UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 01º de Junho de 2017

- CRIPTOGRAFIA RSA
  - ADLEMAN (EUA)
  - SHAMIR (ISRAEL)
  - RIVEST (EUA)

=> Desenvolvido entre 1977 e 1979

=> Os 3 ganharam o prêmio Turing de 2002 pelo RSA (US$ 250 mil)

=> Primeiro método concreto de criptografia de chave pública.

- CRIPTOGRAFIA DE CHAVE PÚBLICA:

=> Duas chaves (inter-relacionadas)

=> Chave pública para encriptação

=> Chave privada para decriptação (apenas o destinatário da mensagem possui).

- PRIMEIRA FASE: GERAÇÃO DO PAR DE CHAVES

1) Seleciono dois primos distintos p e q

2) Calculo $n = pq$

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

(/ /)

4) Selecionar um inteiro e no intervalo $1 < e < \phi(n)$ tal que e possua inverso modulo $\phi(n)$, isto é, $MDC(e, \phi(n)) = 1$

5) Calcule d, o inverso de e modulo $\phi(n)$.

6) A chave pública é o par (n, e)

7) A chave privada é o par (n, d)

=> Quem faz os cálculos da geração dessa chaves é o destinatário, que então divulga a chave pública e mantém para si os demais valores.

- Segunda Fase: Pré Criptografia

=> Se o conteúdo da mensagem a ser encriptada não for numérico, precisamos fazer uma pré-codificação

=> Podemos utilizar qualquer tabela de correspondencia entre caracteres e números como a tabela ASCII ou a tabela Unicode

=> Nas nossas mensagens, utilizaremos apenas letras maiúsculas e espaços. Podemos então utilizar uma tabela simplificada.

- Primeiro impulso de tabela simplificada:

A -> 1
B -> 2
C -> 3
⋮
Z -> 26
Espaço -> 27

Não dá certo!

11 → AA?
11 → K?

- Vamos

A -> 10

B -> 11

⋮

Z -> 35

espaço -> 99

Exemplo:

H	A	Y	N	I	E		W	I	C	Z
↓	↓	↓	↓	↓	↓		↓	↓	↓	↓
17	27	34	23	18	14		32	18	12	35

- Terceira Fase: Encriptação

=> A mensagem é um número grande

=> Preciso quebrar a mensagem em blocos $b_1, b_2, \cdots, b_k$, de forma que:

1) $b_i < n$, para todo $1 \leq i \leq k$.

2) O primeiro algarismo de todos os blocos precisa ser diferente de zero.

Exemplo:

$p = 11, \quad q = 13$

$n = p \cdot q = 11 \cdot 13 = 143$

$\phi(n) = (p-1)(q-1) = 10 \cdot 12 = 120$

$e = 2, 3, 4, 5, 6, 7$

$d =$

/ /

$d \cdot 17 = 108$

R	Q	X	Y
7	-	1	0
120	-	0	1
7	0	1	0
1	17	-17	1
0	7	-	-

- QUEBRANDO A MENSAGEM EM BLOCOS

HRYNIGWICZ

⇓

17 2 7 3 4 23 18 14 3 2 18 1 2 3 5

17 - 2 - 7 3 - 4 2 - 8 1 - 8 - 14 - 32 - 18 - 123 - 5

⇒ Encriptamos cada bloco separadamente e enviamos os blocos encriptados também separadamente

⇒ Seja b um bloco. A encriptação de b, denotada por $c(b)$ é a forma reduzida de b^e módulo n.

EXEMPLO:

$c(17) = 17^7 \pmod{143} = 30$

$c(2) = 2^7 \pmod{143} = 128$

⋮

$c(5) = 5^7 \pmod{143} = 47$

30 - 128 - ... - 47

Quarta Fase: Decriptação

Seja b' um bloco encriptado. A decriptação do b', denotada por $D(b)$ é a forma reduzida de $(b')^d$ módulo n.

