IPE

Vinicius de Novaes

Fundamentos de Criptografia

Fundamentos de Criptografia

- Quando fazemos compras pela internet, temos que enviar o número do cartão de crédito para efetivar a compra.
- A internet é uma rede pública, e qualquer um pode acessar os pacotes de dados que são transmitidos através dela.

Fundamentos de Criptografia

- Quando fazemos compras pela internet, temos que enviar o número do cartão de crédito para efetivar a compra.
- A internet é uma rede pública, e qualquer um pode acessar os pacotes de dados que são transmitidos através dela.
- É mais seguro se você disfarçar os dados do seu cartão de alguma maneira.
- E é o que fazemos quando, por exemplo, usamos um site que começa com “https” ao invés de “http”.

- Muitas informações podem ser roubadas em conexões pela internet.
- Informações enviadas de/para forças armadas, diplomáticas, cartão de crédito, etc...

- Muitas informações podem ser roubadas em conexões pela internet.
- Informações enviadas de/para forças armadas, diplomáticas, cartão de crédito, etc...
- Portanto além de precisarmos de formas de criptografar e decifrar informações, esse métodos precisam ser dificílimos de derrotar.

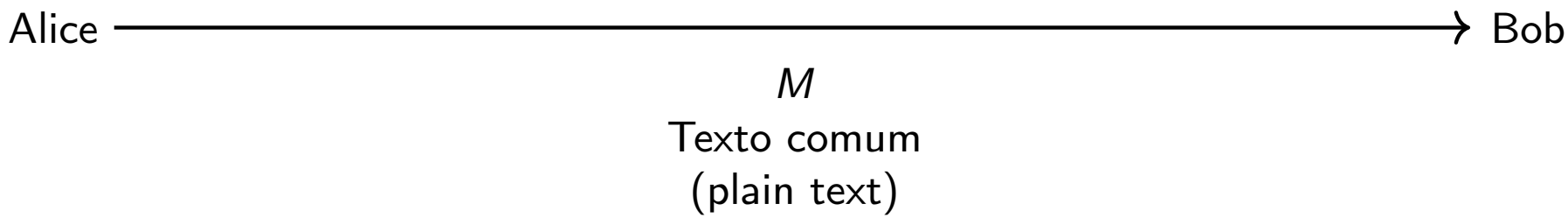
O que é criptografia?

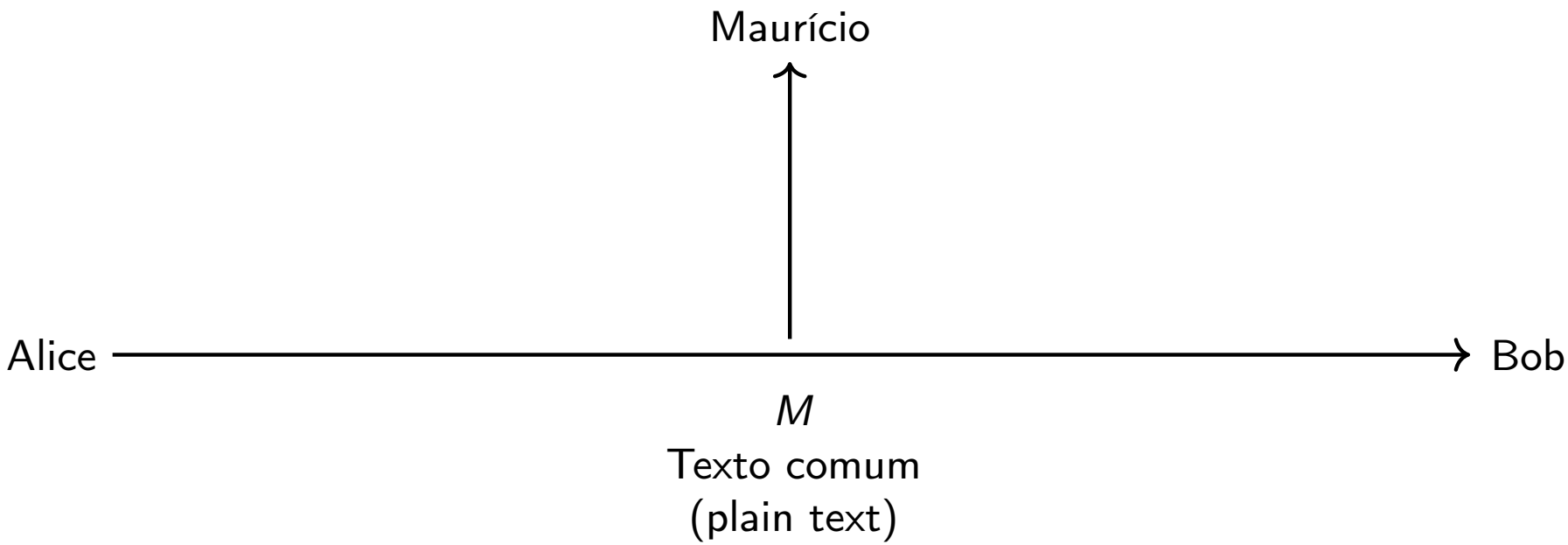
O que é criptografia?

- O estudo das técnicas de fazer comunicação segura entre duas partes, onde existe uma terceira parte que não pode ter acesso à comunicação.

O que é criptografia?

- O estudo das técnicas de fazer comunicação segura entre duas partes, onde existe uma terceira parte que não pode ter acesso à comunicação.
- Imagine uma situação onde a pessoa A manda uma mensagem para a pessoa B, mas somente a pessoa A e a pessoa B podem *entender* a mensagem, apesar da imagem poder ser *acessada* por qualquer pessoa.


Alice
Bob
M
Texto comum
(plain text)


Maurício
Alice
Bob
M
Texto comum
(plain text)

