



RSA

João Veloso 49475
Luís Grilo 48235



Sumário

01

Contexto Histórico

02

Função Totiente de Euler

03

Algoritmo

04

Ataques



Contexto
histórico

Contexto histórico



1960

A criptografia era baseada apenas em chaves simétricas.

Desvantagens das chaves simétricas



Necessidade de possuir
uma chave, distinta, para
cada um dos seus
clientes



As chaves necessitam
ser mudadas
frequentemente



As chaves tem de ser
mantidas seguras
durante a distribuição e
no serviço



Numa população de n
pessoas, um total de
 $\frac{n(n-1)}{2}$
chaves são necessárias

Contexto histórico

1960

A criptografia era baseada apenas em chaves simétricas.

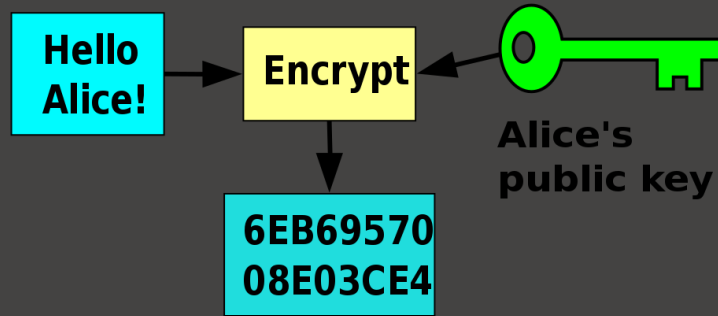
1970

Em 1970 James Ellis, engenheiro britânico trabalhou num conceito para recorrer ao uso de uma encriptação com chave pública.

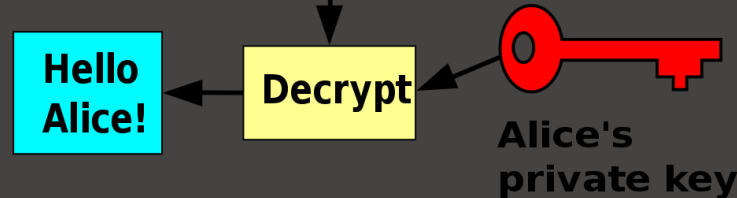


Criptografia de chave pública

Bob



Alice



Vantagens da Criptografia de chave pública



Não é compartilhada a
chave secreta

Possibilidade de validar
assinatura com a chave
privada através da chave
pública

Permite o não-repúdio,
pois é possível verificar
as chaves

É escalável em
comparação com a
criptografia de chaves
privadas

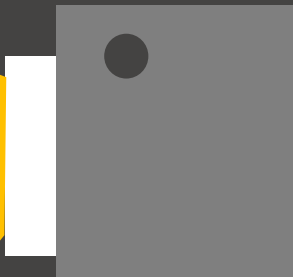
Desvantagens da Criptografia de chave pública



Lenta



Necessário uma autoridade de
certificação



Função Totiente de Euler

$$\phi(x) = \# \{k \in \mathbb{N} | k \leq x \wedge \text{mdc}(k, x) = 1\}$$

Função Totiente de Euler

Duas propriedades que são úteis para a utilização desta função no algoritmo RSA:

01 Sendo P um número primo então $\Phi(P) = P - 1$

02 $\Phi(A * B) = \Phi(A) * \Phi(B)$ se $\text{mdc}(A, B) = 1$

Contexto histórico

Cliffor Cocks, um matemático Inglês desenvolveu um sistema equivalente

O RSA é publicado

1973

1978

1977

Ron Rivest, Adi Shamir e Leonard Adleman, foram os “primeiros” a descrever o algoritmo

