

Martin Hellman

Diffie Hellman key exchange DH

1976

New Directions in Cryptography

1976

子

1978

R. L. Rivest

A. Shamir

L. M. Adleman

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

1978

RSA

RSA

RSA

2002

RSA= $\langle p, q, n, m, e, d, k, c \rangle$

1976

1 $p, q, n, m, e, d, k, c \in Z^*, Z^* = \{1, 2, 3, \dots\}$

2 p, q 各 $n = p \times q$

3 $(e, n): (d, n):$

4 $m: m < n$

5 $c:$

6 $k(m^{k(p-1)(q-1)} \pmod n) = 1$

7 $k(ed = k(p-1)(q-1)+1)$

8 $c = m^e \pmod n$

9 $m = c^d \pmod n$

1 各 p, q

2 $e \in (p-1)(q-1) \quad 0 < e < (p-1)(q-1)$

3 $d \in k(ed = k(p-1)(q-1)+1)$

3. RSA 1976

1 $m \quad c = m^e \pmod n$

2 $c \quad m = c^d \pmod n$

RSA 1976 $(e, n) \quad (d, n) \quad p \quad q$

$k(m^{k(p-1)(q-1)} \pmod n) = 1$

CS

例 $p=3, q=11, n = 3 \times 11 = 33$

$m=2 \quad m < n, k=1$

$m^{k(p-1)(q-1)} \pmod n = 2^{1 \times (3-1) \times (11-1)} \pmod 33$

$= 2^{20} \pmod 33$

$= 1048576 \pmod 33$

$$\begin{aligned}
&= 1 \\
m=2 \quad m < n, \quad k=2 \\
m^{k(p-1)(q-1)}(\bmod n) &= 2^{2 \times (3-1) \times (11-1)}(\bmod 33) \\
&= 2^{40}(\bmod 33) \\
&= 1\,099\,511\,627\,776 \pmod{33} \\
2 &= 1 \\
m=2 \quad m < n, \quad k=3 \\
m^{k(p-1)(q-1)}(\bmod n) &= 2^{3 \times (3-1) \times (11-1)}(\bmod
\end{aligned}$$

$$=2187 \pmod{33}$$

$$=9$$

例 $p=223092827, q=218610473 \quad n=487\,704\,284\,333\,771\,171$ RSA
 p, q, n

e

$$p=223\,092\,827, q=218\,610\,473 \quad (p-1) \times (q-1) = (223\,092\,827-1) \times (218\,610\,473-1)$$

$$= 48\,770\,427\,991\,673\,872$$

RSA $e \quad 48\,770\,427\,991\,673\,872$

$$e=2 \quad 48\,770\,427\,991\,673\,872 \pmod{2} = 0$$

$$e=3 \quad 48\,770\,427\,991\,673\,872 \pmod{3} = 1$$

$$3 \quad 48\,770\,427\,991\,673\,872 \quad e=3$$

d

子 $k \quad ed = k(p-1)(q-1) + 1$ 子 k

$$d = (k(p-1)(q-1) + 1) / e$$

$$e = 3 \quad p=223\,092\,827, q=218\,610\,473$$

$$d = (48\,770\,427\,991\,673\,872k + 1) / 3$$

$$k=1 \quad d = 48\,770\,427\,991\,673\,873 / 3$$

$$k=2 \quad d = 97\,540\,855\,983\,347\,745 / 3$$

$$= 32\,513\,618\,661\,115\,915$$

$$d \quad d = 32\,513\,618\,661\,115\,915$$

RSA $(3, 487\,704\,284\,333\,771\,171)$

(32 513 618 661 115 915, 487 704 284 333 771 171)

RSA $\overline{c^e} \quad e, n \quad (c)$

了 够 $p \quad q \quad n=p \quad q \quad ,$

位

⇒

$p=11, q=13$

RSA

9