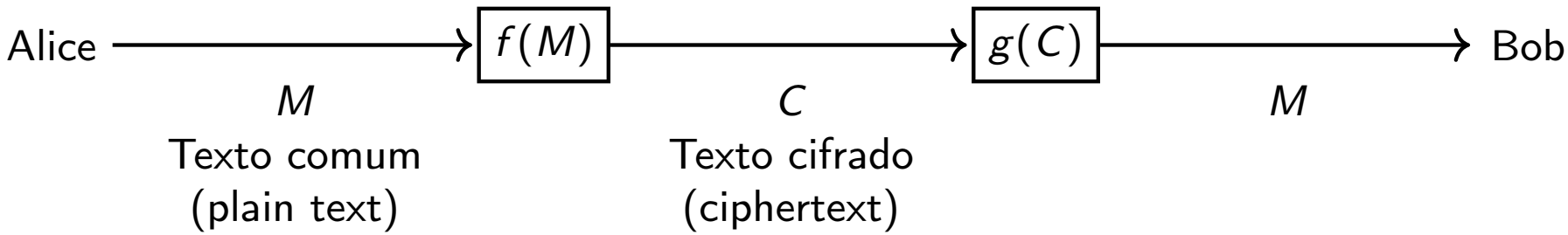
Exemplos

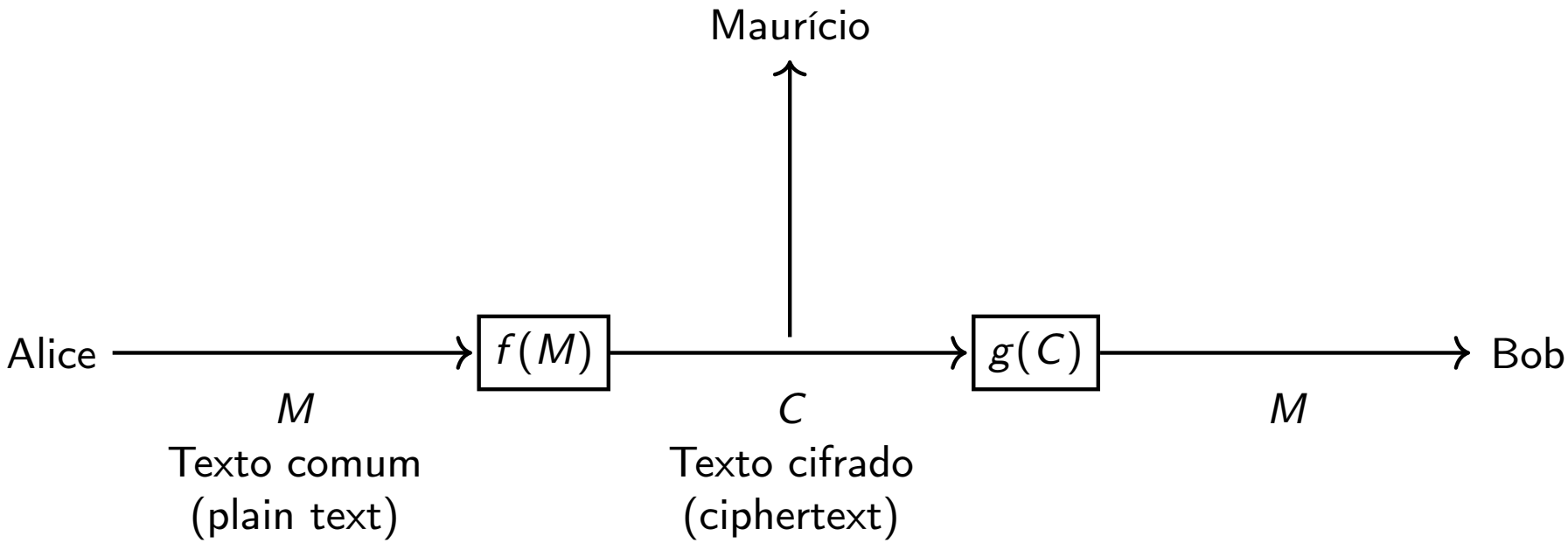
Exemplos

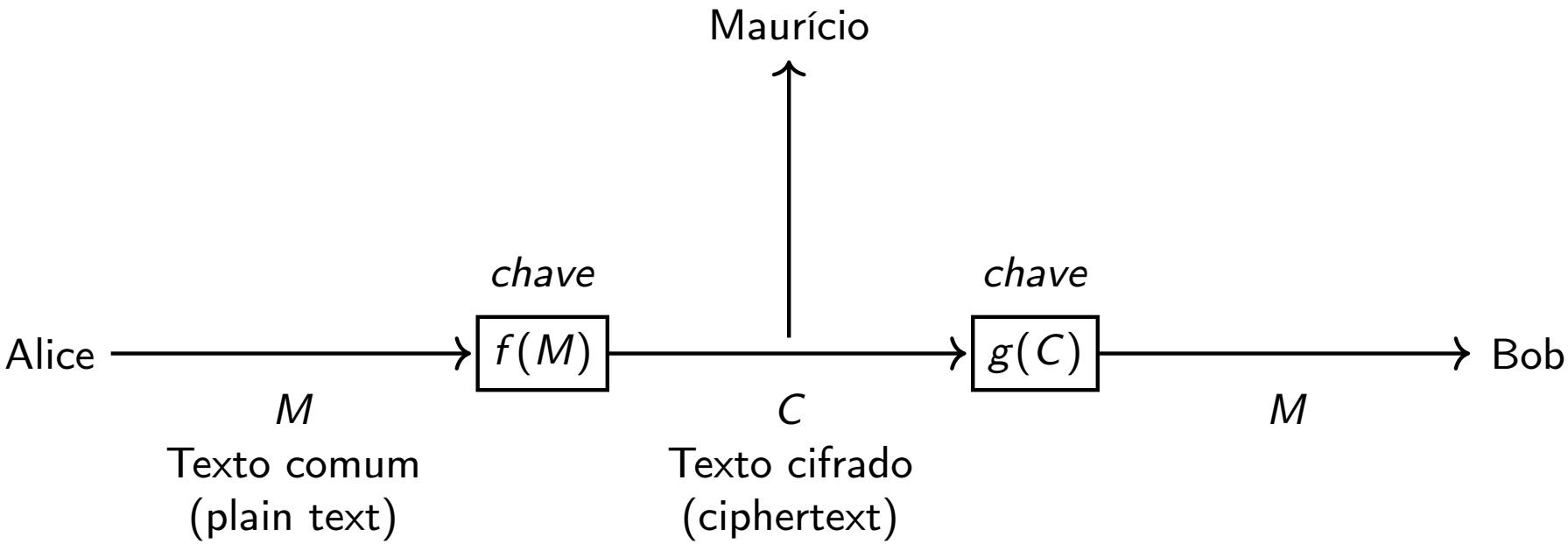
- cartas enviadas que poderiam ser interceptadas sem correr o risco do interceptador conseguir ler o conteúdo. Júlio César, o imperador romano, tinha uma técnica de criptografia para que as cartas fossem enviadas de forma segura.

Exemplos

- cartas enviadas que poderiam ser interceptadas sem correr o risco do interceptador conseguir ler o conteúdo. Júlio César, o imperador romano, tinha uma técnica de criptografia para que as cartas fossem enviadas de forma segura.
- mensagens de rádio que podem ser ouvidas por terceiros, sem que estes terceiros entendam a mensagem. Alan Turing, cientista da computação, ficou famoso por fazer um computador capaz de **quebrar a criptografia** da inteligência nazista durante a segunda guerra mundial.


Alice
$f(M)$
$g(C)$
Bob
M
Texto comum
(plain text)
C
Texto cifrado
(ciphertext)
M


Maurício
Alice
$f(M)$
$g(C)$
Bob
M
Texto comum
(plain text)
C
Texto cifrado
(ciphertext)
M


Maurício
chave
chave
Alice
f(M)
g(C)
Bob
M
C
M
Texto comum
(plain text)
Texto cifrado
(ciphertext)

Cifra de deslocamento

Cifra de deslocamento

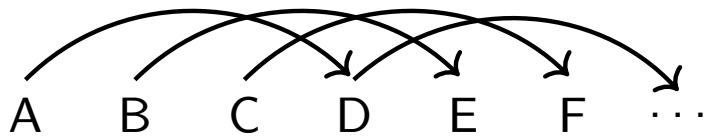
- Supostamente, Júlio César teria se comunicado com seus generais usando uma cifra de deslocamento.

Cifra de deslocamento

- Supostamente, Júlio César teria se comunicado com seus generais usando uma cifra de deslocamento.
- Nessa cifra substitui-se cada letra pela que aparece 3 lugares adiante no alfabeto.

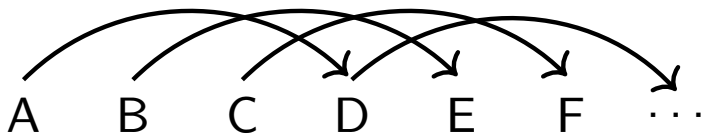
Cifra de deslocamento

- Supostamente, Júlio César teria se comunicado com seus generais usando uma cifra de deslocamento.
- Nessa cifra substitui-se cada letra pela que aparece 3 lugares adiante no alfabeto.



