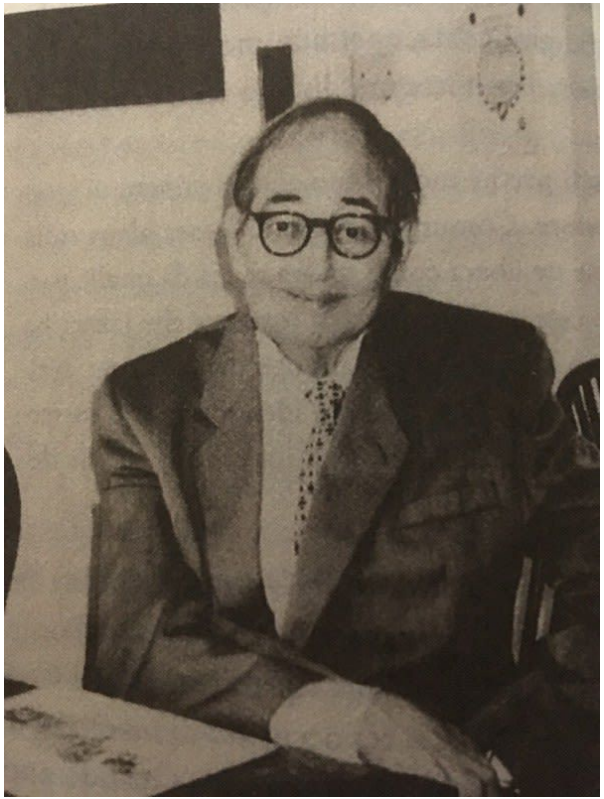
RSA
Rivest Shamir Adleman

Algoritmo de criptografia

Martim Vieira nº47268
Ruben Belo nº55967

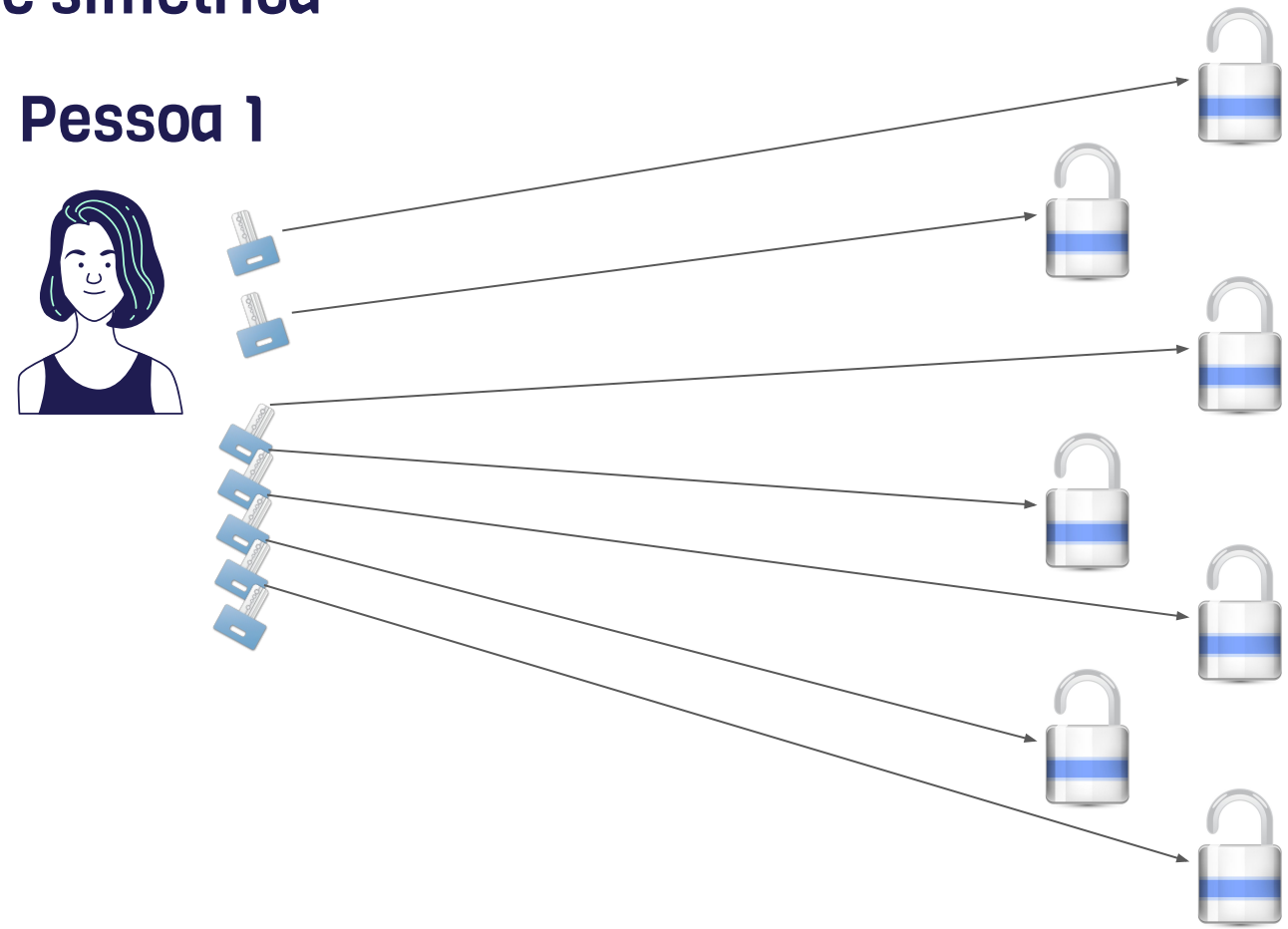
História

- Até aos anos 70 apenas existiam chaves simétricas
    - Ambas as partes necessitavam da mesma chave;
    - Dificuldades em transmitir a chave caso as partes não estivessem fisicamente no mesmo lugar



