemplo

Substituindo ‘s’ por ‘i’ (devido a masor)

```
a reVYMPiGa JederIXiHa do MraZiP e o maior
e maiZ VoVYPoZo VaiZ da ameriGa PaXiLa e o
QYiLXo maior em area e VoVYPaGao do mYLdo
```

I->a = 18 (17%)	R->m = 6 (6%)
N->o = 13 (13%)	Y = 5 (5%)
T->e = 10 (10%)	S->d = 5 (5%)
K->i = 10 (10%)	P = 5 (5%)
E->r = 7 (10%)	Z = 4 (4%)
V = 6 (6%)	X,L,G = 3 ...

Criptoanálise - Exemplo

Substituindo 'Z' por 's' (devido a maiZ)

```
a reVYMPiGa JederIXiHa do MraZiP e o maior
e maiZ VoVYPoZo VaiZ da ameriGa PaXiLa e o
QYiLXo maior em area e VoVYPaGao do mYLdo
```

```
I->a = 18 (17%)  R->m = 6 (6%)
N->o = 13 (13%)     Y = 5 (5%)
T->e = 10 (10%)  S->d = 5 (5%)
K->i = 10 (10%)     P = 5 (5%)
E->r = 7  (10%)  Z->s = 4 (4%)
   V = 6   (6%)     X,L,G = 3 ...
```

Criptoanálise - Exemplo

Substituindo 'Z' por 's' (devido a maiZ)

```
a reVYMPiGa JederIXiHa do MrasiP e o maior
e mais VoVYPoso Vais da ameriGa PaXiLa e o
QYiLXo maior em area e VoVYPaGao do mYLdo
```

I->a	18 (17%)	R->m	6 (6%)
N->o	13 (13%)	Y	5 (5%)
T->e	10 (10%)	S->d	5 (5%)
K->i	10 (10%)	P	5 (5%)
E->r	7 (10%)	Z->s	4 (4%)
V	6 (6%)	X,L,G	3 ...

Criptoanálise - Exemplo

Substituindo 'G' por 'c' (devido a ameriGa)

```
a reVYMPiGa JederIXiHa do MrasiP e o maior
e mais VoVYPoso Vais da ameriGa PaXiLa e o
QYiLXo maior em area e VoVYPaGao do mYLdo
```

```
I->a = 18 (17%)  R->m = 6 (6%)
N->o = 13 (13%)     Y = 5 (5%)
T->e = 10 (10%)  S->d = 5 (5%)
K->i = 10 (10%)     P = 5 (5%)
E->r = 7  (10%)  Z->s = 4 (4%)
   V = 6   (6%)     X,L,G = 3 ...
```

Criptoanálise - Exemplo

Substituindo 'G' por 'c' (devido a ameriGa)

```
a reVYMPica JederIXiHa do MrasiP e o maior
e mais VoVYPoso Vais da america PaXiLa e o
QYiLXo maior em area e VoVYPacao do mYLdo
```

I->a	18 (17%)	R->m	6 (6%)
N->o	13 (13%)	Y	5 (5%)
T->e	10 (10%)	S->d	5 (5%)
K->i	10 (10%)	P	5 (5%)
E->r	7 (10%)	Z->s	4 (4%)
V	6 (6%)	X,L,G	3 ...

Criptoanálise - Exemplo

Substituindo 'V' por 'p' (devido a Vais)

```
a reVYMPica JederIXiHa do MrasiP e o maior
e mais VoVYPoso Vais da america PaXiLa e o
QYiLXo maior em area e VoVYPacao do mYLdo
```

I->a = 18	(17%)	R->m = 6	(6%)
N->o = 13	(13%)	Y = 5	(5%)
T->e = 10	(10%)	S->d = 5	(5%)
K->i = 10	(10%)	P = 5	(5%)
E->r = 7	(10%)	Z->s = 4	(4%)
V->p = 6	(6%)	X,L,G = 3	...

Criptoanálise - Exemplo

Substituindo 'V' por 'p' (devido a Vais)

```
a repYMPica JederIXiHa do MrasiP e o maior
e mais popYPoso pais da america PaXiLa e o
QYiLXo maior em area e popYPacao do mYLdo
```

I->a = 18	(17%)	R->m = 6	(6%)
N->o = 13	(13%)	Y = 5	(5%)
T->e = 10	(10%)	S->d = 5	(5%)
K->i = 10	(10%)	P = 5	(5%)
E->r = 7	(10%)	Z->s = 4	(4%)
V->p = 6	(6%)	X,L,G = 3	...

Criptoanálise - Exemplo

Substituindo 'Y' por 'u' (popYPoso e mYLdo)

```
a repYMPica JederIXiHa do MrasiP e o maior
e mais popYPoso pais da america PaXiLa e o
QYiLXo maior em area e popYPacao do mYLdo
```

```
I->a = 18 (17%)  R->m = 6 (6%)
N->o = 13 (13%)     Y = 5 (5%)
T->e = 10 (10%)  S->d = 5 (5%)
K->i = 10 (10%)     P = 5 (5%)
E->r = 7  (10%)  Z->s = 4 (4%)
V->p = 6   (6%)     X,L,G = 3 ...
```

Criptoanálise - Exemplo

Substituindo 'Y' por 'u' (popYPoso e mYLdo)

```
a repuMPica JederIXiHa do MrasiP e o maior
e mais popuPoso pais da america PaXiLa e o
QuiLXo maior em area e popuPacao do muLdo
```

I->a = 18	(17%)	R->m = 6	(6%)
N->o = 13	(13%)	Y = 5	(5%)
T->e = 10	(10%)	S->d = 5	(5%)
K->i = 10	(10%)	P = 5	(5%)
E->r = 7	(10%)	Z->s = 4	(4%)
V->p = 6	(6%)	X,L,G = 3	...