Cifra de deslocamento

- Supostamente, Júlio César teria se comunicado com seus generais usando uma cifra de deslocamento.
- Nessa cifra substitui-se cada letra pela que aparece 3 lugares adiante no alfabeto.



- Nesse caso a *chave* é 3 o que é muito óbvio, então se quisermos usar a cifra de deslocamento, o ideal seria escolher outra chave.

mnocaj ijikxvkj

mnocaj ijikxvkj

0: mnocaj ijikxvkj

mnocaj ijikxvkj

0: mnocaj ijikxvkj
1: lmnb izhihjwuji
2: klmazhyghgivtih
3: jkl ygxfgfhushg

mnocaj ijikxvkj

0: mnocaj ijikxvkj
1: lmnb izhihjwuji
2: klmazhyghgivtih
3: jkl ygxfgfhushg
4: ijkzxfwefegtrgf
5: hijywevdedfsqfe
6: ghixvducdcerped
7: fghwuctbcbdqodc
8: efgvtbsabacpncb
9: defusar a bomba
10: cdetr qz zanla
11: bcdsqzpyzy mk z
12: abcrpyoxyxzljzy
13: abqoxnwxwykiyx
14: z apnwmvwvxjhxw
15: yz omvluvuwigwv
16: xyznluktutvhfvu
17: wxymktjstsugeut
18: vwxljsirsrtfdts
19: uvwkirhqrqsecsr
20: tuvjhqgpqprdbrq
21: stuigpfopoqcaqp
22: rsthfoenonpb po
23: qrsgendmnmoazon
24: pqrfdmclmln ynm
25: opqeclbklkmzxml
26: nopdbkajkjlywlk

mnocaj ijikxvkj

0: mnocaj ijikxvkj
1: lmnb izhihjwuji
2: klmazhyghgivtih
3: jkl ygxfgfhushg
4: ijkzxfwefegtrgf
5: hijywevdedfsqfe
6: ghixvducdcerped
7: fghwuctbcbdqodc
8: efgvtbsabacpncb
9: defusar a bomba
10: cdetr qz zanla
11: bcdsqzpyzy mk z
12: abcrpyoxyxzljzy
13: abqoxnwxwykiyx
14: z apnwmvwvxjhxw
15: yz omvluvuwigwv
16: xyznluktutvhfvu
17: wxymktjstsugeut
18: vwxljsirsrtfdts
19: uvwkirhqrqsecsr
20: tuvjhqgpqprdbrq
21: stuigpfopoqcaqp
22: rsthfoenonpb po
23: qrsgendmnmoazon
24: pqrfdmclmln ynm
25: opqeclbklkmzxml
26: nopdbkajkjlywlk

mnocaj ijikxvkj

0: mnocaj ijikxvkj
1: lmnb izhihjwuji
2: klmazhyghgivtih
3: jkl ygxfgfhushg
4: ijkzxfwefegtrgf
5: hijywevdedfsqfe
6: ghixvducdcerped
7: fghwuctbcbdqodc
8: efgvtbsabacpncb
9: defusar a bomba
10: cdetr qz zanla
11: bcdsqzpyzy mk z
12: abcrpyoxyxzljzy
13: abqoxnwxwykiyx
14: z apnwmvwvxjhxw
15: yz omvluvuwigwv
16: xyznluktutvhfvu
17: wxymktjstsugeut
18: vwxljsirsrtfdts
19: uvwkirhqrqsecsr
20: tuvjhqgpqprdbrq
21: stuigpfopoqcaqp
22: rsthfoenonpb po
23: qrsgendmnmoazon
24: pqrfdmclmln ynm
25: opqeclbklkmzxml
26: nopdbkajkjlywlk

defusar a bomba

Cifra de substituição simples

Cifra de substituição simples

- Na cifra de deslocamento existem 26 chaves distintas, fácil de testar todas.

Cifra de substituição simples

- Na cifra de deslocamento existem 26 chaves distintas, fácil de testar todas.
- Mas podemos fazer algo mais seguro substituindo cada carácter por outro qualquer, não necessariamente o que está a 3 posições no alfabeto.

Cifra de substituição simples

- Na cifra de deslocamento existem 26 chaves distintas, fácil de testar todas.
- Mas podemos fazer algo mais seguro substituindo cada carácter por outro qualquer, não necessariamente o que está a 3 posições no alfabeto.

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

- Agora existem 26! permutações (chaves) diferente, difícil de testar uma a uma.

- Agora existem 26! permutações (chaves) diferente, difícil de testar uma a uma.
- Entretanto ainda é bastante fácil descobrir um texto criptografado dessa maneira.

j wjzwugxqej gkiij fje j sgezqegj pgutxq
uauckq qz veqo xqixq j fetuh xq uwgeh tui
khaezui iqzutui u gkiieu ljtlqtagjk iku
jfqtieou sgetlesuhzqtaq tui hetrui xq fgqtaq
tj hqiaq q tj ikh qzwjgu zjiljk jluiejtuhzqtaq
uauckq jkagji hkpugqi tu luzsutru sugu
xqiagkeg u etfguqiagkakgu zeheaug xu klguteu q
whjckqug gqzqiiui xq ugzui jlexqtauei

```
j wjzwugxqej gkiij fje j sgezqegj pgutxq
uauckq qz veqo xqixq j fetuh xq uwgeh tui
khaezui iqzutui u gkiieu ljtlqtagjk iku
jfqtieou sgetlesuhzqtaq tui hetrui xq fgqtaq
tj hqiaq q tj ikh qzwjgu zjiljk jluiejtuhzqtaq
uauckq jkagji hkpugqi tu luzsutru sugu
xqiagkeg u etfguqiagkakgu zeheaug xu klguteu q
whjckqug gqzqiiui xq ugzui jlexqtauei
```

- Uma ideia é usar frequência de cada carácter, se soubermos que o texto está em português.

u	41
q	33
i	26
g	24
j	22
e	21
t	21

Em pt-br.

a	14.63%
e	12.57%
o	10.73%
s	7.81%
r	6.53%
i	6.18%
n	5.05%

- u deve ser A.

```
j wjzwAgxqej gkiij fje j sgezqegj pgAtxq
AaAckq qz veqo xqixq j fetAh xq Awgeh tAi
khaezAi iqzAtAi A gkiieA ljtlqtagjk ikA
jfqtieoA sgetlesAhzqtaq tAi hetrAi xq fgqtaq
tj hqiaq q tj ikh qzwjgA zjiljk jlAiejtAhzqtaq
AaAckq jkagji hkpAgqi tA lAzsAtrA sAgA
xqiagkeg A etfgAqiagkakgA zeheaAg xA klgAteA q
whjckqAg gqzqiiAi xq AgzAi jlexqtaAei
```

- Parece ok.

u	41
q	33
i	26
g	24
j	22
e	21
t	21

Em pt-br.

a	14.63%
e	12.57%
o	10.73%
s	7.81%
r	6.53%
i	6.18%
n	5.05%

- q deve ser E.

```
j wjzwAgxEej gkiij fje j sgezEegj pgAtxE
AaAckE Ez veEo xEixE j fetAh xE Awgeh tAi
khaezAi iEzAtAi A gkiieA ljtlEtagjk ikA
jfEtieoA sgetlesAhzEtaE tAi hetrAi xE fgEtaE
tj hEiaE E tj ikh EzwjgA zjiljk jlAiejtAhzEtaE
AaAckE jkagji hkpAgEi tA lAzsAtrA sAgA
xEiagkeg A etfgAEiagkakgA zeheaAg xA klgAteA E
whjckEAg gEzEiiAi xE AgzAi jlexEtaAei
```