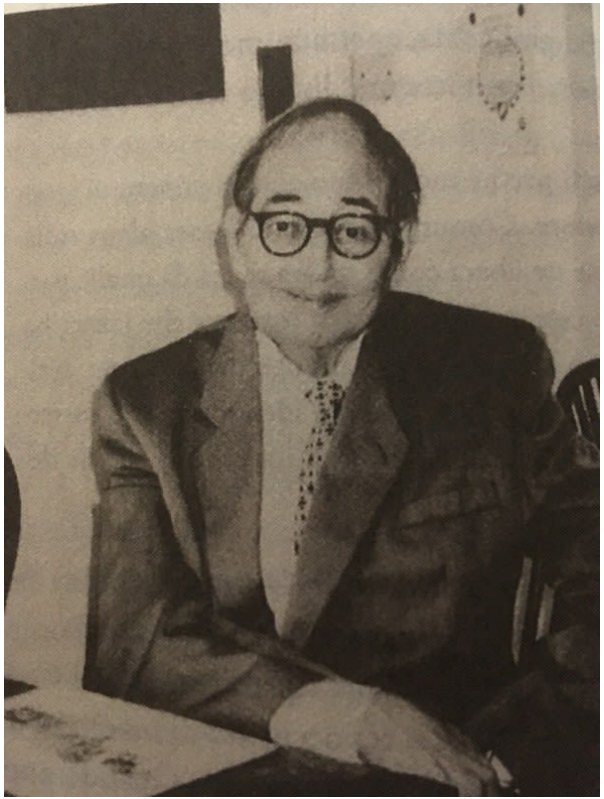
Chave simetrica

Pessoa 1

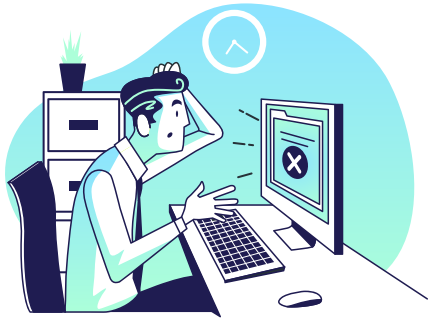


História

- Até aos anos 70 apenas existiam chaves simétricas
    - Ambas as partes necessitavam da mesma chave;
    - Dificuldades em transmitir a chave caso as partes não estivessem fisicamente no mesmo lugar
- 1970, James H. Ellis sugere “encriptação não secreta”(actualmente encriptação chave pública)
    - bloquear e desbloquear são operações inversas



