



# Cifras Clássicas

MI/CEI 2002

José Carlos Bacelar Almeida  
([bacelar@di.uminho.pt](mailto:bacelar@di.uminho.pt))

# Cifras clássicas

## ◆ Cifras por Substituição

O alfabeto da mensagem é transformado no alfabeto do criptograma.

- mono-alfabéticas

Existe uma única substituição envolvida...

- poli-alfabéticas

São várias as substituições envolvidas...

## ◆ Cifras por Transposição

A ordem de ocorrência dos símbolos na mensagem é trocada para a produção do criptograma.



---

# Cifras Mono-Alfabéticas

---

- ◆ Cifra de César
- ◆ Cifra linear
- ◆ Cifra por substituição genérica
- ◆ ...variantes...

# Cifra de César

- ◆ Cifra de César (Utilizada por Júlio César na campanha da Gália)
- ◆  $E(x) = x + k \pmod{26}$
- ◆  $D(y) = y - k \pmod{26}$

+6

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

- ◆ Exemplo: “IGWZGMUKYZGTUUVGVU”

(CartagoEstaNoPapo)

- ◆ N° de chaves: 26 (uma delas “**fraca**”)

# Cripto-análise da C. César

- ◆ Baixo número de chaves permite um ataque por força bruta

CRIPTOGRAMA :	FXLNTQCLOPNPDL	
+1 :	GYMOURDMPQOQEMD	
+2 :	HZNPVSENQRPRFNE	
.... :	.....	
[MSG] +15 :	UMACIFRADECESAR	(K=26-15=11)
.... :	.....	
+24 :	DVJLROAJMNLNBJA	
+25 :	EWKMSPBKNOMOCKB	

- ◆ Análise de frequências permite ataques mais eficientes... (???)  
(alta frequência de 'L' sugere chave ('L'-'A'))

# Cifra Linear

- ◆ Generalização da Cifra de César
- ◆  $E(x) = a*x + b \text{ [mod } 26]$
- ◆ Parâmetros  $a$  e  $b$  devem ser escolhidos de tal forma que  $E(-)$  disponha de inversa...
- ◆ Necessário que  $\gcd(a, 26) = 1$   
...  $26 = 2*13$
- ◆ Número de chaves superior à Cifra de César (quantas?)

# Substituição arbitrária

- ◆ Utiliza uma substituição arbitrária.

$$f : \Sigma \rightarrow \Delta$$

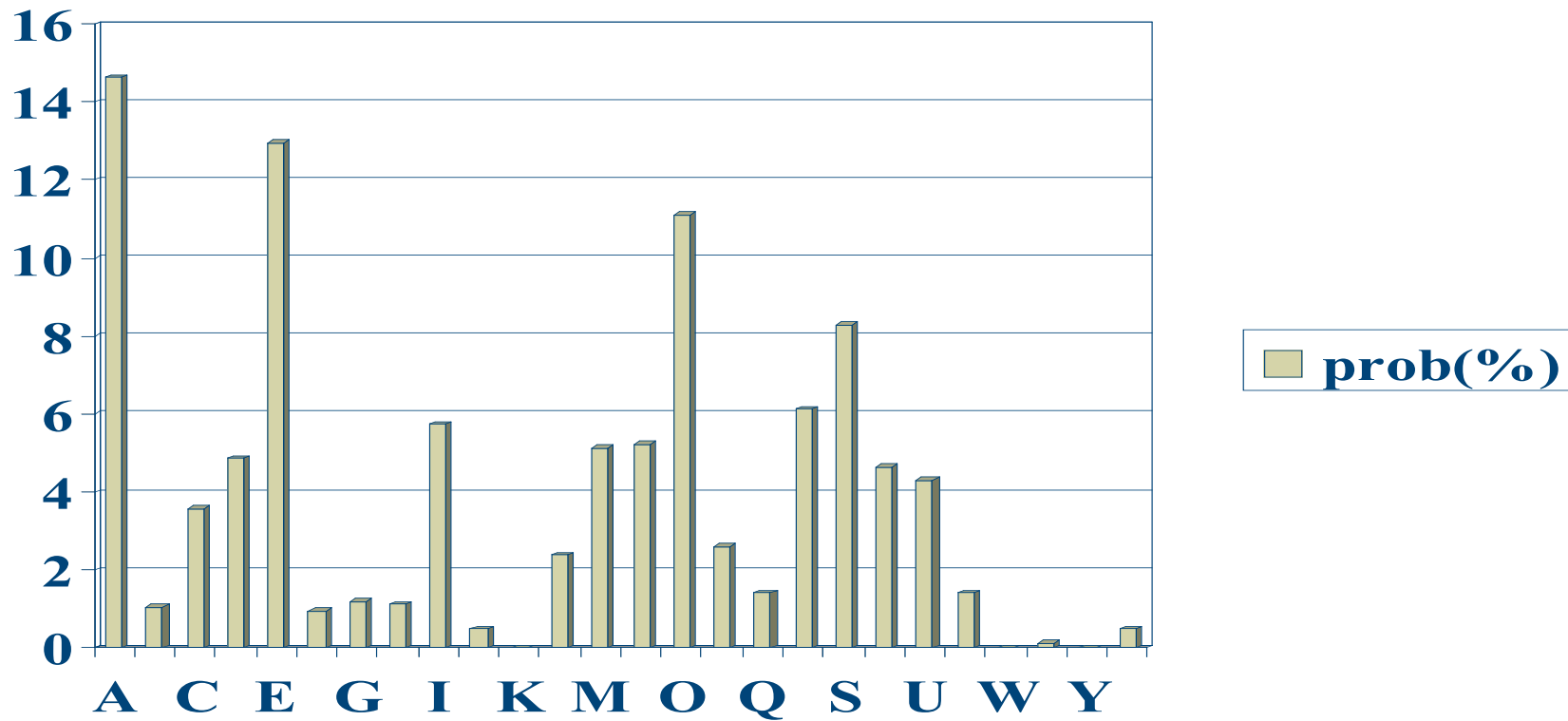
- ◆ Substituição inversa usada na decifragem ( $f^{-1}$ )
- ◆ Muito utilizada em meios diplomáticos nos sec. XVI/XVII.
- ◆ Número de chaves elevado torna inviável ataque por força bruta (sem recurso a meios computacionais)
- ◆  $E(x) = f(x)$
- ◆  $D(y) = f^{-1}(y)$