- Parece ok.

u	41
q	33
i	26
g	24
j	22
e	21
t	21

Em pt-br.

a	14.63%
e	12.57%
o	10.73%
s	7.81%
r	6.53%
i	6.18%
n	5.05%

- i deve ser O.

```
j wjzwAgxEej gkOOj fje j sgezEegj pgAtxE
AaAckE Ez veEo xEOxE j fetAh xE Awgeh tAO
khaezAO OEzAtAO A gkOOeA ljtlEtagjk OkA
jfEtOeoA sgetlesAhzEtaE tAO hetrAO xE fgEtaE
tj hEOaE E tj Okh EzwjgA zjOljk jlAOejtAhzEtaE
AaAckE jkagjO hkpAgEO tA lAzsAtrA sAgA
xEOagkeg A etfgAEOagkakgA zeheaAg xA klgAteA E
whjckEAg gEzEOOAO xE AgzAO jlexEtaAeO
```

- Ficou estranho, note o OOAO. Pode ser S

u	41
q	33
i	26
g	24
j	22
e	21
t	21

Em pt-br.

a	14.63%
e	12.57%
o	10.73%
s	7.81%
r	6.53%
i	6.18%
n	5.05%

- (i)O deve ser S.

```
j wjzwAgxEej gkSSj fje j sgezEegj pgAtxE
AaAckE Ez veEo xESxE j fetAh xE Awgeh tAS
khaezAS SEzAtAS A gkSSeA ljtlEtagjk SkA
jfEtSeoA sgetlesAhzEtaE tAS hetrAS xE fgEtaE
tj hESaE E tj Skh EzwjgA zjSljk jlASejtAhzEtaE
AaAckE jkagjS hkpAgES tA lAzsAtrA sAgA
xESagkeg A etfgAESagkakgA zeheaAg xA klgAteA E
whjckEAg gEzESSAS xE AgzAS jlexEtaAeS
```

- Parece Ok.

u	41
q	33
i	26
g	24
j	22
e	21
t	21

Em pt-br.

a	14.63%
e	12.57%
o	10.73%
s	7.81%
r	6.53%
i	6.18%
n	5.05%

- g deve ser O.

```
j wjzwAOxEej OkSSj fje j sOezEeOj pOAtxE
AaAckE Ez veEo xESxE j fetAh xE AwOeh tAS
khaezAS SEzAtAS A OkSSeA ljtlEtaOjk SkA
jfEtSeoA sOetlesAhzEtaE tAS hetrAS xE fOEtaE
tj hESaE E tj Skh EzwjOA zjSljk jlASejtAhzEtaE
AaAckE jkaOjS hkpAOES tA lAzsAtrA sAOA
xESaOkeO A etfOAESaOkakOA zeheaAO xA klOAteA E
whjckEAO OEzESSAS xE AOzAS jlexEtaAeS
```

- Note a palavra OEzESSAS. Deve ser R

u	41
q	33
i	26
g	24
j	22
e	21
t	21

Em pt-br.

a	14.63%
e	12.57%
o	10.73%
s	7.81%
r	6.53%
i	6.18%
n	5.05%

- (g)O deve ser R.

```
j wjzwARxEej RkSSj fje j sRezEeRj pRAtxE
AaAckE Ez veEo xESxE j fetAh xE AwReh tAS
khaezAS SEzAtAS A RkSSeA ljtlEtaRjk SkA
jfEtSeoA sRetlesAhzEtaE tAS hetrAS xE fREtaE
tj hESaE E tj Skh EzwjRA zjSljk jlASejtAhzEtaE
AaAckE jkaRjS hkpARES tA lAzsAtrA sARA
xESaRkeR A etfRAESaRkakRA zeheaAR xA klRAteA E
whjckEAR REzESSAS xE ARzAS jlexEtaAeS
```

- Parece ok.

u	41
q	33
i	26
g	24
j	22
e	21
t	21
Em pt-br.	
a	14.63%
e	12.57%
o	10.73%
s	7.81%
r	6.53%
i	6.18%
n	5.05%

- j deve ser O.

```
O wOzwARxEeO RkSSO fOe O sRezEeRO pRAtxE
AaAckE Ez veEo xESxE O fetAh xE AwReh tAS
khaezAS SEzAtAS A RkSSeA lOtlEtaROk SkA
OfEtSeoA sRetlesAhzEtaE tAS hetrAS xE fREtaE
tO hESaE E tO Skh EzwORA zOSlOk OlASeOtAhzEtaE
AaAckE OkaROS hkpARES tA lAzsAtrA sARA
xESaRkeR A etfRAESaRkakRA zeheaAR xA klRAteA E
whOckEAR REzESSAS xE ARzAS OlexEtaAeS
```

- Parece ok.

u	41
q	33
i	26
g	24
j	22
e	21
t	21

Em pt-br.

a	14.63%
e	12.57%
o	10.73%
s	7.81%
r	6.53%
i	6.18%
n	5.05%

- e deve ser I.

O wOzwARxEIO RkSSO fOI O sRIzEIRO pRAtxE
AaAckE Ez vIEo xESxE O fItAh xE AwRIh tAS
khaIzAS SEzAtAS A RkSSIA lOtlEtaROk SkA
OfEtSIoA sRItlIsAhzEtaE tAS hItrAS xE fREtaE
tO hESaE E tO Skh EzwORA zOSlOk OlASIOtAhzEtaE
AaAckE OkaROS hkpARES tA lAzsAtrA sARA
xESaRkIR A ItfRAESaRkakRA zIhIaAR xA klRAtIA E
whOckEAR REzESSAS xE ARzAS OlIxEtaAIS

- Parece ok.

u	41
q	33
i	26
g	24
j	22
e	21
t	21

Em pt-br.

a	14.63%
e	12.57%
o	10.73%
s	7.81%
r	6.53%
i	6.18%
n	5.05%

- t deve ser N.

```
O wOzwARxEIO RkSSO fOI O sRIzEIRO pRANxE
AaAckE Ez vIEo xESxE O fINAh xE AwRIh NAS
khaIzAS SEzANAS A RkSSIA lONlENaROk SkA
OfENSIoA sRINlIsAhzENaE NAS hINrAS xE fRENaE
NO hESaE E NO Skh EzwORA zOSlOk OlASIONAhzENaE
AaAckE OkaROS hkpARES NA lAzsANrA sARA
xESaRkIR A INfRAESaRkakRA zIhIaAR xA klRANIA E
whOckEAR REzESSAS xE ARzAS OlIxENaAIS
```

- Parece ok.

u	41
q	33
i	26
g	24
j	22
e	21
t	21

Em pt-br.

a	14.63%
e	12.57%
o	10.73%
s	7.81%
r	6.53%
i	6.18%
n	5.05%

- O próximo seria k por D.

O wOzwARxEIO RDSSO fOI O sRIzEIRO pRANxE AaAcDE Ez vIEo xESxE O fINAh xE AwRIh NAS DhaIzAS SEzANAS A RDSSIA lONlENaROD SDA OfENSIoA sRINlIsAhzENaE NAS hINrAS xE fRENaE NO hESaE E NO SDh EzwORA zOSlOD OlASIONAhzENaE AaAcDE ODaROS hDpARES NA lAzsANrA sARA xESaRDIR A INfRAESaRDaDRA zIhIaAR xA DlRANIA E whOcDEAR REzESSAS xE ARzAS OlIxENaAIS

- O próximo seria k por D.

