Algoritmos

Pedro Hokama

Fontes

- [*clrs*] Algoritmos: Teoria e Prática (Terceira Edição) Thomas H. Cormen, Charles Eric Leiserson, Ronald Rivest e Clifford Stein.
- [*timr*] Algorithms Illuminated Series, Tim Roughgarden
- Desmistificando Algoritmos, Thomas H. Cormen.

Apresentação Baseada:

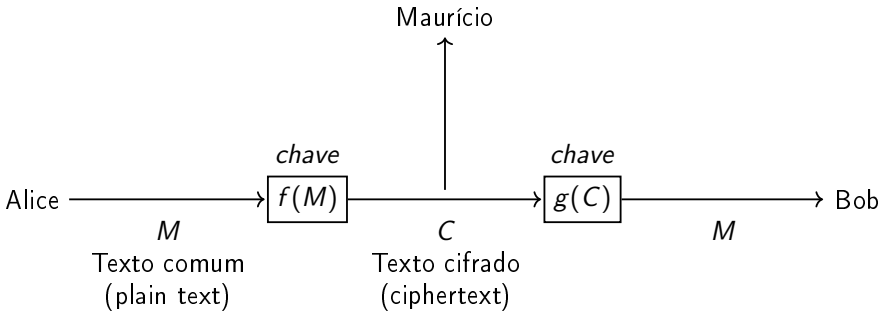
- Stanford Algorithms
  `https://www.youtube.com/playlist?list=PLXFMmlk03Dt7Q0xr1PIAriY5623cKiH7V`
  `https://www.youtube.com/playlist?list=PLXFMmlk03Dt5EMI2s2WQBsLsZl7A5HEK6`
- Conjunto de Slides dos Professores Cid C. de Souza, Cândida N. da Silva, Orlando Lee, Pedro J. de Rezende
- Conjunto de Slides do Professores Cid C. de Souza para a disciplina MO420

Qualquer erro é de minha responsabilidade.

Fundamentos de Criptografia

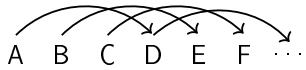
- Quando fazemos compras pela internet, temos que enviar o número do cartão de crédito para efetivar a compra.
- A internet é uma rede pública, e qualquer um pode acessar os pacotes de dados que são transmitidos através dela.
- É mais seguro se você disfarçar os dados do seu cartão de alguma maneira.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

- Apesar de ser uma dor de cabeça o roubo do número do cartão de crédito não é a pior coisa que pode ser roubada.
- Informações enviadas de/para forças armadas, diplomáticas, nudes, etc etc...
- Portanto além de precisarmos de formas de criptografar e decifrar informações, esse métodos precisam ser dificílimos de derrotar.



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.

xlyol yfopd

3: uivli vclma
4: thukh ubklz
5: sgtjg tajky
6: rfsif szijx
7: qerhe ryhiw
8: pdqgd qxghv
9: ocpfc pwfgu
10: nboeb oveft
11: manda nudes
11: manda nudes
12: lzmcz mtcdr
13: kylby lsbcq
14: jxkax krabp
15: iwjzw jqzao
16: hviyv ipyzn
17: guhxu hoxym
18: ftgwt gnwxl
19: esfvs fmvwk
20: dreur eluvj
21: cqdtq dktui
22: bpcsp cjsth
23: aobro birsg
24: znaqn ahqrf
25: ymzpm zgpqe
1: wkxnk xenoc
2: vjwmj wdmnb

manda nudes

Cifra de substituição simples

- Na cifra de deslocamento existem 25 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	v	w	x	y	z
u	w	l	x	q	f	p	r	e	n	v	h	z	t	j	s	c	g	i	a	k	o	d	m	y	b

- 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
```

- 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
```

- 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
```

- 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
```

- 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
```

- 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
```

- 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

- 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

- 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

- 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

- 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.
- 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

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

$$0 \oplus 0 = 0 \quad (1)$$
$$0 \oplus 1 = 1 \quad (2)$$
$$1 \oplus 0 = 1 \quad (3)$$
$$1 \oplus 1 = 0 \quad (4)$$

- 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,

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

- 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:

	n	u	d	e
	110	117	100	101
M	01101110	01110101	01100100	01100101
	$\oplus$	$\oplus$	$\oplus$	$\oplus$
chave	00110101	00100000	11011111	01101011
C	01011011	01010101	10111011	00001110

	n	u	d	e
	110	117	100	101
M	01101110	01110101	01100100	01100101
	$\oplus$	$\oplus$	$\oplus$	$\oplus$
chave	00110101	00100000	11011111	01101011
C	01011011	01010101	10111011	00001110
	$\oplus$	$\oplus$	$\oplus$	$\oplus$
chave	00110101	00100000	11011111	01101011
M	01101110	01110101	01100100	01100101
	n	u	d	e

- 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.