Conceito de chave pública



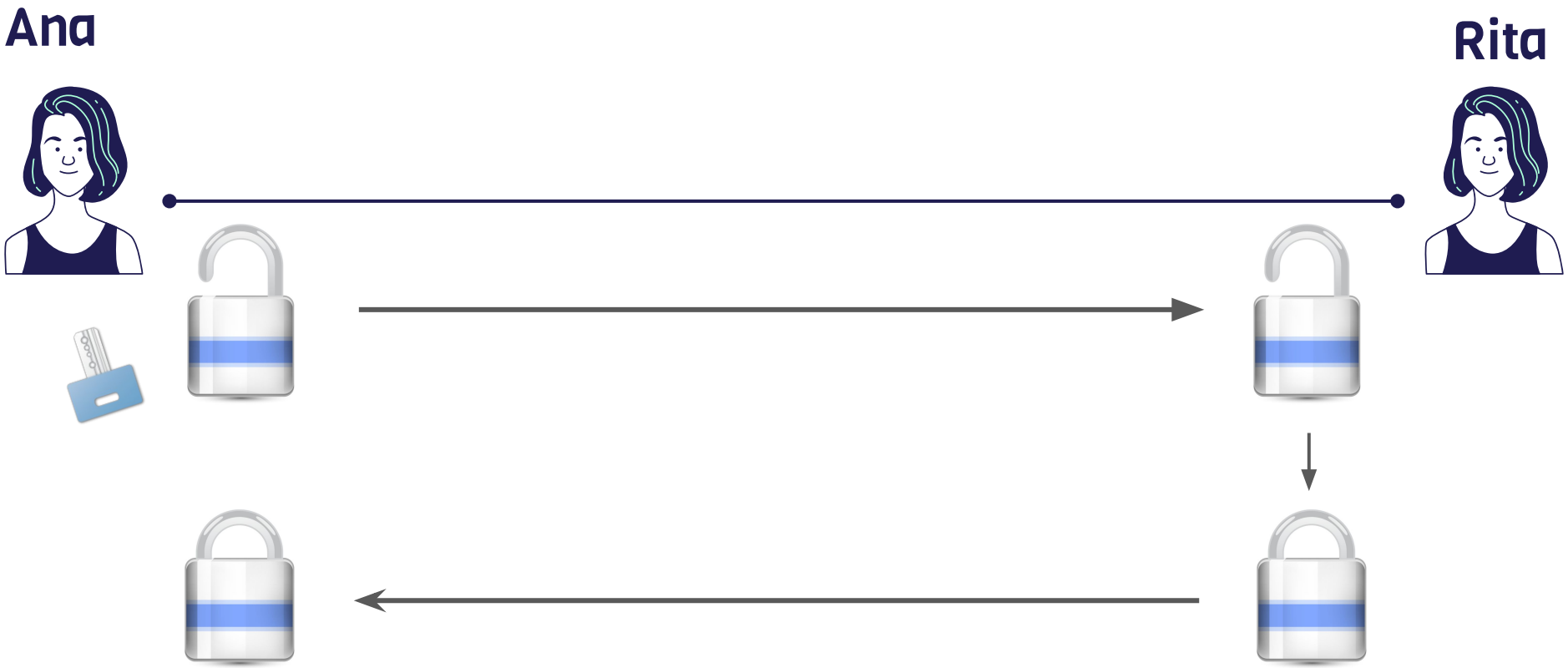
Chave de encriptação

Usada para encriptar uma mensagem, é a chave pública

Chave de Desencriptação

Usada para desencriptar uma mensagem, é a chave privada

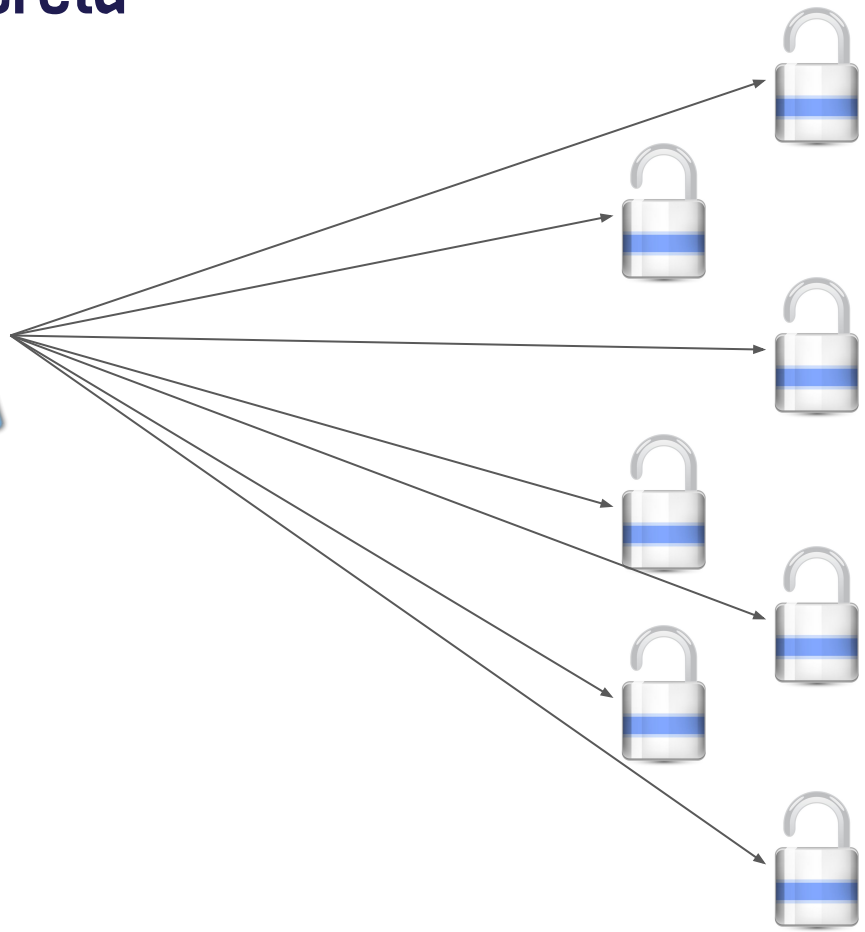
Encriptação não secreta



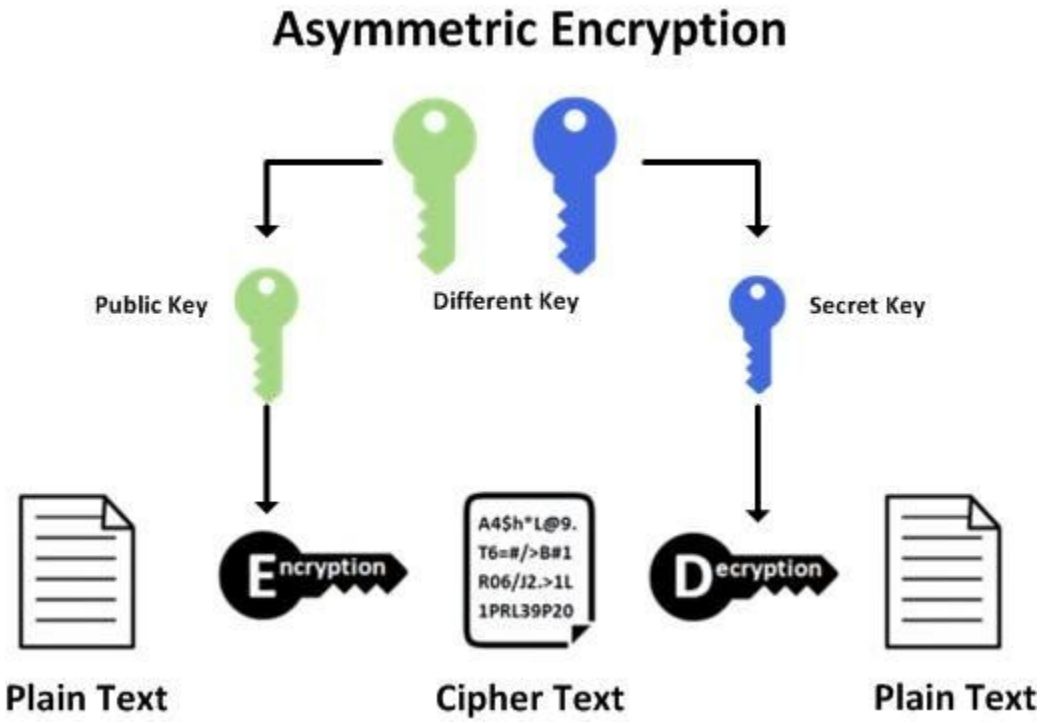
Encriptação não secreta

R

Pessoa



Caso típico de encriptação

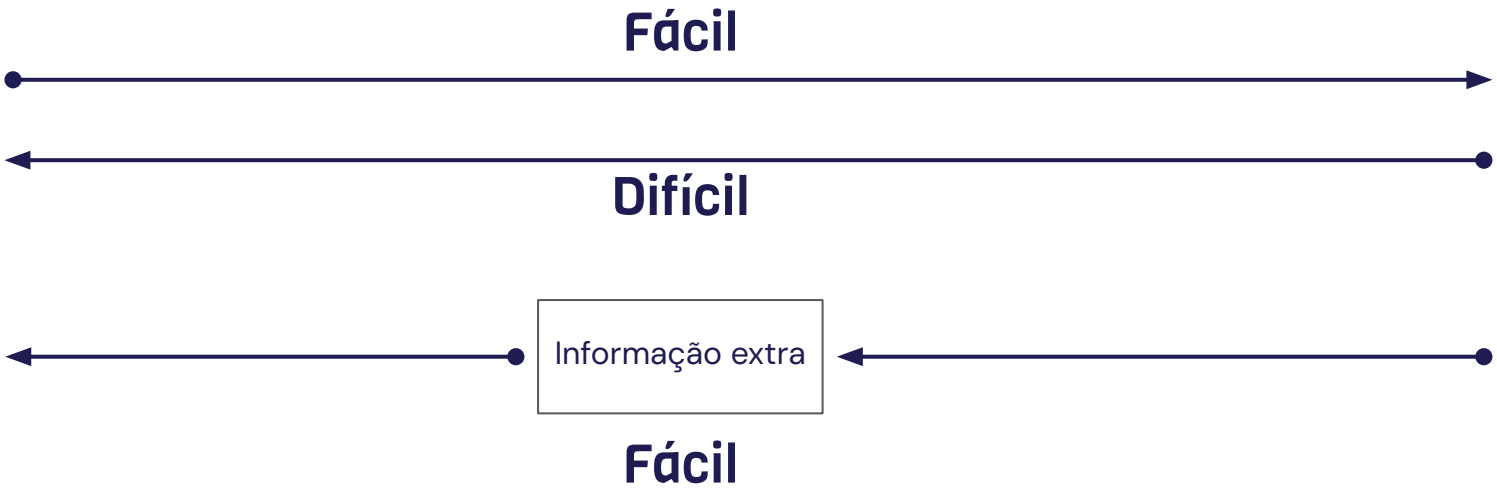


History

No entanto era necessário uma maneira de fazer estas funções de caminho único matematicamente

A solução foi descoberta por Clifford Cocks em 1973.