# Cripto-análise de cifras por substituição

- ◆ Análise de frequências (caracteres, pares, triplos).
- ◆ A descoberta da inversa de um símbolo não revela toda a substituição...
- ◆ Explorar peculiaridades da linguagem (e.g. “qu”; distribuição homogénea das vogais; etc).



# Frequências de caracteres...





# Outros padrões comuns...



- ◆ Pares

AS; OS; ES; RA; DE; EM; DO; AN; QU; AO; MA; AR; EN; TE; TA; UE; ER;...

- ◆ Triplos

QUE; EST; ENT; NAO; ...

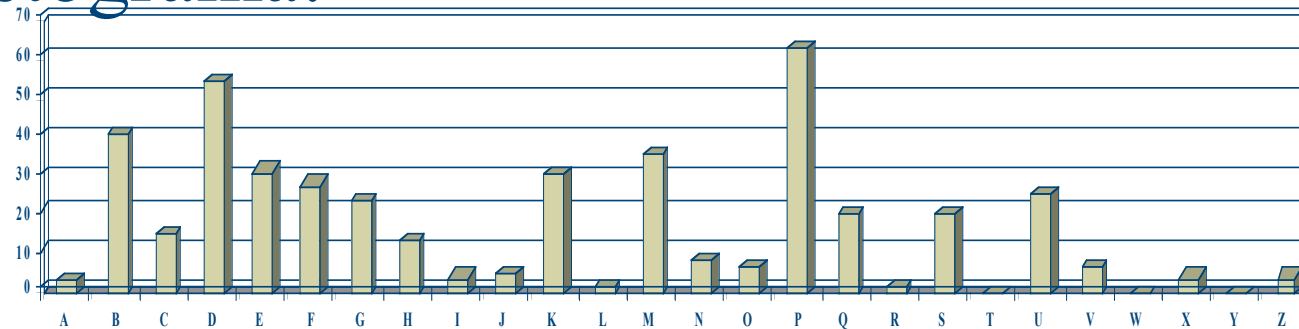
- ◆ Probabilidades condicionais; etc. etc.

# Exemplo de cripto-análise...

## ◆ Criptograma:

FPGFBNBVPKFBMSBEMDMGUCDKDGUGDMUSPMMDBEFLEFEQDCPPGIDEXDCBKPMDHKPMFFQBUGPSUGHKEGPFQB  
MPXPKSESEBSURBHKHBHMEQBFUFSDSBGHKPPFCECPHDKQPDHDKQPFDBADVEDDFDCDDCEZPKLDZEDGMPPMNDKP  
MDGDVPEMPDNUPFQDQVDMPCPZGEFUQBMCPUGMEOPFSEBHPFBMBFBDUNPCDPXSEQDSDBCBBUQBFBCPMUKNEKDG  
UGDMHPKMBFDNPFMCPBKENPGBIMSUKDSBGJUPGPFQKQEVPSBFSEOEDIUOBMPGKPMQDUKDFQPMXPSPFQKESB  
MPMMPMQKDZEDGUGDHPKNUFQDQPKKEVPOBJUPPJUPVDEMUSPCPKKPMHBFCEOAPMJUPFDBMDIEDPPOPMBOADK  
DGHDKDBHKDQBSBGEFJUEPQDSDB