- 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

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

  - 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

- 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.
- 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.

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

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.

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

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

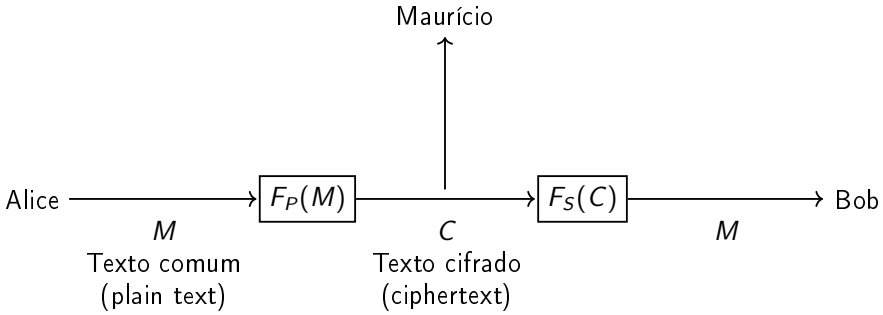
$$t_1 = D(c_1) \oplus c_0 = (t_1 \oplus c_0) \oplus c_0 \quad (19)$$
$$t_2 = D(c_2) \oplus c_1 \quad (20)$$
$$t_3 = D(c_2) \oplus c_2 \quad (21)$$
$$\ldots \quad (22)$$
$$t_l = D(c_l) \oplus c_{l-1} \quad (23)$$

- 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.
- 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.

Criptografia de Chave Pública

- Para Alice e Bob se comuniquem eles precisam conhecer a chave que cifra e decifra o texto, certo? Errado.
- Na **Criptografia de Chave Pública** cada participante tem duas chaves.
- Uma **chave pública** que todo mundo sabe.
- Uma **chave secreta** que que só ele conhece.

- Bob tem a chave pública P que todos conhecem, inclusive Maurício.
- E tem uma chave secreta S.



- As chaves têm a seguinte relação:

$$M = F_S(F_P(M))$$

- Para que isso funcione dois textos comuns diferentes M_1 e M_2 não podem ter o mesmo resultado C quando aplicado em F_P.
- Nesse caso $F_S(C)$ não saberia se o texto original é M_1 ou M_2,

- Por outro lado é permitido (e até recomendável) que um mesmo texto M tenha mais de uma representação cifrada.
- Esse tipo de sistema funciona melhor se a chave for maior que o bloco a ser cifrado (que a Imagem seja maior que o Domínio).
- Em particular podemos colocar algum recheio aleatório na informação a ser cifrada, desde que $F_S()$ esteja preparada para lidar com isso.

Criptossistema RSA

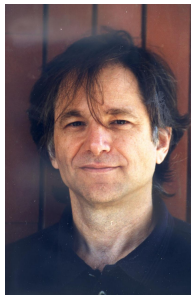
O sistema de criptografia RSA se baseia na diferença entre

- a facilidade de encontrar números primos grandes
- e a dificuldade de fatorar o produto de números primos grandes.

Criptossistema RSA

Ron Rivest

Adi Shamir



Leonard Adleman

O RSA depende de algumas facetas da Teoria dos Números, uma delas é a **aritmética modular**.

- Na aritmética modular escolhemos um inteiro positivo n e sempre que chegamos a n imediatamente voltamos a 0.
- É como aritmética em um relógio, sempre que chega a 12, voltamos para 0. Se você vai dormir as 11 e dorme 8 horas, você acorda as 7.

- É como aritmética com inteiros, mas sempre dividimos por n e tomamos o resto. Por exemplo, em uma aritmética módulo 5 os únicos valores possíveis são 0, 1, 2, 3 e 4.
- Em módulo 5:

$$3 + 4 \equiv 2$$

- Pois 7 dividido por 5 tem resto 2. Definimos um operador **mod** para essa operação. de forma que $7 \bmod 5 = 2$

O operador **mod** tem algumas propriedade interessantes:

- $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$,
- $ab \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$,
- $a^b \bmod n = (a \bmod n)^b \bmod n$.

- Na matemática o **inverso multiplicativo** de um número x é um número y tal que $x \cdot y = 1$.
- Na aritmética modular temos uma definição parecida. O **inverso multiplicativo** de um número x em **modulo** n é um inteiro y tal que

$$x \cdot y \bmod n \equiv 1 \bmod n$$

- Por exemplo o inverso multiplicativo em módulo 5 de 3 é 2 pois

$$3 \cdot 2 \bmod 5 = 6 \bmod 5 \equiv 1 \bmod 5$$

- Note que se x e n tem fatores em comum por exemplo $x = 2$ e $n = 6$ não existe inverso multiplicativo.

$$2 * 1 \bmod 6 = 2 \bmod 6$$
$$2 * 2 \bmod 6 = 4 \bmod 6$$
$$2 * 3 \bmod 6 = 6 \bmod 6 \equiv 0 \bmod 6$$
$$2 * 4 \bmod 6 = 8 \bmod 6 \equiv 2 \bmod 6$$
$$2 * 5 \bmod 6 = 10 \bmod 6 \equiv 4 \bmod 6$$

- Mas se x e n são primos relativos o inverso multiplicativo existe.