E redescoberta por Ron Rivest, Adi Shamir e Leonard Adleman, que descreveram o algoritmo publicamente em 1977



Ron Rivest

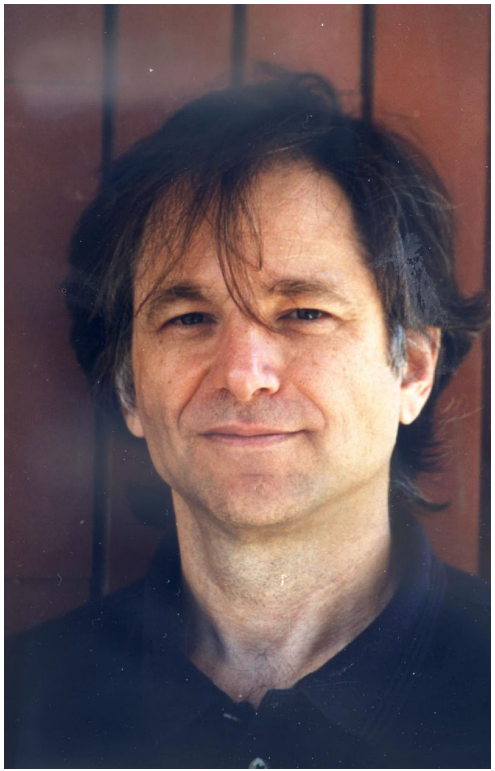
- Nasceu a 6 de Maio de 1947
- Licenciado em matemática em Yale
- Criptógrafo e Professor do MIT
- Departamento de Engenharia Electrotécnica e de computadores
- Tinha 30 anos quando inventou o algoritmo RSA

Adi Shamir

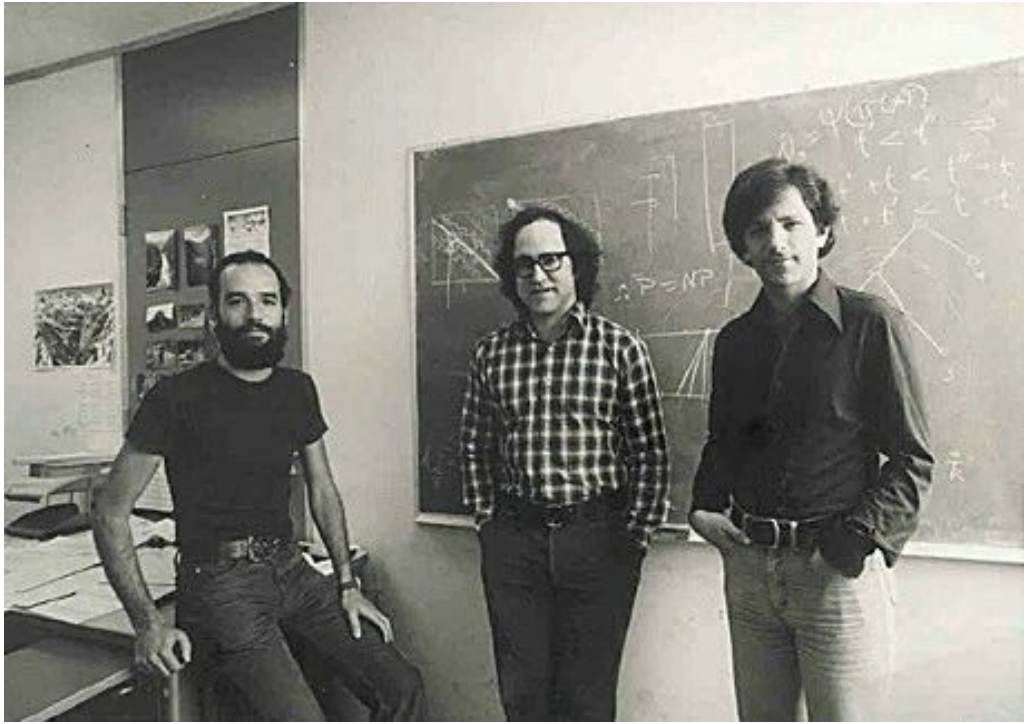
- Nasceu a 6 de Julho de 1952
- Licenciado em matemática na Universidade de Tel Aviv
  - Doutorado em filosofia
- Criptógrafo e fez investigação no MIT de 1977 a 1980
- Inventor de um método geral para decifrar cifras de bloco
- Tinha 25 anos quando inventou o algoritmo RSA

Leonard Adleman

- Nasceu a 6 de Maio de 1947
- Licenciado em matemática em Berkeley
  - Doutorado em Engenharia Electrotécnica e de computadores
- Criptógrafo
- Criou o estudo de computação de DNA
- Tinha 32 anos quando inventou o algoritmo RSA



Rivest–Shamir–Adleman



Exponenciação modular

Função unidirecional

Fácil

m mensagem
e expoente público
N número
c cifra

$$m^e \bmod N \equiv \boxed{c}$$

Difícil

a não ser que se tenha a chave

$$\boxed{?}^e \bmod N \equiv c$$

Fácil

Função unidirecional

$$m^e \bmod N \equiv c$$

Encripta →

$$c^d \bmod N \equiv m$$

← Desencripta

$$n^{ed} \bmod N \equiv m$$

↔ Encripta e Desencripta

Função unidirecional

$e*d$

e Encriptação
d Desencriptação

É necessário encontrar uma função e*d que torne difícil alguém encontrar o d.

Para isso é necessária outra função de caminho único.