## ◆ Histograma:



# Cripto-análise (cont.)

## ◆ Alguns palpites:

- 'P', 'D', 'B' devem ser imagem de 'A', 'E', 'O'
- PM, PF, MP, KD, PK, KP
- PFQ, KPM, JUP

ME-MO-O-E-MOAS-O-SAS-U-A-A-U-ASU-ESSAO-M--M--A-EE--A--A-O-ESA--ESEM-OU-E-U-----  
EM-OSE-E-----O-U-O--O-OS--OMUM-A-O---EEM---E-A--EA-A--EMAO-A--AMA-AA---E--A--A-  
SEES-A-ESA-A-E-SEA-UEM-A-ASE-E---MU-OS-EU-S--EM--O-EMOSOMOAU-E-AE-----A-AO-OOU-  
OMO-ESU----A-U-AS-E-SOMA-EMS-EO---E-O-S-U-A-O-QUE-EM--E---E-OM----A-U-OSE--ES-  
AU-AM-ESE--EM----OSESSES--A--A-U-A-E--UM-A-E----E-OQUEEQUE-A-SU-E-E--ES-OM----  
ESQUEMAOSA--AEE-ESO--A-A--A-AO--A-O-O--MOU-E-A-AO

# Cripto-análise (cont.)

## ◆ Backtracking...

NE-NO-O-ERNOAS-O-SAS-U-ARA-U-ASU-ESSAO-N--N-TA-EE--A--A-ORESA-RESENTOU-E-U--R--  
ENTOSE-ER----O-U-O-RO-OS-TONUN-A-O--REEN---E-ARTEA-ARTENAO-A--ANA-AA---ER-A--A-  
SEES-ARESA-A-E-SEA-UENTA-ASE-E---NUTOS-EU-S--EN--O-ENOSNOAU-E-AE---TA-AO-OOUTONO-  
ESUR--RA-U-AS-ERSONA-ENS-EOR--E-O-S-URA-O-QUE-ENTRET--E-ON----A-U-OSE-  
RESTAURANTESE--ENTR--OSESSESTRA--A-U-A-ER-UNTATERR--E-OQUEEQUE-A-SU-E-ERRES-ON----  
ESQUENAOSA--AEE-ESO--ARA--ARAO-RATO-O--NQU-ETA-AO

## ◆ ...e continuando...

NEMNOGOVERNOASCOISASMUDARAMUMASUCCESSAOINFINITADEEMBAIXADORESAPRESENTOUMECUMPRIMENTO  
SEXERCICIOCUJOPROPOSITONUNCACOMPREENDIDEPARTEAPARTENAOHAVIANADAADIZERFAZIAMSEESGARE  
SAMAVEISEAGUENTAVASEDEZMINUTOSDEUMSILENCIOPENOSNOAUGEDAEXCITACAODOOUTONODESURGIRAM  
UMASPERSONAGENSDEORIGEMOBSCURACOMQUEMENTRETIVECONCILIABULOSEMRESTAURANTESEXCENTRICO  
SESSESTRAZIAMUMAPERGUNTATERRIVELOQUEEQUEVAISUCEDERRESPONDILHESQUENAOSABIAEELLESOLHAR  
AMPARAOPRATOCOMINQUIETACAO

# Práticas/Extensões...

- ◆ As substituições arbitrárias são difíceis de memorizar/transmitir. Diferentes esquemas foram desenvolvidos para obviar problema.

e.g.

frase chave: CARTAGO ESTA NO PAPO
chave gerada: CARTGOESNPBDFHIJKLMQUVWYZ

- ◆ Análise de frequências é dificultada com a utilização de nulos; sílabas; palavras secretas; substituição homomórfica...

$$f('A') = 32 \vee 63 \vee 231$$



# Cifras Poli-alfabéticas

- ◆ Cifra de *Vigenère*
- ◆ Cifra *AutoKey*
- ◆ Cifra *Book*
- ◆ Cifra *Vernam (one-time-pad)*



---

# Cifra de Vigenère

---

- ◆ Inventada por Blaise Vigenère (finais sec. XVI)
- ◆ “le chiffre indéchiffrable”!!!
- ◆ Utiliza uma combinação de “cifras por deslocamento”
- ◆ Quebrada no sec. XIX por Charles Babbage e Friedrich Kasiski





## Descrição da cifra...



- ◆ Uma chave é utilizada para determinar a substituição a ser utilizada na cifra
- ◆ Tamanho da chave determina número de substituições utilizadas
- ◆ Cada substituição é um simples deslocamento determinado pelo carácter respectivo da chave (c.f. cifra de César)

# Exemplo...

◆ K="BACO"

Chave	<i>B</i>	<i>A</i>	<i>C</i>	<i>O</i>	<i>B</i>	<i>A</i>	<i>C</i>	<i>O</i>	<i>B</i>	<i>A</i>	<i>C</i>	<i>O</i>	<i>B</i>	<i>A</i>	<i>C</i>	<i>O</i>	<i>B</i>
Mensagem	C	I	F	R	A	I	N	D	E	C	I	V	R	A	V	E	L
Criptograma	D	I	H	F	B	I	P	R	F	C	K	J	S	A	X	S	M

◆ tabela de Vigenère...