No **sistema de criptografia de chave pública RSA** um participante cria suas chaves públicas e secreta com o seguinte procedimento:

1. Seleciona aleatoriamente dois números primos grandes (de pelo menos 1024 bits) distintos p e q.
2. Calcule $n = pq$ (Esse número tem pelo menos 2048 bits ou 618 dígitos decimais.)
3. Calcule $r = (p-1)(q-1)$ que é quase tão grande quando n

4. Seleciona um inteiro ímpar pequeno e tal que e seja **relativamente primo** de r, ou seja, o único divisor comum é 1. Qualquer inteiro pequeno serve.
5. Calcule d como o *inverso multiplicativo* de e, módulo r. Isto é $ed \bmod r$ deve ser igual a 1.
6. Divulgue o par $P = (e, n)$ como a chave pública.
7. Mantenha $S = (d, n)$ em segredo como a chave secreta.

- Para criptografar uma mensagem M fazemos

$$F_P(M) = M^e (\mathtt{mod}\ n)$$

- Para transformar um texto cifrado C:

$$F_S(C) = C^d (\mathtt{mod}\ n)$$

Exemplo

- Bob sorteia $p = 17$ e $q = 29$ (Na prática sorteia números de no mínimo 1024 bits)
- Calcula $n = pq = 493$
- Calcula $r = (p-1)(q-1) = 448$
- Seleciona $e = 5$ que é um primo relativo de 448
- Calcula $d = 269$, já que $5 \cdot 269 \bmod r = 1345 \bmod r = 1$
- Publica a chave $P = (5, 493)$
- Guarda com carinho a chave $S = (269, 493)$

Chaves de Bob $P = (5, 493)$ e $S = (269, 493)$

- Alice quer enviar a mensagem 327

$$F_P(327) = 327^5 \bmod 493 \quad (24)$$
$$= 3.738.856.210.407 \bmod 493 \quad (25)$$
$$= 259 \quad (26)$$

- Na verdade Alice não precisa lidar com números astronômicos. (iclusive muito maiores que esse)

$$327^5 \bmod 493 \quad (27)$$
$$327^2 \cdot 327^3 \bmod 493 \quad (28)$$
$$(327^2 \bmod 493 \cdot 327^3 \bmod 493) \bmod 493 \quad (29)$$
$$(106929 \bmod 493 \cdot 327^3 \bmod 493) \bmod 493 \quad (30)$$
$$(441 \cdot 327^3 \bmod 493) \bmod 493 \quad (31)$$
$$(441 \cdot 441 \cdot 327 \bmod 493) \bmod 493 \quad (32)$$
$$78153 \bmod 493 = 259 \quad (33)$$

Chaves de Bob $P = (5, 493)$ e $S = (269, 493)$

- Bob então recebe a mensagem criptografada $C = 259$. E decifra ela:

$$F_S(259) = 259^{269} \bmod 493 = 327$$

- Que de fato é a mensagem original de Alice!

Corretude do RSA

Mostrando que F_P e F_S são inversas uma da outra

- Para criptografar um texto M fazemos: $F_P(M) = M^e (\mathrm{mod}\, n)$
- Para transformar um cifrado C: $F_S(C) = C^d (\mathrm{mod}\, n)$

O sistema RSA de fato é capaz de encriptar e decodificar mensagens

$$F_S(F_P(M)) = F_S(M^e (\mathrm{mod}\, n))$$
$$= (M^e (\mathrm{mod}\, n))^d (\mathrm{mod}\, n)$$
$$= M^{ed} (\mathrm{mod}\, n)$$

- Queremos mostrar então que

$$M^{ed}(\mathrm{mod}\, n) = M \bmod n$$

e como $M < n$ então

$$M \bmod n = M$$

- Começaremos mostrando que

$$M^{ed}(\mathrm{mod}\, p) = M(\mathrm{mod}\, p)$$

- Lembrando que $r = (p-1)(q-1)$,
- e que e é um primo relativo de r,
- e que d é um inverso multiplicativo de e em aritmética módulo r, o que equivale a dizer que existe um inteiro h tal que:

$$ed = 1 + h(p-1)(q-1)$$

- Seja $\mathbb{Z}_p = \{0, 1, \ldots, n-1\}$
- Seja $\mathbb{Z}_p^*$ o conjunto dos elementos de $\mathbb{Z}_p$ que são primos relativos de p. Ou seja, se $a \in \mathbb{Z}_p^*$ então $mdc(p, a) = 1$.