  O wOzwARxEIO RDSSO fOI O sRIzEIRO pRANxE AaAcDE Ez vIEo xESxE O fINAh xE AwRIh NAS DhaIzAS SEzANAS A RDSSIA lONlENaROD SDA OfENSIoA sRINlIsAhzENaE NAS hINrAS xE fRENaE NO hESaE E NO SDh EzwORA zOSlOD OlASIONAhzENaE AaAcDE ODaROS hDpARES NA lAzsANrA sARA xESaRDIR A INfRAESaRDaDRA zIhIaAR xA DlRANIA E whOcDEAR REzESSAS xE ARzAS OlIxENaAIS

- Ficou estranho, olhe o "RDSSO". Deve ser U.

- O próximo seria k por D.

```
O wOzwARxEIO RDSSO fOI O sRIzEIRO pRANxE AaAcDE Ez vIEo
xESxE O fINAh xE AwRIh NAS DhaIzAS SEzANAS A RDSSIA
lONlENaROD SDA OfENSIoA sRINlIsAhzENaE NAS hINrAS xE
fRENaE NO hESaE E NO SDh EzwORA zOSlOD OlASIONAhzENaE
AaAcDE ODaROS hDpARES NA lAzsANrA sARA xESaRDIR A
INfRAESaRDaDRA zIhIaAR xA DlRANIA E whOcDEAR REzESSAS xE
ARzAS OlIxENaAIS
```

- Ficou estranho, olhe o "RDSSO". Deve ser U.
- Daqui pra frente começa a falhar um pouco.

- (k)D por U.

O wOzwARxEIO RUSSO fOI O sRIzEIRO pRANxE AaAcUE Ez vIEo xESxE O fINAh xE AwRIh NAS UhaIzAS SEzANAS A RUSSIA lONlENaROU SUA OfENSIoA sRINlIsAhzENaE NAS hINrAS xE fRENaE NO hESaE E NO SUh EzwORA zOSlOU OlASIONAhzENaE AaAcUE OUaROS hUpARES NA lAzsANrA sARA xESaRUIR A INfRAESaRUaURA zIhIaAR xA UlRANIA E whOcUEAR REzESSAS xE ARzAS OlIxENaAIS

- (k)D por U.

  O wOzwARxEIO RUSSO fOI O sRIzEIRO pRANxE AaAcUE Ez vIEo xESxE O fINAh xE AwRIh NAS UhaIzAS SEzANAS A RUSSIA lONlENaROU SUA OfENSIoA sRINlIsAhzENaE NAS hINrAS xE fRENaE NO hESaE E NO SUh EzwORA zOSlOU OlASIONAhzENaE AaAcUE OUaROS hUpARES NA lAzsANrA sARA xESaRUIR A INfRAESaRUaURA zIhIaAR xA UlRANIA E whOcUEAR REzESSAS xE ARzAS OlIxENaAIS

- REzESSAS deve ser REMESSAS.

- (k)D por U.

  O wOzwARxEIO RUSSO fOI O sRIzEIRO pRANxE AaAcUE Ez vIEo xESxE O fINAh xE AwRIh NAS UhaIzAS SEzANAS A RUSSIA lONlENaROU SUA OfENSIoA sRINlIsAhzENaE NAS hINrAS xE fRENaE NO hESaE E NO SUh EzwORA zOSlOU OlASIONAhzENaE AaAcUE OUaROS hUpARES NA lAzsANrA sARA xESaRUIR A INfRAESaRUaURA zIhIaAR xA UlRANIA E whOcUEAR REzESSAS xE ARzAS OlIxENaAIS

- REzESSAS deve ser REMESSAS.
- Trocar z por M.

- z por M.

O wOMwARxEIO RUSSO fOI O sRIMEIRO pRANxE AaAcUE EM vIEo xESxE O fINAh xE AwRIh NAS UhaIMAS SEMANAS A RUSSIA lONlENaROU SUA OfENSIoA sRINlIsAhMENaE NAS hINrAS xE fRENaE NO hESaE E NO SUh EMwORA MOSlOU OlASIONAhMENaE AaAcUE OUaROS hUpARES NA lAMsANrA sARA xESaRUIR A INfRAESaRUaURA MIhIaAR xA UlRANIA E whOcUEAR REMESSAS xE ARMAS OlIxENaAIS

- z por M.

  O wOMwARxEIO RUSSO fOI O sRIMEIRO pRANxE AaAcUE EM vIEo xESxE O fINAh xE AwRIh NAS UhaIMAS SEMANAS A RUSSIA lONlENaROU SUA OfENSIoA sRINlIsAhMENaE NAS hINrAS xE fRENaE NO hESaE E NO SUh EMwORA MOSlOU OlASIONAhMENaE AaAcUE OUaROS hUpARES NA lAMsANrA sARA xESaRUIR A INfRAESaRUaURA MIhIaAR xA UlRANIA E whOcUEAR REMESSAS xE ARMAS OlIxENaAIS

- tem xE, xA..

- z por M.

  O wOMwARxEIO RUSSO fOI O sRIMEIRO pRANxE AaAcUE EM vIEo xESxE O fINAh xE AwRIh NAS UhaIMAS SEMANAS A RUSSIA lONlENaROU SUA OfENSIoA sRINlIsAhMENaE NAS hINrAS xE fRENaE NO hESaE E NO SUh EMwORA MOSlOU OlASIONAhMENaE AaAcUE OUaROS hUpARES NA lAMsANrA sARA xESaRUIR A INfRAESaRUaURA MIhIaAR xA UlRANIA E whOcUEAR REMESSAS xE ARMAS OlIxENaAIS

- tem xE, xA..
- x deve ser D

- x por D.

O wOMwARDEIO RUSSO fOI O sRIMEIRO pRANDE AaAcUE EM vIEo DESDE O fINAh DE AwRIh NAS UhaIMAS SEMANAS A RUSSIA lONlENaROU SUA OfENSIoA sRINlIsAhMENaE NAS hINrAS DE fRENaE NO hESaE E NO SUh EMwORA MOSlOU OlASIONAhMENaE AaAcUE OUaROS hUpARES NA lAMsANrA sARA DESaRUIR A INfRAESaRUaURA MIhIaAR DA UlRANIA E whOcUEAR REMESSAS DE ARMAS OlIDENaAIS

- x por D.

  O wOMwARDEIO RUSSO fOI O sRIMEIRO pRANDE AaAcUE EM vIEo DESDE O fINAh DE AwRIh NAS UhaIMAS SEMANAS A RUSSIA lONlENaROU SUA OfENSIoA sRINlIsAhMENaE NAS hINrAS DE fRENaE NO hESaE E NO SUh EMwORA MOSlOU OlASIONAhMENaE AaAcUE OUaROS hUpARES NA lAMsANrA sARA DESaRUIR A INfRAESaRUaURA MIhIaAR DA UlRANIA E whOcUEAR REMESSAS DE ARMAS OlIDENaAIS

- sRIMEIRO deve ser PRIMEIRO

- x por D.

  O wOMwARDEIO RUSSO fOI O sRIMEIRO pRANDE AaAcUE EM vIEo DESDE O fINAh DE AwRIh NAS UhaIMAS SEMANAS A RUSSIA lONlENaROU SUA OfENSIoA sRINlIsAhMENaE NAS hINrAS DE fRENaE NO hESaE E NO SUh EMwORA MOSlOU OlASIONAhMENaE AaAcUE OUaROS hUpARES NA lAMsANrA sARA DESaRUIR A INfRAESaRUaURA MIhIaAR DA UlRANIA E whOcUEAR REMESSAS DE ARMAS OlIDENaAIS

- sRIMEIRO deve ser PRIMEIRO
- s deve ser P

- s por P.