Fatorização de números primos

Se multiplicarmos estes números primos é uma operação rápida

2x5x5 = 50

2 x 2 x 2 x 3 x 3 = 72

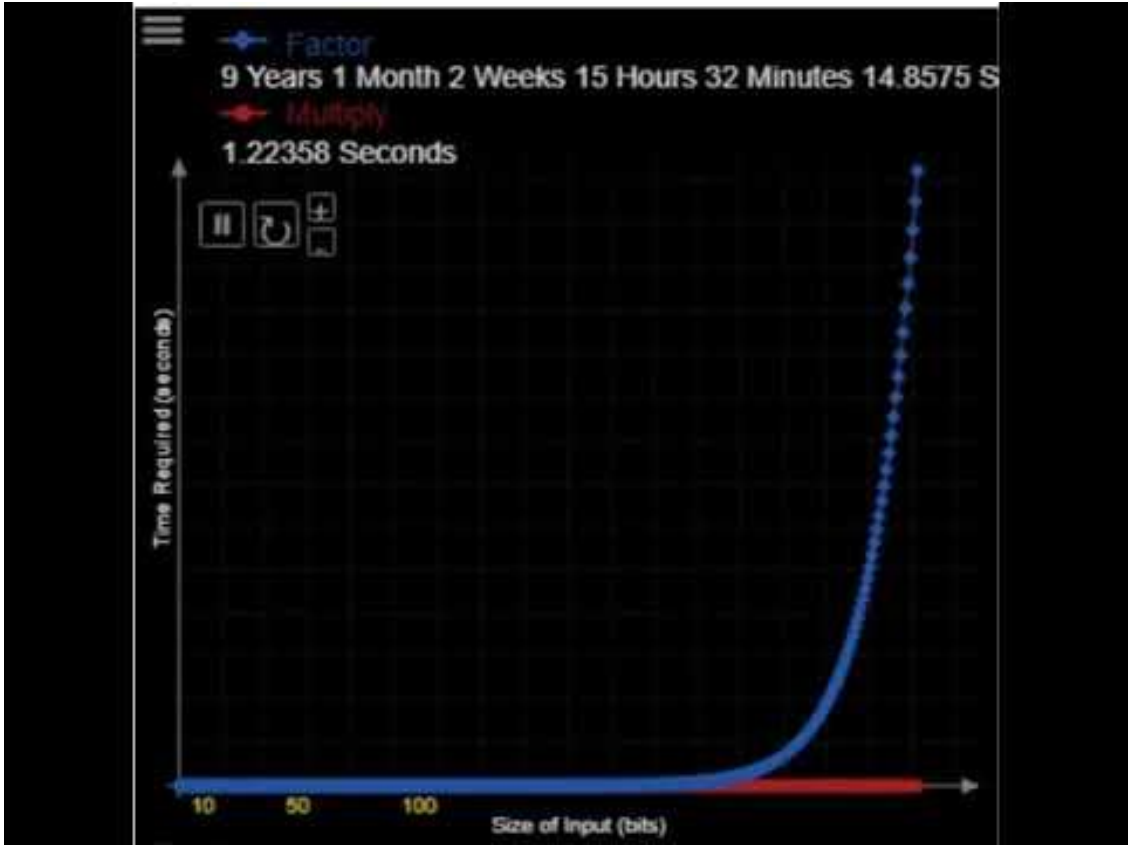
Cada número tem exatamente uma factorização por números primos, este cálculo é difícil

50 = 2x5x5

72 = 2 x 2 x 2 x 3 x 3

Dando um número N a uma pessoa é difícil de descobrir a sua factorização.

Video de complexidade temporal

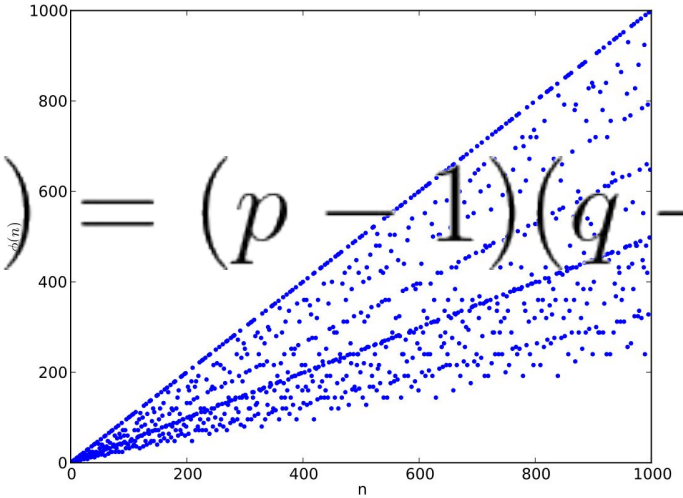


Phi function

Dado um número n a função phi diz-nos quantos inteiros menores ou iguais a n que não partilham nenhum fator comum.

$$\phi(8) = 4$$

$$\phi(n) = (p-1)(q-1)$$



sendo p um número primo

$$\phi(p) = p - 1 \quad \phi(7) = 6$$

$$\phi(a * b) = \phi(a) * \phi(b)$$

Phi function and euler's theorem

$$m^{\phi(n)} \equiv 1 \mod (n)$$

se m = 5 e n = 8

$$5^{\phi(8)} = 1 \mod (8)$$

$$regra\ 1 \rightarrow 1^x = 1$$

$$regra\ 2 \rightarrow 1 * m = m$$

Phi function and euler's theorem

R

$$regra\ 1 \rightarrow 1^x = 1$$
$$regra\ 2 \rightarrow 1 * m = m$$

pela regra 1:

