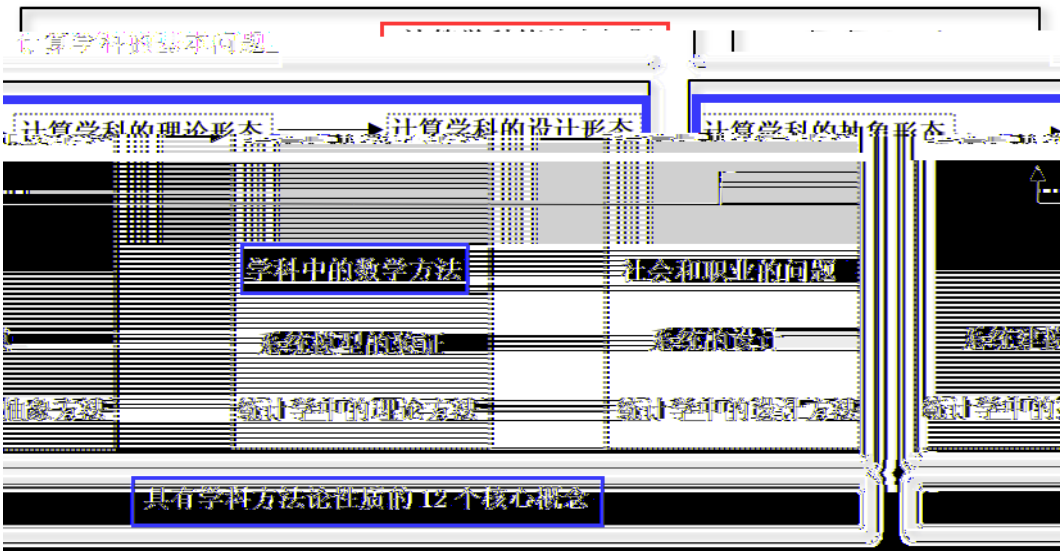
科学思维-样例：RSA 公开密钥密码系统

了 元认知知识

创造 够

1. 严



严

严 参 了

位

严 严

机 严

严 严 加

机

严

严 1976 Whitfield Diffie

Martin Hellman Diffie Hellman key exchange DH
」 *New Directions in Cryptography*
」

子

1978 R. L. Rivest A. Shamir
L. M. Adleman *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*
」 RSA RSA
RSA
2002

RSA=<*p*, *q*, *n*, *m*, *e*, *d*, *k*, *c*>
」

1 *p*, *q*, *n*, *m*, *e*, *d*, *k*, *c* *Z**, *Z**={1,2,3, }
2 *p*, *q* 各 $n = p \times q$
3 (*e*, *n*): (*d*, *n*):
4 *m*: $m < n$
5 *c*:
6 $k(m^{k(p-1)(q-1)} (\mathrm{mod}\ n)) = 1$
7 $k(\ ed = k(p-1)(q-1)+1)$
8 $c = m^e (\mathrm{mod}\ n)$
9 $m = c^d (\mathrm{mod}\ n)$

1 各 *p*, *q*
2 *e* *e* $(p-1)(q-1)$ $0<e<(p-1)(q-1)$
3 *d* $k(\ ed = k(p-1)(q-1)+1)$

3. RSA 」

1 *m* $c = m^e (\mathrm{mod}\ n)$
2 *c* $m = c^d (\mathrm{mod}\ n)$

RSA 」 (*e*, *n*) (*d*, *n*) *p* *q*

$k(m^{k(p-1)(q-1)} (\mathrm{mod}\ n)) = 1$ CS

例 *p*=3, *q*=11, $n = 3 \times 11 = 33$
m=2 $m<n$, *k*=1

$$m^{k(p-1)(q-1)} (\mathrm{mod}\ n) = 2^{1\times(3-1)\times(11-1)} (\mathrm{mod}\ 33)$$
$$= 2^{20} (\mathrm{mod}\ 33)$$
$$= 1\ 048\ 576\ (\mathrm{mod}\ 33)$$

$= 1$

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

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

$= 2^{40} \pmod{33}$

$= 1\ 099\ 511\ 627\ 776 \pmod{33}$

$= 1$

$m=2 \quad m<n \quad , k=3$

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

=2187 (mod 33)

=9

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

p, q, n

e

p=223 092 827, q=218 610 473　　(p–1) ×(q–1) = (223 092 827–1)×(218 610 473–1)

= 48 770 427 991 673 872

RSA　　e　　48 770 427 991 673 872

e=2　48 770 427 991

二、

p=11, q=13　　RSA　　9