	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
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
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
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



# Cripto-análise...

- ◆ Descobrir tamanho da chave;
- ◆ Obter informações sobre a chave;
- ◆ Redução a uma cifra mono-alfabética
- ◆ Ataque a essa cifra...

# Teste Kasiski

- ◆ Observação: sequência de caracteres são cifradas da mesma forma quando posicionadas na mesma posição da chave
- ◆ Procurar padrões comuns no criptograma
- ◆ Calcular sua posição relativa (afastamentos)
- ◆ ... sugestão para tamanho da chave:  $\gcd(p_i)$



# Índice de coincidência



- ◆ Inventado em 1920 por Wolfe Friedman
- ◆ Definido como *a probabilidade de dois caracteres aleatórios de um texto serem iguais.*
- ◆ Característica própria de uma linguagem...

## IC (cont.)

- ◆ Seja  $x = x_1 x_2 \dots x_n$  com  $f_i$  ( $0 \leq i < 26$ ) a frequência de ocorrência de cada carácter.

$$Ic(x) = \frac{\sum_{i=0}^{25} f_i * (f_i - 1)}{n * (n - 1)}$$

## IC (cont.)

- ◆ Cada linguagem, com a sua distribuição de probabilidades pelos caracteres própria, dispõe de um valor  $I_c$  esperado característico.

$$\sum_{i=0}^{25} p_i^2$$

- ◆ Distribuição uniforme ( $p_i=1/26$ ):  $I_c = 0.038$
- ◆ ???  $I_c$  em  $\{0,1\}^*$  com  $p(0)=p(1)=.5$  e com  $p(0)=3/4, p(1)=1/4$  ???

# IC (cont.)

- ◆ Alguns valores para IC...

<i>Português</i>	0,0738
<b>Inglês</b>	0.0661
<b>Francês</b>	0.0778
<b>Italiano</b>	0.0738
<b>Alemão</b>	0.0762
<b>Japonês</b>	0.0819
<b>Russo</b>	0.0529
<b>texto aleatório</b>	0.0385

fonte: Basic Methods of Cryptography; Jan C A van der Lubbe



## IC (cont.)

### ◆ Observações:

- Uma substituição mono-alfabética não altera o valor de  $IC$  – espera-se então que o criptograma disponha de um  $IC$  próximo do valor esperado.
- ...mas se múltiplas substituições forem utilizadas o valor de  $IC$  tende a baixar (aproximando-se, no limite, de  $0.038$ ).
- Pode-se assim procurar (confirmar) o tamanho da chave de uma cifra de Vigenère verificando os valores do  $IC$  para diferentes tamanhos.

# Índice de Coincidência Mútua

- ◆ Definido como *a probabilidade de se escolher um carácter de um texto igual ao de um outro texto.*
- ◆ Sejam  $x=x_1x_2\dots x_n$  e  $y=y_1y_2\dots y_n$  com frequências  $f_i$  e  $f'_i$  ( $0 \leq i < 26$ ).

$$MIc(x, y) = \frac{\sum_{i=0}^{25} f_i * f'_i}{n * n'}$$

## ICM (cont.)

- ◆ *??? Qual é o interesse deste teste ???*

Afinal, é fácil de ver que o valor esperado vai coincidir com o de  $I_c$ , i.e.

$$\sum_{i=0}^{25} p_i * p_i$$

- ◆ ... mas podemos investigar o impacto de uma cifra por deslocamento num dos textos...

## ICM (cont.)

- ◆ Se  $x$  e  $y$  forem dois criptogramas cifrados por deslocamento  $k_1$  e  $k_2$ , temos que o valor esperado de MIC é

$$\sum_{i=0}^{25} p_{i-k_1} * p_{i-k_2} = \sum_{i=0}^{25} p_i * p_{i+k_1-k_2} = \sum_{i=0}^{25} p_i * p_{i-k_1+k_2}$$

- ◆ Logo, MIC só depende da distância relativa das chaves  $k_1$  e  $k_2$

# ICM (cont.)

- ◆ Índices de coincidência mútua esperados...