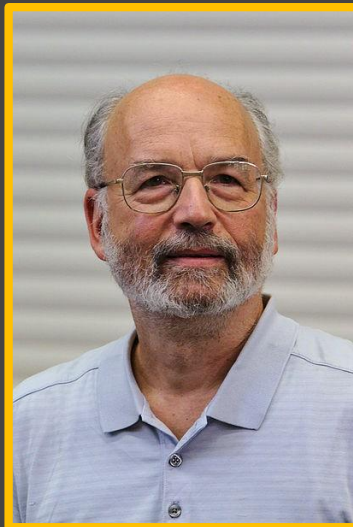
1997

A agência de inteligência britânica (GCHQ) revela ter desenvolvido um algoritmo equivalente

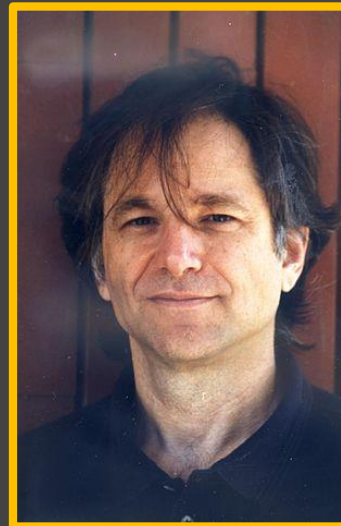
RSA



Ronald Rivest



Adi Shamir

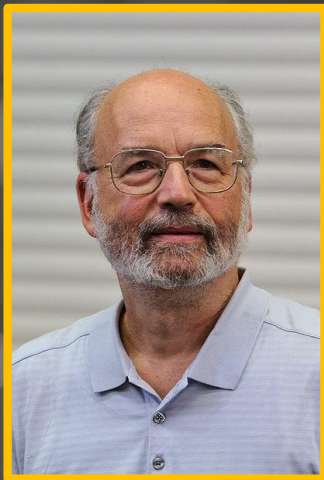


Leonard Adleman



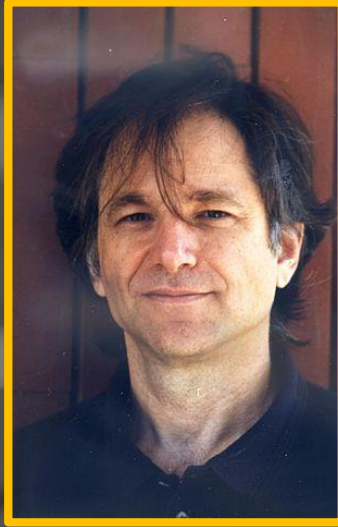
Ronald Rivest

- Nasceu a 6 de Maio de 1947 em New York
- Professor no MIT
- Prémio Turing (2002)
- Prémio Marconi (2007)



Adi Shamir

- Nasceu a 6 de julho de 1952 em Tel Aviv, Israel
- Matemático, criptólogo e cientista da computação
- Prêmio Turing (2002)
- Professor Instituto de Tecnologia de Massachusetts



Leonard Adleman

- Nasceu a 31 de dezembro de 1945 em São Francisco
- Informático e Biólogo Molecular
- Professor na Universidade do Sul da Califórnia
- Professor no Instituto de Tecnologia de Massachusetts
- Prêmio Turing (2002)



Algoritmo

Geração das chaves

Escolher p, q ambos primos e diferentes

Calcular $n = p * q$

Calcular $\Phi(n) = (p - 1)(q - 1)$

Escolher inteiro e $\gcd(\Phi(n), e) = 1, 1 < e < \Phi(n)$

Calcular d

$$d \bmod \phi(n) = 1$$

Chave Publica

$$KU = \{ e, n \}$$

Chave Privada

$$KR = \{d, n\}$$

Encriptação

Plaintext:

$M < n$

Ciphertext:

$$C = M^e \pmod{n}$$

Descrição

Ciphertext :

C

Plaintext :

$$M = c^d \pmod{n}$$

Requisitos do Algoritmo



É possível encontrar valores e, d, n tal que
 $M^{e*d} \bmod n = M$
para todo $M < n$