Exemplo:

$D(30) = 30^d \pmod{143} = 30^{103} \pmod{143} = 17$

$D(128) = 128^{103} \pmod{143} = 2$

$\vdots$

$D(47) = 47^{103} \pmod{143} = 5.$

Duas Perguntas:

(1) Por que funciona?

(2) Por que é seguro?

(1) Quero mostrar que, para qualquer bloco b:

$$D(C(b)) = b$$

$$C(b) \equiv b^e \pmod{n}$$

$$D(C(b)) = (b^e)^d \pmod{n} \equiv b^{ed} \pmod{n}$$

$$ed \equiv 1 \pmod{\phi(n)}$$

$$ed = 1 + k\phi(n) = 1 + k(p-1)(q-1)$$

$$b^{ed} \equiv b^{1+k(p-1)(q-1)} \equiv b\,(\underbrace{b^{p-1}}_{\equiv 1})^{k(q-1)} \equiv b \pmod{p}$$

$$b^{ed} \equiv b^{1+k(p-1)(q-1)} \equiv b\,(\underbrace{b^{q-1}}_{\equiv 1})^{k(p-1)} \equiv b \pmod{q}$$

/ /

p divide $b^{ed} - b$

q divide $b^{ed} - b$

↳ Primos Distintos

$\Rightarrow n = p \cdot q$ divide $b^{ed} - b$

$\Downarrow$

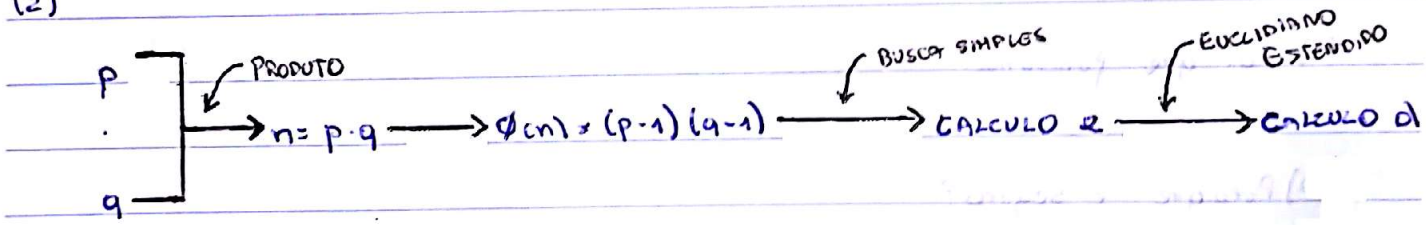
$b^{ed} \equiv b \pmod n$

$D(C(b)) \equiv b^{ed} \equiv b \pmod n$

Mas tanto $D(C(b))$ quanto b estão no intervalo entre 1 e $n-1$. Logo, se são congruentes, são também iguais:

$D(C(b)) = b.$

(2)



Suponha que tenho apenas a chave pública (n, e)

Para calcular $\phi(n)$ preciso conhecer os fatores de n.

$\Downarrow$

Logo, a segurança do RSA depende da dificuldade da fatoração de inteiros grandes).

EXEMPLO. - CAPÍTULO 11

6355 - 5075

n = 7597

e = 4947

Vamos fatorar com o método de Fermat:

$[\sqrt{n}] = [\sqrt{7547}] = 87$, $y = [\sqrt{x^2 - n}]$

x	y	$x^2 - y^2 = n$
87	0	NÃO
88	12	NÃO
89	18	SIM

$x + y = 107$

$x - y = 71$

} FATORES

$\phi(n) = (p-1)(q-1) = 106 \cdot 70 = 7420$

R	Q	x	y
4947	-	1	0
7420	-	0	1
4947	0	1	0
2473	1	-1	1
1	2	3	-2
0	2473	-	-

$D(6355) = 6355^3 \pmod{7597} = 151$

$D(5075) = 5075^3 \pmod{7597} = 822$

151822 = 15-18-22 = F-I-M