Desvio relativo	valor esperado MIC
0	0.065
1	0.039
2	0.032
3	0.034
4	0.044
5	0.033
6	0.036
7	0.039
8	0.034
9	0.034
10	0.038
11	0.045
12	0.039
13	0.043

obs.: para Inglês...

fonte: Cryptography: theory and practice; Stinson

# Exemplo de cripto-análise

## ◆ Estratégia adoptada:

- Obtenção do tamanho da chave pelo método de Kasiski ( $n$ ).
- Confirmação desse valor pelo cálculo de  $I_c$
- Organização do texto numa matriz de  $n$  colunas – obs.: cada coluna resulta do deslocamento determinado por um dos caracteres da chave.
- Criação de uma tabela com todos os possíveis valores de ICM para pares de colunas (13 para cada par de colunas;  $n!$  entradas na tabela)
- Por inspecção da tabela construída, determinar desvio relativo entre elementos da chave.
- Ataque por força bruta para determinar qual o primeiro carácter da chave.

# cripto-análise (cont.)

## ◆ Teste de Kasiski

"RHB": 41, 221 [180]

"BVV": 37, 67 [30]

$2 \cdot 3 \cdot 5 = 2, 3, 5, \underline{6}, 10, 15, 30$

"GT": 7, 28, 34, 163, 205 [21, 27, 156, 198] [6, 135, 177] [48]

"TV": 94, 164, 181 [70, 87] [17]

"TM": 8, 56, 244 [48, 236] [188]

"RH": 40, 220, 250 [180, 210] [30]

"RG": 126, 198, 204 [72, 78] [6]

"QR": 213, 249, 255 [36, 42] [6]

"QJ": 120, 145, 175 [25, 55] [30]

## ◆ ??? 3 ??? 6 ???

# cripto-análise (cont.)

## ◆ Índice de coincidência

1: 0.04217

2: 0.04545 ; 0.04932

3: 0.05747 ; 0.05640 ; 0.05266

4: 0.04009 ; 0.04864 ; 0.04759 ; 0.04663

5: 0.04354 ; 0.05225 ; 0.05354 ; 0.04977 ; 0.04977

**6: 0.06659 ; 0.07293 ; 0.07610 ; 0.05920 ; 0.07198 ; 0.08195**

7: 0.037 ; 0.038 ; 0.037 ; 0.035 ; 0.039 ; 0.046 ; 0.030

8: 0.043 ; 0.038 ; 0.057 ; 0.043 ; 0.047 ; 0.057 ; 0.056 ; 0.040

## ◆ Tamanho previsível da chave: 6



# cripto-análise (cont.)

## ◆ Índice de Coincidência Mútua

0,1

5.79, 5.73, 5.06, 4.65, 3.1, 4.39, 3.36, 1.65, 1.65, 2.84, 3.31, 4.49, 3.31, 5.06, 4.91, **7.85**, 4.18, 3.72, 3.41, 3.41, 1.81, 1.6, 2.94, 2.89, 4.29, 4.6]

0,2

3.2, 3.2, 3.87, 3.05, 4.18, 4.39, **7.9**, 4.03, 4.03, 3.36, 4.49, 2.79, 2.07, 2.27, 3.82, 2.94, 4.34, 4.8, 6.46, 4.55, 3.82, 4.29, 5.22, 3.67, 1.14, 2.12

0,3

5.22, 4.6, 5.22, 4.55, 5.06, 2.32, 2.58, 4.18, 2.27, 2.79, 2.32, 5.06, 4.03, 5.58, 4.13, 4.86, 4.34, 4.49, 3.25, 3.0, 2.63, 3.36, 3.0, 3.2, 4.29, 3.67

0,4

3.22, 3.38, 4.65, 5.13, 4.18, 4.44, 4.12, 5.07, 3.91, 2.22, 2.54, 3.22, 3.01, 5.02, 3.33, 3.91, 3.81, **7.72**, 3.54, 3.38, 3.38, 4.33, 2.96, 2.48, 3.75, 3.2

0,5

3.44, 4.28, 3.7, 3.01, 1.32, 1.69, 3.33, 4.02, 5.6, 2.91, 4.02, 6.24, **7.93**, 3.22, 2.59, 3.49, 2.96, 2.17, 1.8, 2.85, 3.28, 4.65, 5.23, 5.6, 5.87, 4.81

1,2

3.1, 4.55, 2.58, 5.94, 4.7, 4.96, 4.13, 4.75, 4.7, 2.58, 2.12, 2.74, 2.22, 3.77, 2.89, 3.51, 4.6, **8.26**, 4.34, 5.11, 3.46, 5.27, 2.38, 3.05, 0.83, 3.46

1,3

4.96, 4.39, 5.73, 3.05, 4.24, 2.32, 3.82, 2.43, 2.74, 3.31, 3.15, 5.37, 4.6, 5.48, 4.34, 6.15, 2.74, 2.74, 3.46, 2.43, 2.43, 2.89, 4.24, 3.2, **6.46**, 3.36