O wOMwARDEIO RUSSO fOI O PRIMEIRO pRANDE AaAcUE EM vIEo DESDE O fINAh DE AwRIh NAS UhaIMAS SEMANAS A RUSSIA lONlENaROU SUA OfENSIoA PRINlIPAhMENaE NAS hINrAS DE fRENaE NO hESaE E NO SUh EMwORA MOSlOU OlASIONAhMENaE AaAcUE OUaROS hUpARES NA lAMPANrA PARA DESaRUIR A INfRAESaRUaURA MIhIaAR DA UlRANIA E whOcUEAR REMESSAS DE ARMAS OlIDENaAIS

- s por P.

  O wOMwARDEIO RUSSO fOI O PRIMEIRO pRANDE AaAcUE EM vIEo DESDE O fINAh DE AwRIh NAS UhaIMAS SEMANAS A RUSSIA lONlENaROU SUA OfENSIoA PRINlIPAhMENaE NAS hINrAS DE fRENaE NO hESaE E NO SUh EMwORA MOSlOU OlASIONAhMENaE AaAcUE OUaROS hUpARES NA lAMPANrA PARA DESaRUIR A INfRAESaRUaURA MIhIaAR DA UlRANIA E whOcUEAR REMESSAS DE ARMAS OlIDENaAIS

- pRANDE deve ser GRANDE

- s por P.

  O wOMwARDEIO RUSSO fOI O PRIMEIRO pRANDE AaAcUE EM vIEo DESDE O fINAh DE AwRIh NAS UhaIMAS SEMANAS A RUSSIA lONlENaROU SUA OfENSIoA PRINlIPAhMENaE NAS hINrAS DE fRENaE NO hESaE E NO SUh EMwORA MOSlOU OlASIONAhMENaE AaAcUE OUaROS hUpARES NA lAMPANrA PARA DESaRUIR A INfRAESaRUaURA MIhIaAR DA UlRANIA E whOcUEAR REMESSAS DE ARMAS OlIDENaAIS

- pRANDE deve ser GRANDE
- p deve ser G

- p por G.

O wOMwARDEIO RUSSO fOI O PRIMEIRO GRANDE AaAcUE EM vIEo DESDE O fINAh DE AwRIh NAS UhaIMAS SEMANAS A RUSSIA lONlENaROU SUA OfENSIoA PRINlIPAhMENaE NAS hINrAS DE fRENaE NO hESaE E NO SUh EMwORA MOSlOU OlASIONAhMENaE AaAcUE OUaROS hUGARES NA lAMPANrA PARA DESaRUIR A INfRAESaRUaURA MIhIaAR DA UlRANIA E whOcUEAR REMESSAS DE ARMAS OlIDENaAIS

- p por G.

  O wOMwARDEIO RUSSO fOI O PRIMEIRO GRANDE AaAcUE EM vIEo DESDE O fINAh DE AwRIh NAS UhaIMAS SEMANAS A RUSSIA lONlENaROU SUA OfENSIoA PRINlIPAhMENaE NAS hINrAS DE fRENaE NO hESaE E NO SUh EMwORA MOSlOU OlASIONAhMENaE AaAcUE OUaROS hUGARES NA lAMPANrA PARA DESaRUIR A INfRAESaRUaURA MIhIaAR DA UlRANIA E whOcUEAR REMESSAS DE ARMAS OlIDENaAIS

- hUGARES deve ser LUGARES

- p por G.

  O wOMwARDEIO RUSSO fOI O PRIMEIRO GRANDE AaAcUE EM vIEo DESDE O fINAh DE AwRIh NAS UhaIMAS SEMANAS A RUSSIA lONlENaROU SUA OfENSIoA PRINlIPAhMENaE NAS hINrAS DE fRENaE NO hESaE E NO SUh EMwORA MOSlOU OlASIONAhMENaE AaAcUE OUaROS hUGARES NA lAMPANrA PARA DESaRUIR A INfRAESaRUaURA MIhIaAR DA UlRANIA E whOcUEAR REMESSAS DE ARMAS OlIDENaAIS

- hUGARES deve ser LUGARES
- h deve ser L

- h por L.

O wOMwARDEIO RUSSO fOI O PRIMEIRO GRANDE AaAcUE EM vIEo DESDE O fINAL DE AwRIL NAS ULaIMAS SEMANAS A RUSSIA lONlENaROU SUA OfENSIoA PRINlIPALMENaE NAS LINrAS DE fRENaE NO LESaE E NO SUL EMwORA MOSlOU OlASIONALMENaE AaAcUE OUaROS LUGARES NA lAMPANrA PARA DESaRUIR A INfRAESaRUaURA MILIaAR DA UlRANIA E wLOcUEAR REMESSAS DE ARMAS OlIDENaAIS

- h por L.

  O wOMwARDEIO RUSSO fOI O PRIMEIRO GRANDE AaAcUE EM vIEo DESDE O fINAL DE AwRIL NAS ULaIMAS SEMANAS A RUSSIA lONlENaROU SUA OfENSIoA PRINlIPALMENaE NAS LINrAS DE fRENaE NO LESaE E NO SUL EMwORA MOSlOU OlASIONALMENaE AaAcUE OUaROS LUGARES NA lAMPANrA PARA DESaRUIR A INfRAESaRUaURA MILIaAR DA UlRANIA E wLOcUEAR REMESSAS DE ARMAS OlIDENaAIS

- INfRAESaRUaURA deve ser INFRAESTRUTURA

- h por L.

  O wOMwARDEIO RUSSO fOI O PRIMEIRO GRANDE AaAcUE EM vIEo DESDE O fINAL DE AwRIL NAS ULaIMAS SEMANAS A RUSSIA lONlENaROU SUA OfENSIoA PRINlIPALMENaE NAS LINrAS DE fRENaE NO LESaE E NO SUL EMwORA MOSlOU OlASIONALMENaE AaAcUE OUaROS LUGARES NA lAMPANrA PARA DESaRUIR A INfRAESaRUaURA MILIaAR DA UlRANIA E wLOcUEAR REMESSAS DE ARMAS OlIDENaAIS

- INfRAESaRUaURA deve ser INFRAESTRUTURA
- f deve ser F mesmo, e a deve ser T

- f por F, a por T

O wOMwARDEIO RUSSO fOI O PRIMEIRO GRANDE ATAcUE EM vIEo DESDE O fINAL DE AwRIL NAS ULTIMAS SEMANAS A RUSSIA lONlENTROU SUA OfENSIoA PRINlIPALMENTE NAS LINrAS DE fRENTE NO LESTE E NO SUL EMwORA MOSlOU OlASIONALMENTE ATAcUE OUTROS LUGARES NA lAMPANrA PARA DESTRUIR A INfRAESTRUTURA MILITAR DA UlRANIA E wLOcUEAR REMESSAS DE ARMAS OlIDENTAIS

- f por F, a por T

  O wOMwARDEIO RUSSO fOI O PRIMEIRO GRANDE ATAcUE EM vIEo DESDE O fINAL DE AwRIL NAS ULTIMAS SEMANAS A RUSSIA lONlENTROU SUA OfENSIoA PRINlIPALMENTE NAS LINrAS DE fRENTE NO LESTE E NO SUL EMwORA MOSlOU OlASIONALMENTE ATAcUE OUTROS LUGARES NA lAMPANrA PARA DESTRUIR A INfRAESTRUTURA MILITAR DA UlRANIA E wLOcUEAR REMESSAS DE ARMAS OlIDENTAIS

- OIIDENTAIS deve ser OCIDENTAIS

- f por F, a por T

  O wOMwARDEIO RUSSO fOI O PRIMEIRO GRANDE ATAcUE EM vIEo DESDE O fINAL DE AwRIL NAS ULTIMAS SEMANAS A RUSSIA lONlENTROU SUA OfENSIoA PRINlIPALMENTE NAS LINrAS DE fRENTE NO LESTE E NO SUL EMwORA MOSlOU OlASIONALMENTE ATAcUE OUTROS LUGARES NA lAMPANrA PARA DESTRUIR A INfRAESTRUTURA MILITAR DA UlRANIA E wLOcUEAR REMESSAS DE ARMAS OlIDENTAIS

- OIIDENTAIS deve ser OCIDENTAIS
- I deve ser C. E assim por diante.

