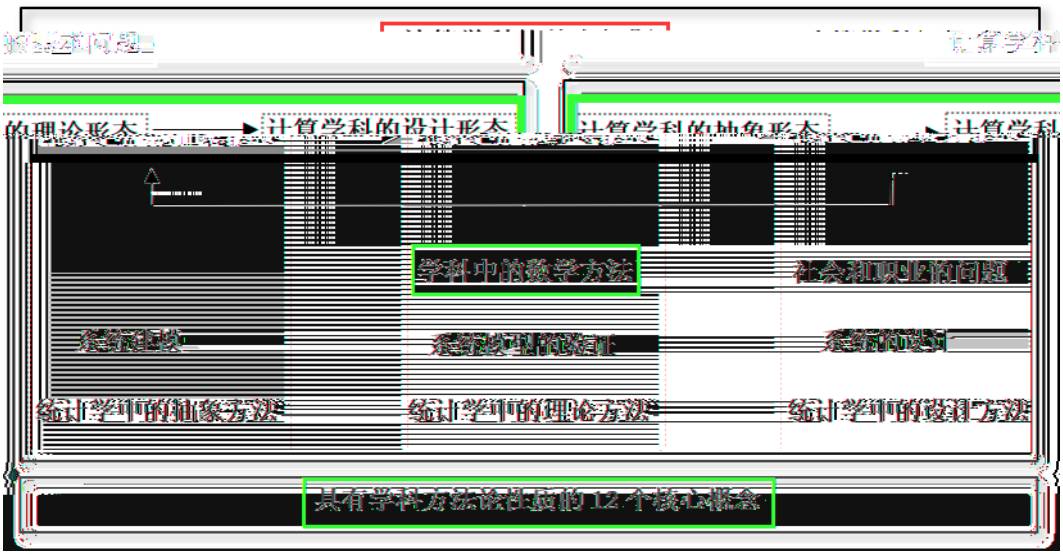
科学思维-样例：RSA 公开密钥密码系统

元认知知识 （

创造 则 （

1.



（

（ （

（ 全 （ 全 （定

（

（ 关 上

（定

（

（ （

（

（ 上

关

（

（ 全

定 保 1976 Whitfield Diffie

上 Martin Hellman Diffie Hellman key exchange（ DH
上 （ *New Directions in Cryptography*
三 保 保
上 （ 径 （
（ 全 （ 全 （
（
（ 曼 1978 R. L. Rivest A. Shamir
L. M. Adleman *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*
RSA 全 （ RSA 全 （ 数
全 RSA 全
2002

全

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* 三 （ $n = p \times q$
3 (*e*, *n*):全 (*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 $m = c^d \pmod n$

全

1 拥 三 *p*, *q*
2 *e*(*e* 上$(p-1)(q-1)$于 （ $0<e<(p-1)(q-1)$
3 *d*(*k*($ed = k(p-1)(q-1)+1$)

3. RSA 全

1 *m* （ $c = m^e \pmod n$
2 *c*($m = c^d \pmod n$

RSA 全 （ (*e*, *n*) 全 （ (*d*, *n*) （ *p* *q* （
（ 三 全
$k(m^{k(p-1)(q-1)} \pmod n) = 1$ （ CS 三 （

例 $p=3$, $q=11$, $n = 3\times11=33$
$m=2$ $m<n$, $k=1$

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

$= 1$

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

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

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

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

$= 1$

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

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

=2187 (mod 33)

=9

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

p, q, n

全

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 全　　（ e　　上 48 770 427 991 673 872 于

e=2（ 48 770 427 991 673 872 mod 2 = 0

e=3（ 48 770 427 991 673 872 mod 3 = 1

（ 3 上 48 770 427 991 673 872 于 （　　（ e=3

d

k　　ed = k(p–1) (q–1)+1（　　（　　k

d= (k(p–1) (q–1)+1)/e

e = 3（ p=223 092 827, q=218 610 473

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

k=1　（ d=48 770 427 991 673 873/3

k=2　（ d=97 540 855 983 347 745/3

=32 513 618 661 115 915

（　d　数 （　　（ d=32 513 618 661 115 915

（　RSA 全　　全　(3, 487 704 284 333 771 171)（

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

RSA 全　　（　　e, n　上　　(c)　　全　　（

p　q（　　n=p　q　　,

全　　（

全

p=11, q=13（ RSA 全 （ 9

（． 1