1,4

4.07, 2.91, **7.77**, 2.75, 4.18, 3.38, 4.92, 3.22, 4.07, 2.17, 2.96, 3.44, 3.49, 3.22, 4.6, 5.44, 5.07, 4.65, 4.81, 4.33, 2.59, 2.33, 2.91, 2.33, 4.86, 3.54

1,5

3.17, 3.33, 2.06, 2.48, 0.95, 2.96, 5.71, 4.39, 4.33, 5.55, 5.71, 4.23, 4.81, 3.54, 3.81, 2.11, 2.11, 1.64, 2.38, 5.13, 2.91, 4.28, 5.92, **8.4**, 4.28, 3.81

2,3

1.55, 4.65, 1.96, 3.46, 2.53, 4.91, 2.94, 6.61, 3.82, 4.13, 4.65, 5.06, 3.77, 3.1, 2.63, 3.36, 3.87, 2.38, 3.77, 4.13, 4.65, 5.11, 4.55, 4.29, 4.75, 3.36

2,4

3.38, 4.6, 3.38, 4.28, 1.22, 3.75, 2.48, 5.76, 3.01, 3.59, 2.75, **7.88**, 3.01, 3.38, 3.38, 4.55, 2.96, 3.91, 2.7, 2.59, 3.86, 4.33, 3.86, 4.92, 4.12, 6.34

2,5

# cripto-análise (cont.)

## ◆ Previsão da chave $(k_0k_1k_2k_3k_4k_5)$

$$k_1 - k_0 = 15$$

$$k_2 - k_0 = 6$$

$$k_4 - k_0 = 17$$

$$k_5 - k_0 = 12$$

$$k_2 - k_1 = 17$$

$$k_3 - k_1 = 24$$

$$k_4 - k_2 = 2$$

$$k_5 - k_1 = 23$$

$$k_4 - k_2 = 11$$

$$k_5 - k_2 = 6$$

$$k_4 - k_3 = 4$$

$$k_5 - k_4 = 21$$

## ◆ ...que se deduz uma das chaves...

"APGNRM", "BQHOSN", "CRIPTO", "DSJQUP", "ETKRVQ", "FULSWR",  
"GVMTXS", "HWNUYT", "IXOVZU", "JYPWAV", "KZQXBW", "LARYCX",  
"MBSZDY", "NCTAEZ", "ODUBFA", "PEVCGB", "QFWDHC", "RGXEID",  
"SHYFJE", "TIZGKF", "UJAHLG", "VKBIMH", "WLCJNI", "XMDKOJ",  
"YNELPK", "ZOFMQL", "

## cripto-análise (cont.)

- ◆ Uma procura exaustiva revelaria (chave “CRIPTO”):

SE APARECER UM MENSAGEM INESPERADA DURANTE A CONFIGURAÇÃO DO EXCEL NOVAMENTE QUANDO FOR NOVA TENTATIVA DE CONFIGURAÇÃO PODERÁ CRIAR UM FICHEIRO DE REGISTO QUE AJUDA AOS SERVIÇOS DE SUPORTE TÉCNICO DA MICROSOFT A RESOLVER O PROBLEMA DEPOIS DE CRIAR O FICHEIRO CONTACTE OS SERVIÇOS DE SUPORTE TÉCNICO DA MICROSOFT

# Cifra *AutoKey*

- ◆ Generaliza a cifra de Vigenère produzindo uma sequência de chave de tamanho arbitrário.
- ◆ Chave original é estendida com o texto limpo da mensagem a enviar.
- ◆ E.g. (K=“BACO”)

Chave	<i>B</i>	<i>A</i>	<i>C</i>	<i>O</i>	<i>C</i>	<i>I</i>	<i>F</i>	<i>R</i>	<i>A</i>	<i>I</i>	<i>N</i>	<i>D</i>	<i>E</i>	<i>C</i>	<i>I</i>	<i>F</i>	<i>R</i>
Mensagem	<i>C</i>	<i>I</i>	<i>F</i>	<i>R</i>	<i>A</i>	<i>I</i>	<i>N</i>	<i>D</i>	<i>E</i>	<i>C</i>	<i>I</i>	<i>F</i>	<i>R</i>	<i>A</i>	<i>V</i>	<i>E</i>	<i>L</i>
Criptograma	<b><i>D</i></b>	<b><i>I</i></b>	<b><i>H</i></b>	<b><i>F</i></b>	<b><i>C</i></b>	<b><i>Q</i></b>	<b><i>S</i></b>	<b><i>U</i></b>	<b><i>E</i></b>	<b><i>K</i></b>	<b><i>V</i></b>	<b><i>I</i></b>	<b><i>V</i></b>	<b><i>C</i></b>	<b><i>D</i></b>	<b><i>J</i></b>	<b><i>C</i></b>

- ◆ Problema: chave herda redundância da linguagem utilizada. (??? ...e se se utilizar o criptograma ???)