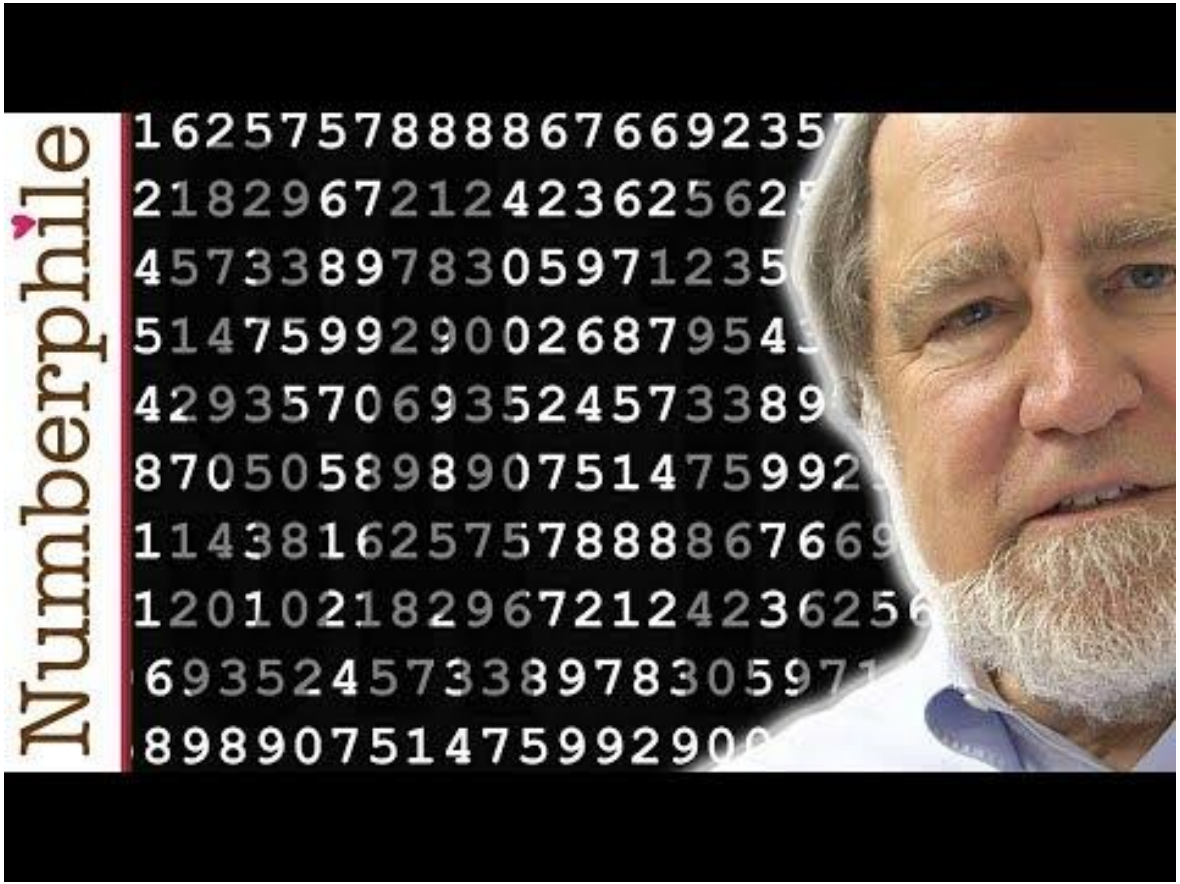
$$m^{\phi(n)*x} \equiv 1 \mod n$$

pela regra 2:

$$m * m^{\phi(n)*x} \equiv m \mod n$$

$$m^{\phi(n)*x+1} \equiv m \mod n \qquad m^{e*d} \equiv m \mod n$$

$$d * e = \phi(n) * x + 1 \qquad d = \frac{\phi(n) * x + 1}{e}$$


Numberphile

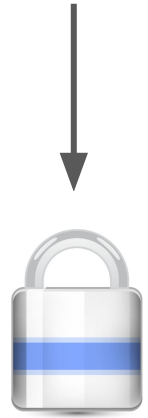
RSA e como codificar

Escolher 2 números primos **q** e **p**.

A chave **n** vai ser **q***p e ainda precisamos de h em que **h** = φ(n)=(p-1)*(q-1).

Escolher um número **e**, tal que mdc(e, h) = 1(números primos entre si); 3<=e<λ(n)

Escolher uma mensagem **m**.



Com **p** = 7 e **q** = 11
temos que:
n = 77
h = 60
e = 13
m = "RSA"

$$\lambda(n) = mmc(\lambda(p), \lambda(q))$$

$$mmc(\lambda(p), \lambda(q)) = mmc(\phi(p), \phi(q))$$

$$mmc(\phi(p), \phi(q)) = mmc(p-1, q-1)$$

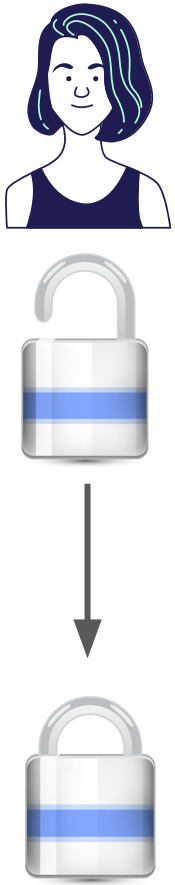
RSA e como codificar

n = 77
e = 13
m = “RSA” -> 27 28 10

Codificação é do tipo b^e = a (mod n) com b igual a blocos da mensagem.

27^13 mod 77 = 48
28^13 mod 77 = 07
10^13 mod 77 = 10

Mensagem codificada é agora 48 07 10



RSA e como decodificar

n = 77
h = 60
e = 13

Primeiro precisamos de um novo número d, onde d*e ≡ 1 mod h (Modular Multiplicative Inverse), sendo assim d = 37

Mensagem codificada 48 07 10
Decodificação é do tipo b^d mod n= m

48^37 mod 77= 27
07^37 mod 77= 28
10^37 mod 77= 10

Mensagem depois da decodificação “RSA”.

Segurança

Nos tempos correntes usa-se 2048-RSA e isso equivale a uma chave com 617 dígitos.

Impossível em tempo real descobrir os 2 primos que deram origem a esta chave, logo é impossível descobrir a chave privada para decodificar a mensagem.

RSA exemplo real

p:11857407391753961498983063157882742809161776602065139425839485863245671150175442433397785505916199222668279819714869888183067295357435343896677593769659139346271877017110953986519443415970108426602191212138509703548884881221446641077266706497741456463691727206656507053389547795074581120313125992349878260709 99

q:16775263924552680832641895548215537513170427364573409439873993347355672041925673009392047189949907824752566617871452169005036183468045781597773446971031120546687924536749801552902310144754438362875218199840875027813650507371103192252024283400800293355834147566021441917060871528094711791924474216296619144 5487

n:19891113845761452720822428847814269406813707639686639272643718513690549999086644755305505321652633168656870656942124766997658987684896556500505215070611172861619532799743220406537017793879262723319963016166698723011454651498036983372292480274135038051229380739044633874842479992895406078352560220533618412201779924922955319156628865628960846268422489930526491159531076692948100124093094320240882956424866459909534090568268257249695443207793728312474538246032946679534381878437815667334018920233116267592598162391470287717547312401665212131081374126163632099538988987650395092126366159411383677269120761367575719771221 3