É relativamente fácil
calcular M e C para todos
os valores de $M < n$

É inviável determinar d
dado E e N

Exemplo RSA



Escolher dois números
primos
 $p = 17$ e $q = 11$



Calcular
 $n = p * q$
 $17 * 11 = 187$



$\Phi(n) = (p - 1)(q - 1)$
 $= 16 * 10$
 $= 160$



Escolher e tal que seja
relativamente primo a
 $\Phi(n)$ e menor que $\Phi(n)$
Escolhemos $e = 7$



Determinar d tal que
 $\text{mod } 160 = 1$ e $d < 160$
Assim obtemos
 $d = 23$ pois,
 $23 * 7 = 161 = (1 * 160) + 1$

Resultado do Exemplo

O resultado anterior são as chave pública $PU = \{7, 187\}$ e a chave privada $PR = \{23, 187\}$





Ataques

Ataques

RSA é um sistema muito utilizado por isso vem tendo vulnerabilidades ao longo dos anos.

Existe uma lista completa de todos os ataques que se conhecem num artigo de um professor, Dan Boneh.



Ataques matemáticos

- Factorização de n nos números primos iniciais o que permite o cálculo de $\Phi(n) = (p - 1) * (q - 1)$ o que por sua vez permite determinar $d \equiv e^{-1}(\text{mod } \phi(n))$.
- Determinar $\Phi(n)$ diretamente sem necessidade de determinar p e q o que permite determinar $d \equiv e^{-1}(\text{mod } \phi(n))$.
- Determinar d directamente sem primeiro determinar $\Phi(n)$.



Força Bruta

A defesa para ataques de forma bruta é a mesma para outros sistemas criptográficos, nomeadamente usar uma chave grande. Assim um maior d é mais seguro porém a descriptação e encriptação fica mais complexa tornando o sistema mais lento.

Expoente Público pequeno

Tal como o expoente privado pequeno, pode-se cair na tentação de escolher um expoente público pequeno e na tentativa de acelerar processo de encriptação.

Ao contrário do ataque anterior, este não leva à ruptura da segurança do RSA, mas o objectivo é descriptar uma mensagem sem precisar de descobrir a chave privada.

Ciphertext:

$$C = M^e \pmod{n}$$



Expoente Privado pequeno

Isto acontece quando, na tentativa de tornar o processo de descriptação mais rápido, podemos acabar por escolher um expoente privado “pequeno”.

Isto pode levar à ruptura total da segurança do RSA, ou seja, consegue-se determinar o expoente privado d e consequentemente a factorização de n .

Number of Decimal Digits	Approximate Number of Bits	Date Achieved	MIPS-Years
100	332	April 1991	7
110	365	April 1992	75
120	398	June 1993	830
129	428	April 1994	5000
130	431	April 1996	1000
140	465	February 1999	2000
155	512	August 1999	8000
160	530	April 2003	—
174	576	December 2003	—
200	663	May 2005	—

Conclusão



01

Rivest, Shamir e Adleman são os principais responsáveis pelo algoritmo RSA.

02

Até hoje, é considerado a mais bem sucedida implementação de sistemas de chaves assimétricas.


03

Funciona com um par de chaves, uma pública e privada.

04

Hoje em dia está presente em locais como emails, compras na internet, etc

Bibliografia

- 
- W. Stallings, Network Security Essentials - Applications and Services, Pearson, 6/E, 2017
W. Stallings, L. Brown, Computer Security: Principles and Practice, Pearson 4/E, 2014
W. Stallings, Cryptography and Network Security - Principles and Practice, Pearson 7/E, 2017
D. Gollmann, Computer Security, 3rd Ed, Wiley, 2011
B. Schneier, Applied Cryptography, 1996, Wiley
A. Zúquete, Segurança em Redes Informáticas, 5ª Ed., 2018, Ed. FCA
M. Correia, P. Sousa, Segurança no Software, 2ª Ed. , 2017 Ed. FCA
<https://pt.wikipedia.org/wiki/RSA>
https://www.youtube.com/watch?v=wXB-V_Keiu8
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.182.9999&rep=rep1&type=pdf>



Obrigado

Questões ?