# Cifra *Book*

- ◆ A sequência de chave é retirada de um livro acordado entre as partes (clássicos são candidatos óbvios: bíblia; Alice no país das maravilhas; O memorial do convento; etc.)
- ◆ E.g. (MC, pag. 59)

Levar este pão à boca é gesto fácil, excelente de fazer se a fome o reclama....

- ◆ Problema: redundância da linguagem do “livro” é preservada na chave.

# Cifra de Vernam (*one time pad*)

- ◆ Sequência de chave é “verdadeiramente” aleatória.
- ◆ Descrita originalmente por *Gilbert Vernam* (1917) mas principais propriedades foram só estabelecidas por *Claude Shannon* (1947/9)
- ◆ Interesse é principalmente teórico: tamanho da chave torna-a impraticável.
- ◆ CIFRA PERFEITA! (? o que quer isto dizer ?)



---

# Cifras por Transposição

---

Reordenam os símbolos do texto limpo para produzir o criptograma

- ◆ ...alguns exemplos muitos simples
- ◆ Cifra por transposição de linhas
- ◆ Cifra por transposição de colunas

# Cifras Transposição (cont.)

- ◆ Espelho...

UMAMENSAGEM -> MEGASNEMAMU

- ◆ Linha de comboio...

U A E S G M  
M M N A E      -> UAESGMMMNAE

- ◆ ...

- ◆ Ideia base na cifra: escrever a mensagem de acordo com uma convenção e ler o criptograma com outra convenção. Uma chave pode ser utilizada para determinar um dos processos envolvidos (ou ambos).

- ◆ Decifragem deve inverter procedimento da cifra.



# Transposição de linhas

- ◆ Ideia base consiste em organizar o texto limpo numa matriz com  $n$  colunas (linha a linha).
- ◆ Aplicar uma permutação nas colunas (*write-in key*).
- ◆ O criptograma consiste na releitura da matriz (tb. linha a linha).
- ◆ Decifragem consiste na aplicação da permutação inversa nas colunas (*read-off key*).

# Exemplo de aplicação

- ◆ Chave (permutação) é normalmente representada como uma String

E.g. palavra chave: **BARCO**  
remoção de repetidos: **BARCO**  
ordem lexicográfica (CHAVE): **21534**  
permutação inversa: **21453**

- ◆ Texto limpo: **EXEMPLODEUMACIFRA**

E	X	E	M	P
L	O	D	E	U
M	A	C	I	F
R	A			

X	E	P	E	M
O	L	U	D	E
A	M	F	C	I
A	R			

E	X	E	M	P
L	O	D	E	U
M	A	C	I	F
R	A			

- ◆ Criptograma: **XEPEMOLUDEMFCIAR**

# Cripto-análise C. Transposição

- ◆ Uma distribuição de frequências compatível com a esperada sugere que se trata de uma cifra por transposição.
- ◆ Ideia base: procurar determinar o período (tamanho do bloco) e testar aí as permutações possíveis.
- ◆ Ajudas:
  - Boa base de pares, triplos, etc...
  - Concentrar-se nas permutações que distribuem uniformemente as vogais.
  - ...habilidade para resolver anagramas...

# Exemplo de cripto-análise

## ◆ Quebrar o seguinte criptograma...

**AMSRAASBESAORAOSSESLIAANDUOQESDIACDOELNAPTRLAAUISNIAAT**

AM SR AA SB ES AO RA OS SE SL IA AN DU OQ ES DI AC DO EL NA PT RL AA UI SN IA AT

MA RS AA ...

AMS RAA SBE SAO RAO SSE SLI AAN DUO QES DIA CDO ELN APT RLA AUI SNI AAT

MAS ARA BSE ...

AMSR AASB ESAO RAOS SESL IAAN DUOQ ESDI ACDO ELNA PTRL AAUI SNIA AT

AMSRA ASBES AORAO SSES LI IAAND UOQES DIACD OELNA PTRLA AUISN IAAT

AMARS ASS...

AMARS BSA...

ASARM ABE...