RSA exemplo real

R

e:3

d:132607425638409684805482858985428462712091384264577595150958123424603666660577631702036702144350887791045804379614165113317726584565977043336701433804074485744130218664954802710246785292528418155466420107779914867430310099869132224819498684942335870081958715936308924989498666193027071890170681368907894146783419483442600834286482711350316532540010515103990174044357547582499918726732880319872874915266690190807549608712129012833822648597883145798672480352817094642761471792263660786306477778159448053541383531966060199078985134204844153183472209084339356647964207525181142877061049339214292290458877410595281491064 19

msg cifrada:
205597153136827524204201637979402762823511735838012497706260289708548851222455417942123804311915200572818256586604333455214843671957074987528028311086931581295668715971002865518754943727414962559177329525449119875112600653851831981941448199953470725093641674 7

msg decifrada: Atacar a ultima posiçao dos inimigos

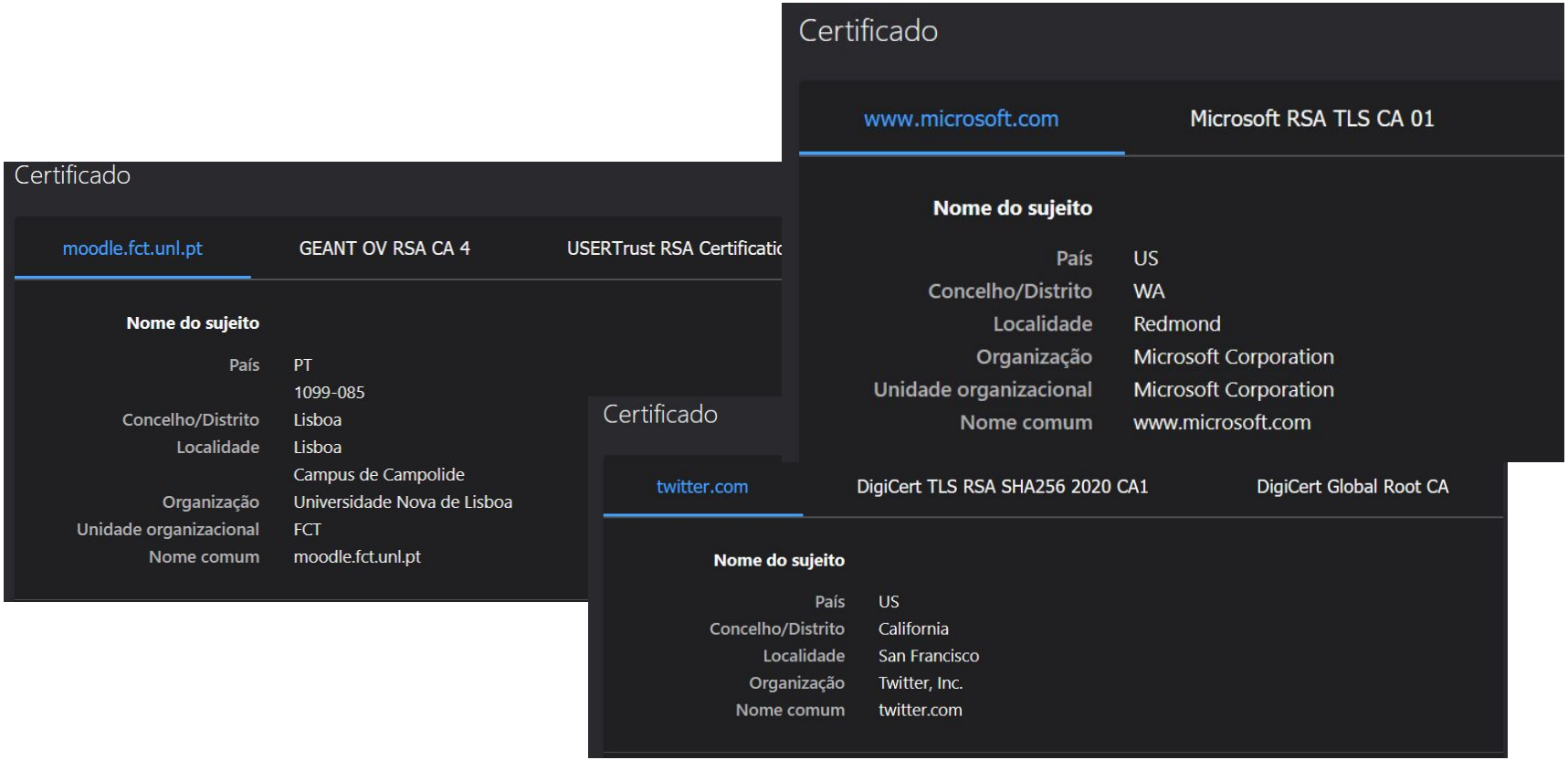
RSA exemplo real

Chave pública:
n:19891113845761452720822428847814269406813707639686639272643718513690549999086644
75530550532165263316865687065694212476699765898768489655650050521507061117286161
95327997432204065370177938792627233199630161669872301145465149803698337229248027 4
13503805122938073904463387484247999289540607835256022053361841220177992492295531
91566288656289608462684224899305264911595310766929481001240930943202408829564 24
86645990953409056826825724969544320779372831247453824603294667953438187843781 5
66733401892023311626759259816239147028771754731240166521213108137412616363209953898 8
98765039509212636615941138367726912076136757571977122 13

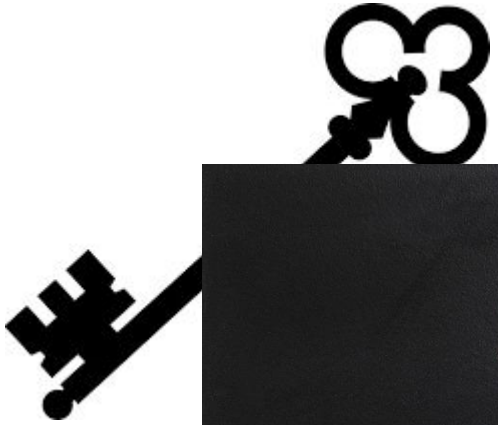
e:3

Chave privada:
d:13260742563840968480548285898542846271209138426457759515095812342460366666057 7
63170203670214435088779104580437961416511331772658456597704333670143380407448574 41
30218664954802710246785292528418155466420107779914867430310099869132224819498684 9
42335870081958715936308924989498666193027071890170681368907894146783419483442600 0
83428648271135031653254001051510399017404435754758249991872673288031987287491526 66
90190807549608712129012833822648597883145798672480352817094642761471792263660786 3
06477778159448053541383531966060199078985134204844153183472209084339356647964207 5
25181142877061049339214292290458877410595281491064 19

Uso do RSA


Certificado
www.microsoft.com
Microsoft RSA TLS CA 01
Nome do sujeito
País US
Concelho/Distrito WA
Localidade Redmond
Organização Microsoft Corporation
Unidade organizacional Microsoft Corporation
Nome comum www.microsoft.com
Certificado
moodle.fct.unl.pt
GEANT OV RSA CA 4
USERTrust RSA Certificatic
Nome do sujeito
País PT
1099-085
Concelho/Distrito Lisboa
Localidade Lisboa
Campus de Campolide
Organização Universidade Nova de Lisboa
Unidade organizacional FCT
Nome comum moodle.fct.unl.pt
Certificado
twitter.com
DigiCert TLS RSA SHA256 2020 CA1
DigiCert Global Root CA
Nome do sujeito
País US
Concelho/Distrito California
Localidade San Francisco
Organização Twitter, Inc.
Nome comum twitter.com