- terminando

O BOMBARDEIO RUSSO FOI O PRIMEIRO GRANDE ATAQUE EM KIEV DESDE O FINAL DE ABRIL NAS ULTIMAS SEMANAS A RUSSIA CONCENTROU SUA OFENSIVA PRINCIPALMENTE NAS LINHAS DE FRENTE NO LESTE E NO SUL EMBORA MOSCOU OCASIONALMENTE ATAQUE OUTROS LUGARES NA CAMPANHA PARA DESTRUIR A INFRAESTRUTURA MILITAR DA UCRANIA E BLOQUEAR REMESSAS DE ARMAS OCIDENTAIS

- terminando

  O BOMBARDEIO RUSSO FOI O PRIMEIRO GRANDE ATAQUE EM KIEV DESDE O FINAL DE ABRIL NAS ULTIMAS SEMANAS A RUSSIA CONCENTROU SUA OFENSIVA PRINCIPALMENTE NAS LINHAS DE FRENTE NO LESTE E NO SUL EMBORA MOSCOU OCASIONALMENTE ATAQUE OUTROS LUGARES NA CAMPANHA PARA DESTRUIR A INFRAESTRUTURA MILITAR DA UCRANIA E BLOQUEAR REMESSAS DE ARMAS OCIDENTAIS

- Note que não é preciso muito esforço.

- terminando

  O BOMBARDEIO RUSSO FOI O PRIMEIRO GRANDE ATAQUE EM KIEV DESDE O FINAL DE ABRIL NAS ULTIMAS SEMANAS A RUSSIA CONCENTROU SUA OFENSIVA PRINCIPALMENTE NAS LINHAS DE FRENTE NO LESTE E NO SUL EMBORA MOSCOU OCASIONALMENTE ATAQUE OUTROS LUGARES NA CAMPANHA PARA DESTRUIR A INFRAESTRUTURA MILITAR DA UCRANIA E BLOQUEAR REMESSAS DE ARMAS OCIDENTAIS

- Note que não é preciso muito esforço.
- Mesmo tendo $26!$ chaves.

- Além disso, suponha que você vai encriptar o número do cartão de crédito trocando os dígitos de 0 a 9.

- Além disso, suponha que você vai encriptar o número do cartão de crédito trocando os dígitos de 0 a 9.
- Nesse caso seriam apenas 10! chaves possíveis, ou 3.628.800.

- Além disso, suponha que você vai encriptar o número do cartão de crédito trocando os dígitos de 0 a 9.
- Nesse caso seriam apenas 10! chaves possíveis, ou 3.628.800.
- Que é possível simplesmente testar todas as combinações. Em particular se Maurício tiver roubado o número encriptado de vários cartões.

Cifras de Chave Única

Cifras de Chave Única

- Uma criptografia mais robusta que a cifra de substituição simples. Envolve a utilização de uma chave maior, e da operação $\oplus$ (XOR, ou exclusivo).

$$0 \oplus 0 = 0 \tag{1}$$
$$0 \oplus 1 = 1 \tag{2}$$
$$1 \oplus 0 = 1 \tag{3}$$
$$1 \oplus 1 = 0 \tag{4}$$

- A cifra de chave única se baseia no fato de que se ao bit x é aplicado um XOR com um bit y duas vezes, ele volta a ser x, ou seja,

$$(x \oplus y) \oplus y = x$$

- A cifra de chave única se baseia no fato de que se ao bit x é aplicado um XOR com um bit y duas vezes, ele volta a ser x, ou seja,

$$(x \oplus y) \oplus y = x$$

- Você pode entender o XOR como: se y for 0 o resultado é o x, se y for 1 o resultado é o inverso de x.

- Toda informação digital pode ser convertida em bits. Utilizando o padrão ASCII por exemplo:

b o m b

- Toda informação digital pode ser convertida em bits. Utilizando o padrão ASCII por exemplo:

b	o	m	b
98	111	109	98

- Toda informação digital pode ser convertida em bits. Utilizando o padrão ASCII por exemplo:

	b	o	m	b
	98	111	109	98
M	0110 0010	0110 1111	0110 1101	0110 0010

- Toda informação digital pode ser convertida em bits. Utilizando o padrão ASCII por exemplo:

	b	o	m	b
	98	111	109	98
M	0110 0010	0110 1111	0110 1101	0110 0010
	$\oplus$	$\oplus$	$\oplus$	$\oplus$
chave	0011 0101	0010 0000	1101 1111	0110 1011

- Toda informação digital pode ser convertida em bits. Utilizando o padrão ASCII por exemplo:

	b	o	m	b
	98	111	109	98
M	0110 0010	0110 1111	0110 1101	0110 0010
	$\oplus$	$\oplus$	$\oplus$	$\oplus$
chave	0011 0101	0010 0000	1101 1111	0110 1011
C	0101 0111	0100 1111	1011 0010	0000 1001

b o m b

b	o	m	b
98	111	109	98

	b	o	m	b
	98	111	109	98
M	0110 0010	0110 1111	0110 1101	0110 0010

	b	o	m	b
	98	111	109	98
M	0110 0010	0110 1111	0110 1101	0110 0010
	$\oplus$	$\oplus$	$\oplus$	$\oplus$
chave	0011 0101	0010 0000	1101 1111	0110 1011

	b	o	m	b
	98	111	109	98
M	0110 0010	0110 1111	0110 1101	0110 0010
	$\oplus$	$\oplus$	$\oplus$	$\oplus$
chave	0011 0101	0010 0000	1101 1111	0110 1011
C	0101 0111	0100 1111	1011 0010	0000 1001

	b	o	m	b
	98	111	109	98
M	0110 0010	0110 1111	0110 1101	0110 0010
	$\oplus$	$\oplus$	$\oplus$	$\oplus$
chave	0011 0101	0010 0000	1101 1111	0110 1011
C	0101 0111	0100 1111	1011 0010	0000 1001
	$\oplus$	$\oplus$	$\oplus$	$\oplus$
chave	0011 0101	0010 0000	1101 1111	0110 1011

	b	o	m	b
	98	111	109	98
M	0110 0010	0110 1111	0110 1101	0110 0010
	$\oplus$	$\oplus$	$\oplus$	$\oplus$
chave	0011 0101	0010 0000	1101 1111	0110 1011
C	0101 0111	0100 1111	1011 0010	0000 1001
	$\oplus$	$\oplus$	$\oplus$	$\oplus$
chave	0011 0101	0010 0000	1101 1111	0110 1011
M	0110 0010	0110 1111	0110 1101	0110 0010

	b	o	m	b
	98	111	109	98
M	0110 0010	0110 1111	0110 1101	0110 0010
	$\oplus$	$\oplus$	$\oplus$	$\oplus$
chave	0011 0101	0010 0000	1101 1111	0110 1011
C	0101 0111	0100 1111	1011 0010	0000 1001
	$\oplus$	$\oplus$	$\oplus$	$\oplus$
chave	0011 0101	0010 0000	1101 1111	0110 1011
M	0110 0010	0110 1111	0110 1101	0110 0010
	b	o	m	b

- Se todos os bits da chave forem gerados aleatoriamente.