AMSRAA SBESAO RAOSSE SLIAAN DUOQES DIACDO ELNAPT RLAAUI SNIAAT

ASARMA SEOSBA ROESAS SINALA DOSQUE DAOCID ENTALP RAIALU SITANA "136425"

AMSRAAS BESAORA OSSESLI AANDUOQ ESDIACD OELNAPT RLAAUIS NIAAT

**ASARMASEOSBAROESASSINALADOSQUEDAOCIDENTALPRAIALUSITANA**

# Transposição de colunas

- ◆ Cifra consiste em escrever mensagem linha a linha mas ler coluna a coluna (de acordo com chave).
- ◆ Decifragem processa-se de forma dual (escreve colunas de acordo com a chave e lê linha a linha).
- ◆ Quando mensagem não é múltipla do comprimento da chave é necessário cuidado especial na decifragem.
- ◆ E.g. (Chave="cripto" =136425)

E	X	E	M	P	L
O	D	E	U	M	A
C	I	F	R	A	

- ◆ ... criptograma: EOCEEFLAMURXDIPMA
- ◆ ...  $\text{comp.msg}/\text{comp.chave} = 17/6 = 2 + 5/6$

E	X	E	M	P	L
O	D	E	U	M	A
C	I	F	R	A	

# Produto de Cifras

- ◆ Um sistema criptográfico é caracterizado

$$\langle T, C, K, e, d \rangle$$

$$e : K \times T \rightarrow C$$

$$d : K \times C \rightarrow T$$

- ◆  $T$  – espaço de textos limpos
  - ◆  $C$  – espaço de criptogramas
  - ◆  $K$  – espaço de chaves
  - ◆  $e$  – operação de cifra
  - ◆  $d$  – operação de decifragem
  - ◆ tal que:  $d(k, e(k, x)) = x$
- ◆ Se  $C = T$  dizemos que o sistema criptográfico é *endomórfico*.

## Produto de cifras (cont.)

- ◆ Dados os sistemas criptográficos

$$S^1 = \langle T, T, K^1, e^1, d^1 \rangle$$

$$S^2 = \langle T, T, K^2, e^2, d^2 \rangle$$

dizemos que,

$$S^1 \times S^2 = \langle T, T, K^1 \times K^2, e, d \rangle$$

onde :

$$e_{(k_1, k_2)}(x) = e_{k_2}^2(e_{k_1}^1(x))$$

$$d_{(k_1, k_2)}(y) = d_{k_1}^1(d_{k_2}^2(y))$$

## Produto de Cifras (cont.)

- ◆ O produto de cifras é associativo.
- ◆ Quando  $S_1 * S_2 = S_2 * S_1$  os sistemas dizem-se **comutativos**.
- ◆ Quando  $S^2 = S$  o sistema diz-se **idempotente**.
- ◆ Se  $S_1$  e  $S_2$  forem ambos idempotentes e comutarem, então  $S_1 * S_2$  é também idempotente.



# Exercícios

- ◆ Mostre que a cifra de César é idempotente.
- ◆ Mostre que a cifra *affine* pode ser definida como o produto da cifra de César com a cifra multiplicativa (onde  $e_k(x) = k * x \pmod{26}$ ). Mostre ainda que estas cifras comutam.
- ◆ Sejam  $S_1$  e  $S_2$  cifras de Vigenère com chaves de comprimento  $l_1$  e  $l_2$ . Se  $l_2 | l_1$  (i.e.  $l_1 = n * l_2$ ) mostre que  $S_2 * S_1 = S_1 * S_2 = S_1$ .

# Cifra ADFGVX

- ◆ Cifra utilizada pelos Alemães na 1ª grande guerra (quebrada pelos Ingleses).
- ◆ Produto de uma cifra por substituição com uma por transposição – padrão de utilização que ainda hoje encontramos em cifras modernas.
- ◆ Utiliza uma substituição fixa determinada pela tabela:

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

obs.: associa a cada carácter um par (linha,coluna) – e.g. “P”-»”FG”

- ◆ Texto intermédio é cifrado com cifra por transposição de colunas.

# Exemplo de cifra

- ◆ Texto limpo: **PRODUCTIPHERS**
- ◆ Texto intermédio:  
**FGAGVDVFXADGXVDGXFFGVGGAAGXG**
- ◆ Chave: **DEUTSCH (2376514)**

F	G	A	G	V	D	V
F	X	A	D	G	X	V
D	G	X	F	F	G	V
G	G	A	A	G	X	G

- ◆ Criptograma:  
**DXGXFFDGGXGGVVVGVGFGCDFAAAXA**

# Máquinas de cifrar...

- ◆ Em geral, o produto de cifras torna o processo de cifragem demasiadamente complexo para ser realizado manualmente.
- ◆ Surgem assim dispositivos mecânicos responsáveis por essas operações.
- ◆ Exemplo famoso: **Enigma** – máquina utilizada pelos Alemães na 2<sup>a</sup> grande guerra (quebrada pelos Ingleses).



# Referências



- ◆ Cryptography: Theory and Practice – Stinson [cap. 1]
- ◆ The code book – Simon Singh [cap. 1..4]
- ◆ The code breakers – Kahn [cap. 2..8]
- ◆ Elementary Cryptoanalysis, Sinkov – [cap. 1..3]