Falhas do RSA

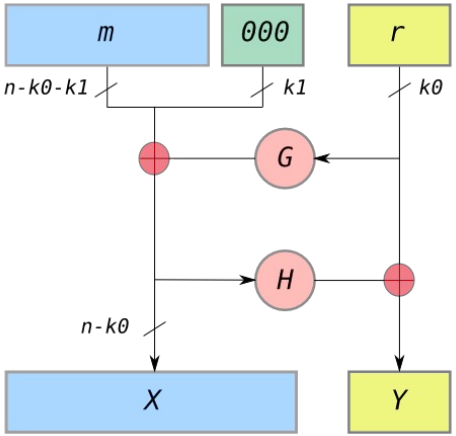


Conseguir

utacional

Falhas do RSA

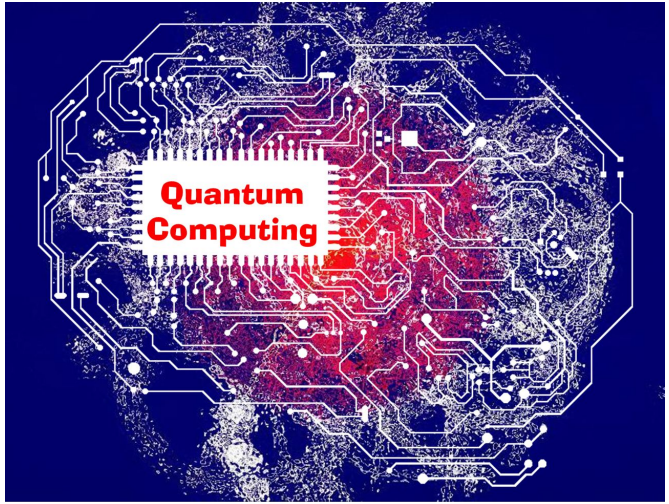
- Usar geradores fracos de números primos.
- Fraca geração de chaves.
- Side channel attacks.



RSA o futuro e a computação quântica

- Por agora é considerado seguro.
- Chaves de 2048 bits até 2030.
- Chaves de 3072 bits além de 2030.

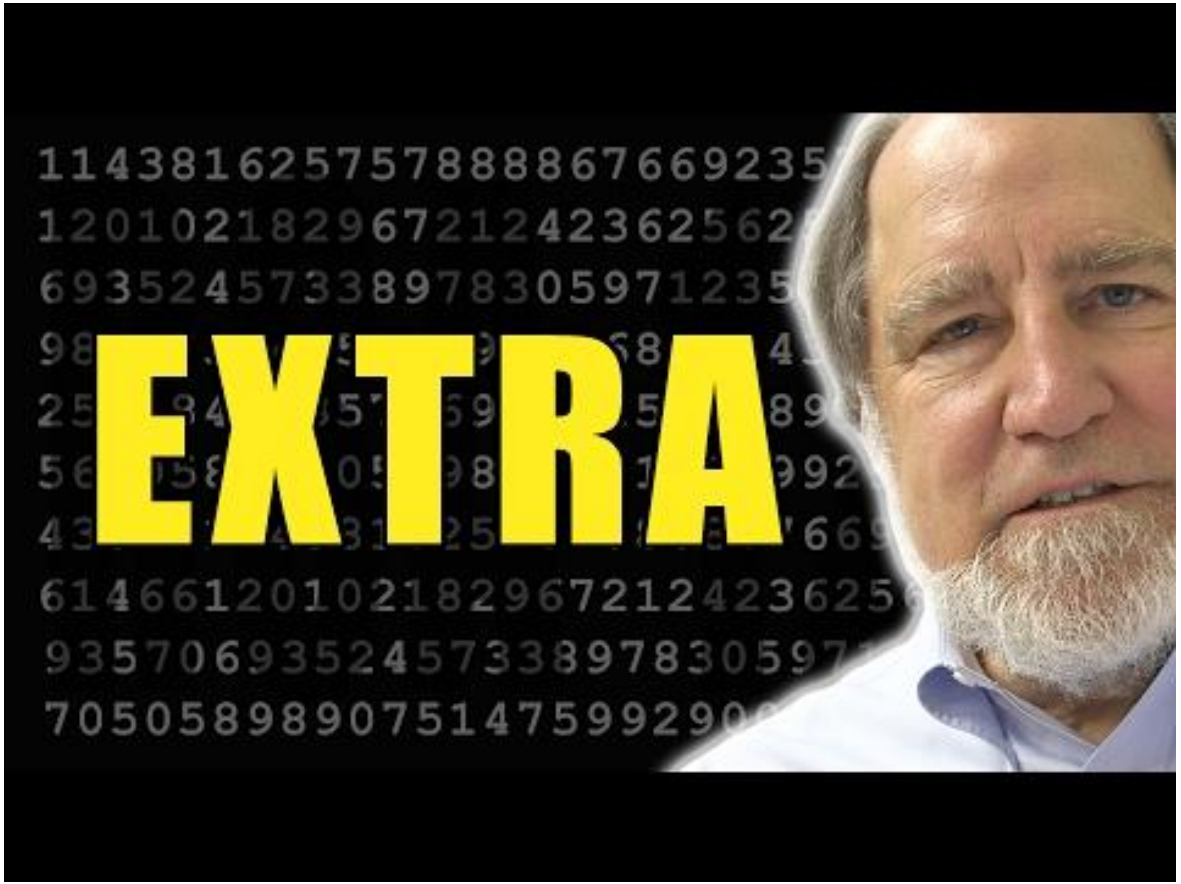
RSA o futuro e a computação quântica



Problemas:

- the integer factorization problems
- the discrete logarithm problem
- the elliptic-curve discrete logarithm problem.

RSA o futuro e a computação quântica



RSA vs outros

Tamanho da chave equivalente (bits)		
Simétrico	**ECDSA**	**RSA**
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

RSA VS Curvas Elípticas[R]

- Vantagem do titular
- Forte segurança
- Suporte Amplo

- Melhor segurança
- Melhor eficiência
- Perfect forward secrecy

Obrigado!

Do you have any questions?

Trabalho de Criptografia

RSA

Martim Vieira nº47268
Ruben Belo nº55967