- Se todos os bits da chave forem gerados aleatoriamente.
- Cada bit de C tem 50% de chance de ser igual ao bit original e 50% de ser o inverso.
- Ou seja, o bit de C não te dará nenhuma informação sobre M, ou sobre a chave.

- Se todos os bits da chave forem gerados aleatoriamente.
- Cada bit de C tem 50% de chance de ser igual ao bit original e 50% de ser o inverso.
- Ou seja, o bit de C não te dará nenhuma informação sobre M, ou sobre a chave.
- Portanto podemos considerar que é uma criptografia robusta nesse sentido, entretanto...

Desvantagens da cifra de chave única.

Desvantagens da cifra de chave única.

- Se M exige b bits, então a chave precisa ter b bits.

Desvantagens da cifra de chave única.

- Se M exige b bits, então a chave precisa ter b bits.
- Você só pode usar a chave uma única vez:
  - Suponha que Maurício obtenha 2 textos cifrados C_1 e C_2.

Desvantagens da cifra de chave única.

- Se M exige b bits, então a chave precisa ter b bits.
- Você só pode usar a chave uma única vez:
  - Suponha que Maurício obtenha 2 textos cifrados C_1 e C_2.
  - Apesar de não ter a chave Maurício faz

$$C_1 \oplus C_2 \tag{5}$$

$$(M_1 \oplus chave) \oplus (M_2 \oplus chave) \tag{6}$$

$$M_1 \oplus M_2 \tag{7}$$

Desvantagens da cifra de chave única.

- Se M exige b bits, então a chave precisa ter b bits.
- Você só pode usar a chave uma única vez:
  - Suponha que Maurício obtenha 2 textos cifrados C_1 e C_2.
  - Apesar de não ter a chave Maurício faz

$$C_1 \oplus C_2 \tag{5}$$
$$(M_1 \oplus chave) \oplus (M_2 \oplus chave) \tag{6}$$
$$M_1 \oplus M_2 \tag{7}$$

  - Ou seja, Maurício obtém a informação dos bits em que as mensagens originais era iguais (inclusive se ela for toda igual)

Cifra de bloco e encadeamento

Cifra de bloco e encadeamento

- Quanto a mensagem a ser passada é muito grande, precisar de uma chave igualmente grande pode ser ruim.

Cifra de bloco e encadeamento

- Quanto a mensagem a ser passada é muito grande, precisar de uma chave igualmente grande pode ser ruim.
- Podemos usar uma chave mais curta e desmembrar o M em vários blocos, aplicando a chave em cada bloco.

- Digamos que temos uma função $E()$ que usa uma certa *chave* e consegue encriptar um bloco de tamanho b.

- Digamos que temos uma função $E()$ que usa uma certa *chave* e consegue encriptar um bloco de tamanho b.
- Quebramos nosso texto comum M em blocos $t_1, t_2, \ldots, t_l$, cada um com tamanho b.

- Digamos que temos uma função $E()$ que usa uma certa *chave* e consegue encriptar um bloco de tamanho b.
- Quebramos nosso texto comum M em blocos $t_1, t_2, \ldots, t_l$, cada um com tamanho b.
- Poderíamos agora encriptar cada bloco com $E()$, porém isso ainda daria informação à Maurício sobre quais blocos de M são iguais.

- Digamos que temos uma função $E()$ que usa uma certa *chave* e consegue encriptar um bloco de tamanho b.
- Quebramos nosso texto comum M em blocos $t_1, t_2, \ldots, t_l$, cada um com tamanho b.
- Poderíamos agora encriptar cada bloco com $E()$, porém isso ainda daria informação à Maurício sobre quais blocos de M são iguais.
- Então aplicamos a técnica de encadeamento.

$$c_1 = E(t_1) \tag{8}$$
$$c_2 = E(t_2 \oplus c_1) \tag{9}$$
$$c_3 = E(t_3 \oplus c_2) \tag{10}$$
$$\dots \tag{11}$$
$$c_l = E(t_l \oplus c_{l-1}) \tag{12}$$

$$c_1 = E(t_1) \tag{8}$$
$$c_2 = E(t_2 \oplus c_1) \tag{9}$$
$$c_3 = E(t_3 \oplus c_2) \tag{10}$$
$$\ldots \tag{11}$$
$$c_l = E(t_l \oplus c_{l-1}) \tag{12}$$

Maurício agora não consegue ver quais blocos são iguais, entretanto se a mensagem for toda igual, a sequencia de blocos também será. Vamos consertar isso com um **vetor de inicialização** c_0 gerado aleatoriamente.

$$c_0 = random(); \tag{13}$$
$$c_1 = E(t_1 \oplus c_0) \tag{14}$$
$$c_2 = E(t_2 \oplus c_1) \tag{15}$$
$$c_3 = E(t_3 \oplus c_2) \tag{16}$$
$$\ldots \tag{17}$$
$$c_l = E(t_l \oplus c_{l-1}) \tag{18}$$

- Bob por sua vez, tem a função D e *chave* capaz de decifrar um bloco de tamanho b e recebe os blocos $c_0, c_1, c_2, \ldots, c_l$.

$$t_1 = D(c_1) \oplus c_0 = (t_1 \oplus c_0) \oplus c_0 \tag{19}$$

- Bob por sua vez, tem a função D e *chave* capaz de decifrar um bloco de tamanho b e recebe os blocos $c_0, c_1, c_2, \ldots, c_l$.

$$t_1 = D(c_1) \oplus c_0 = (t_1 \oplus c_0) \oplus c_0 \tag{19}$$
$$t_2 = D(c_2) \oplus c_1 \tag{20}$$
$$t_3 = D(c_2) \oplus c_2 \tag{21}$$
$$\ldots \tag{22}$$
$$t_l = D(c_l) \oplus c_{l-1} \tag{23}$$

- Um exemplo desse sistema é o AES (*Advanced Encryption Standard*) que faz algo mais elaborado que um XOR, e usa chaves de 128, 192 ou 256 bits para encriptar blocos de 128 bits.

- Um exemplo desse sistema é o AES (*Advanced Encryption Standard*) que faz algo mais elaborado que um XOR, e usa chaves de 128, 192 ou 256 bits para encriptar blocos de 128 bits.
- Apesar de eficiente esses sistemas tem um grande desafio. Ambas as partes precisam concordar com a *chave* a priori.

- Um exemplo desse sistema é o AES (*Advanced Encryption Standard*) que faz algo mais elaborado que um XOR, e usa chaves de 128, 192 ou 256 bits para encriptar blocos de 128 bits.
- Apesar de eficiente esses sistemas tem um grande desafio. Ambas as partes precisam concordar com a *chave* a priori.
- Seria ineficiente, que todo site que frequentamos/compramos exigisse que fossemos num lugar físico pegar a chave em um pendrive.