Criptoanálise - Exemplo

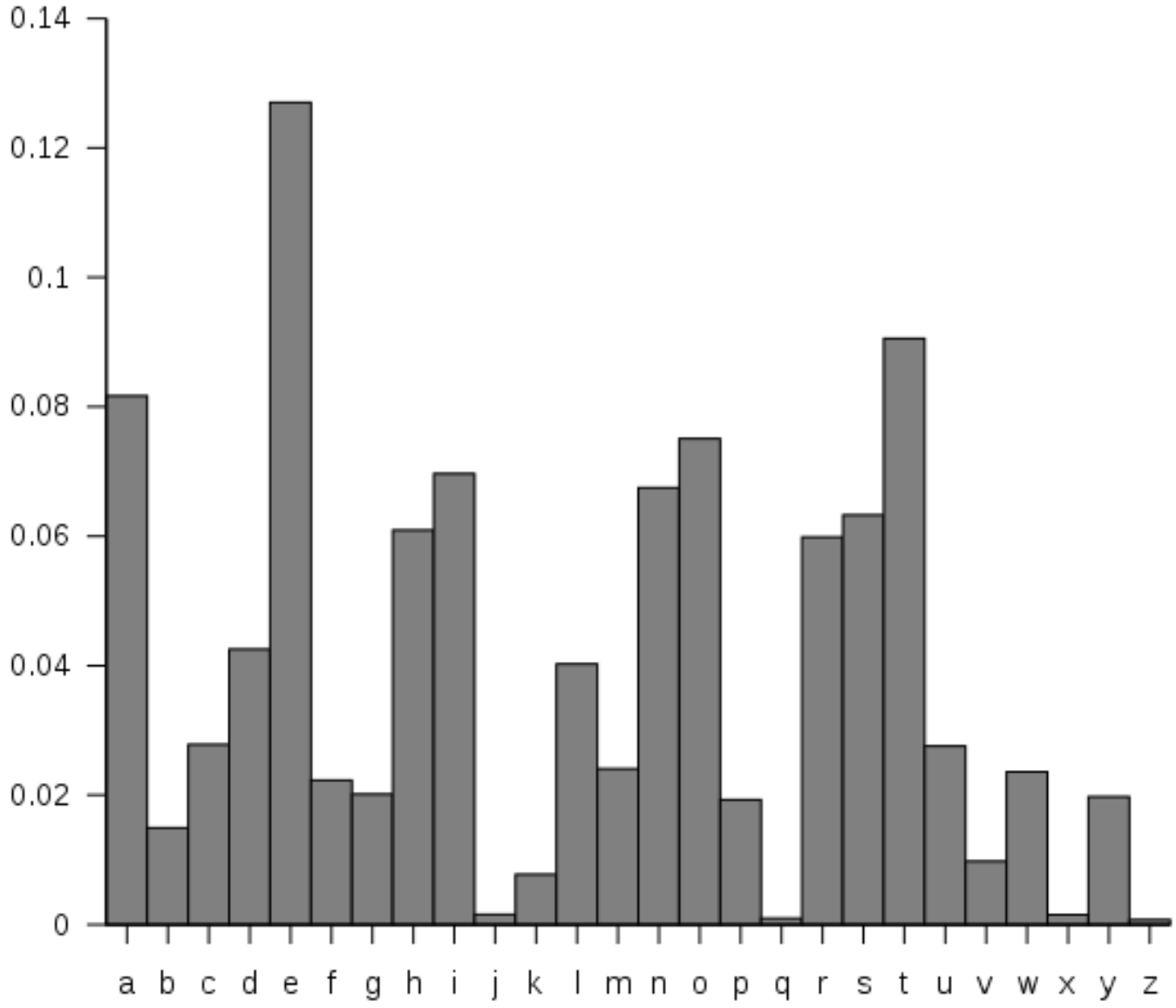
Texto decrifrado:

```
a republica federativa do brasil e o maior
e mais populoso pais da america latina e o
quinto maior em area e populacao do mundo
```

```
I->a = 18 (17%)   R->m = 6 (6%)
N->o = 13 (13%)      Y = 5 (5%)
T->e = 10 (10%)   S->d = 5 (5%)
K->i = 10 (10%)      P = 5 (5%)
E->r = 7  (10%)   Z->s = 4 (4%)
V->p = 6   (6%)      X,L,G = 3 ...
```

Análise de frequência

Frequência de letras - **Inglês**



Criptoanálise

Curiosidade: em 1969 o romancista francês Georges Perec escreveu *La Disparition*, um romance de 200 páginas que não usa palavras que continham a letra **e**. Duplamente extraordinário é o fato de que o crítico e romancista inglês Gilbert Adair conseguiu traduzir o livro mantendo a ausência da letra **e**, obra intitulada *A void*, a tradução é surpreendentemente bem escrita.

Criptoanálise

Curiosidade (renascimento): os criptógrafos da Espanha, ingênuos se comparados ao rivais do resto da europa, mal puderam acreditar quando perceberam que suas mensagens eram perfeitamente legíveis aos franceses. O rei Filipe II da Espanha chegou ao ponto de enviar uma petição ao Vaticano, afirmando que a única explicação para a criptoanálise de François Viéte era a de que ele seria "um arquiinimigo compactuado com o demônio" e que fosse julgado por ações demoníacas. O papa ciente que seus próprios criptoanalistas já liam havia anos as cifras espanholas rejeitou a petição do rei. Com o acontecimento, os criptógrafos espanhóis viram piada em toda a Europa. — O livro dos códigos de Simon Singh.