Pequeno teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}_p^*$, então

$$a^{p-1} \equiv 1(\mathrm{mod}\, p)$$

Prova:

Considere a sequência $L = (a, 2a, 3a, \ldots, (p-1)a)$ de $(p-1)$ múltiplos de a.

- Nenhum é múltiplo de p já que a e p são primos relativos. E para todo $ka \in L$, $k \leq (p-1)$.
- Em L não tem 2 elementos congruentes em módulo p.

- Suponha por absurdo que exitem $k_1, k_2 \in \{1, 2, \ldots, p-1\}$ com $k_1 \neq k_2$ tal que

$$ak_1 \bmod p \equiv ak_2 \bmod p \quad (34)$$

Seja a' o inverso multiplicativo de a.

$$a'ak_1 \bmod p \equiv a'ak_2 \bmod p \quad (35)$$
$$k_1 \bmod p \equiv k_2 \bmod p \quad (36)$$

Como k_1 e k_2 são menores que p

$$k_1 = k_2 (ABSURDO) \quad (37)$$

Prova:

Considere a sequência $L = (a, 2a, 3a, \ldots, (p-1)a)$ de $(p-1)$ múltiplos de a.

- Nenhum é múltiplo de p já que a e p são primos relativos. E para todo $ka \in L$, $k \leq (p-1)$.
- Em L não tem 2 elementos congruentes em módulo p.
- Cada $l \in L$ então é congruente a $\{1, 2, \ldots, p-1\}$

$$a \cdot 2a \ldots (p-1)a \equiv 1 \cdot 2 \ldots (p-1) (\mathrm{mod} p) \quad (38)$$
$$a^{p-1}.(p-1)! \equiv (p-1)! (\mathrm{mod} p) \quad (39)$$
$$a^{p-1} \equiv 1 (\mathrm{mod} p) \quad (40)$$

$$\begin{aligned}
&M^{ed} (\mathrm{mod} p) \\
&= (M \bmod p)^{ed} \bmod p \\
&= (M \bmod p)^{1+h(p-1)(q-1)} \bmod p \\
&= (M \bmod p) \cdot (M \bmod p)^{h(p-1)(q-1)} \bmod p \\
&= (M \bmod p) \cdot ((M \bmod p)^{(p-1)})^{h(q-1)} \bmod p \\
&= (M \bmod p) \cdot ((M \bmod p)^{(p-1)} \bmod p)^{h(q-1)} \bmod p \\
&= (M \bmod p) \cdot (1)^{h(q-1)} \bmod p \\
&= (M \bmod p)
\end{aligned}$$

- Analogamente $M^{ed} (\mathrm{mod} q) = (M \bmod q)$.
- Além disso se

$$x \bmod p = y \bmod p$$

e

$$x \bmod q = y \bmod q$$

então

$$x \bmod pq = y \bmod pq$$

- Como $M^{ed} (\mathrm{mod} p) = M \bmod p$,
- e $M^{ed} \bmod q = M \bmod q$
- então

$$M^{ed} (\mathrm{mod} pq) = M \bmod pq$$

- Como $pq = n$
- então

$$M^{ed} (\mathrm{mod} n) = M \bmod n$$

- e portanto a chave secreta de Bob decifra C

- Além disso, talvez você tenha reparado que se Bob cifrar um texto comum com a sua chave secreta $S = (d, n)$:

$$F_S(M) = M^d (\mathrm{mod} n)$$

- Alice pode decifra-la com a chave pública.

$$F_P(M^d (\mathrm{mod} n)) = M^{de} (\mathrm{mod} n) = M^{ed} (\mathrm{mod} n) = M$$

- Isso não tem muita utilidade se o objetivo era esconder M já que todo mundo conhece P.

- Entretanto serve para Bob provar que foi ele quem escreveu M. Já que ninguém mais conseguiria cifrar M dessa forma.
- Se Bob então enviar M e $F_S(M)$, Alice e quem mais quiser terá certeza que foi Bob que enviou a mensagem.
- Além disso se Bob enviar M e $F_S(M)$, Alice terá certeza que a mensagem M não foi corrompida por exemplo.

- Note que Alice pode gerar as suas próprias chaves e Bob também poderá enviar mensagens cifradas que só ela poderá ler.
- Além disso se toda a codificação e decodificação usando aritmética modular for pesado para a quantidade de informações que Alice e Bob querem trocar. Eles podem usar o RSA para trocar chaves simétricas que sejam mais rápidas de calcular.