Camlin Page
Date / /

• Fermat's Theorem

→ if p is a prime no
→ a is positive integer not divisible by p

$$a^{p-1} \equiv 1 \bmod p \Rightarrow a^{p-1} \bmod p = 1$$

(1) $a = 7$
$p = 11$

$7^{11-1} \bmod 11$
$7^{10} \bmod 11$
$7^2 \bmod = 5$
$7^4 \bmod 11 = (7^2 \bmod 11)(7^2 \bmod 11)$
$= (5 \times 5) \bmod 11$
$= 3$

$7^8 \bmod 11 = (7^4 \bmod 11)(7^4 \bmod 11)$
$= (3 \times 3) \bmod 11$
$= 9$

$7^{10} = (7^8 \bmod 11)(7^2 \bmod 11)$
$= (9 \times 5) \bmod 11$
$= 1$

(2) $3^{12} \bmod 13$

$3^2 \bmod 13 = 9$
$3^4 \bmod 13 = 81 \bmod 13$
$= 3$

$3^8 \bmod 13 = 9$

→ $3^{12} \bmod 11$

$(3^{10} \times 3^2) \bmod 11$

$= 3^{10} \bmod 11 \times 3^2 \bmod 11$

$= (1 \times 9) \bmod 11$

$= 9$

→ $3^{202} \bmod 11$

For n time 3^{10}, ans is 1

$(\underbrace{3^{10} \times \ldots \times 3^{10}}_{20 \text{ times}} \times 3^2) \bmod 11$

$= 9$

→ $456^{17} \bmod 17$

$(456^{16} \bmod 17)(456 \bmod 17)$

1×14

$= 14$

Camlin Page
Date / /

Euler's phi function

The function finds two things
(i) No of integers smaller than n
(ii) Nos. which are relative prime to n

(1) $\phi(1) = 0$

(2) $\phi(p) = p-1$ if p is prime

(3) $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are co-prime.

(4)

P.T.O $\phi(7) = 6$

There are 6 nos. relatively prime to 7

$\phi(35) = \phi(7) \times \phi(5)$
$= 6 \times 4$
$= 24$

~~Z35~~

1 (2) (3) (4) 5 (6) 7 (8) (9) 10
(11) (12) (13) ~~(14)~~ 14 15 (16) (17) (18) (19) 20
21 (22) (23) (24) 25 (26) (27) 28 (29) 30
(31) (32) (33) (34)

$\phi(49) = \phi(7) \times \phi(7)$
$= 6 \times 6$
$= 36$

Page
Date / /

1 2 3 4 5 6 7 8 9 10

④ $\phi(p^e) = p^e - p^{e-1}$

$\phi(49) = \phi(7^2)$

$= 49 - 7$

$= 42$

Euler's theorem

① $a^{\phi(n)} \equiv 1 \bmod n$

a & n are relatively prime

② if $n = p \times q$, $a < n$ and k is an integer then

$a^{k \times \phi(n)+1} \equiv a \bmod n$

$6^{24} \bmod 35$

$20^{62} \bmod 77$ ___ non-prime ∴ Euler's

$\phi(77) = 60$

Now, $20 < 77$

$20^{k \cdot \phi(77)+1} \bmod 77$

Put $k=1$

$$(20^{\phi(77)+1} \bmod 77)(20 \bmod 77)$$

$$(20 \times 20) \bmod 77$$

$$= 15$$

$$- \quad 10^{147} \bmod 91$$

$$\phi(13) \times \phi(7)$$

$$= 72$$

~~$k=1$~~

~~$(10^{\phi(72)+1} \bmod 91)(10 \bmod 91)$~~

$$(10^{72} \times 10^{72} \times 10^{3}) \bmod 91$$

$$(1 \times 1 \times 1000) \bmod 91$$

$$= 90$$

OR

$$(10^{2 \times \phi(91)+1} \bmod 91)(10^{2} \bmod 91)$$

Now $10 < 91$

$$(10 \times 100) \bmod 91$$

$$= 90$$

Multiplicative inverse

$3^{-1} \bmod 5$

$r1 = 5$

$r2 = 3$

q	r1	r2	r	t1	t2	t
1	5	3	2	0	1	-1
1	3	2				

$5^{-1} \bmod 7$

$r1 = 7$

$r2 = 5$

q	r1	r2	r	t1	t2	t
1	7	5	2	0	1	-1
2	5	2	1	1	-1	3
2	2	1	0	-1	3	-7
	1	0		3	-7	

- **Theorem : Extended Fermat's Theorem**

→ If a and n are co-prime

→ n is prime then

$$a^{-1} = a^{n-2} \bmod n$$

eg: $3^{-1} \bmod 5 = 3^{5-2} \bmod 5$

$= 27 \bmod 5$

$= 2$

eg: $5^{-1} \bmod 7 = 5^{7-2} \bmod 7$

$= 5^5 \bmod 7$

$= (25 \times 25 \times 5) \bmod 7$

$= (4 \times 4 \times 5) \bmod 7$

$= (2 \times 5) \bmod 7$

$= 2$

- CHINESE REMAINDER

(1) Find $M = m_1 \times m_2 \times m_3 \times \ldots \times m_n$

(2) Find $M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, \ldots, M_n = \frac{M}{m_n}$

(3) Find the multiplicative inverse of $M_1, M_2, \ldots, M_n$ using corresponding $m_1, m_2, \ldots, m_n$

(4) Solution is

$$x = (a_1 \times M_1 \times M_1^{-1} + \ldots + a_n \times M_n \times M_n^{-1}) \bmod M$$

eg:
$$\begin{aligned} X &\equiv 2 \bmod 3 \\ X &\equiv 3 \bmod 5 \\ X &\equiv 2 \bmod 7 \end{aligned}$$ — moduli.

Cond^n: ~~All the~~ moduli must be co-prime for all n equations

$a_1 = 2, \ a_2 = 3, \ a_3 = 2$

(i) $M = m_1 \times m_2 \times m_3 = 105$

(ii) $M_1 = 35, \ M_2 = 21, \ M_3 = 15$

(iii) $M_1^{-1} \rightarrow Z_3$

$= 35^{-1} \bmod 3$

$= 35^{3-2} \bmod 3$

$= 2$

$M_2^{-1} \rightarrow Z_5$

$= 21^{-1} \bmod 5$

$= 21^{5-2} \bmod 5$

$= 1$

$M_3^{-1} \rightarrow Z_7$

$= 15^{-1} \bmod 7$

$= 15^{7-2} \bmod 7$

$= 1$

(iv) $x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + a_3 \times M_3 \times M_3^{-1}) \bmod M$

$= 233 \bmod 105$

$= 23$

eg: $X \equiv 3 \bmod 7$

$X \equiv 3 \bmod 13$

$X \equiv 0 \bmod 12$

(i) $7 \times 13 \times 12 = 1092$

(ii) $M1 = 156$, $M2 = 84$ Don't calculate for M3

(iii) $M_1^{-1} \longrightarrow Z_7$

$= 156^{-1} \bmod 7$

$= 156^{5} \bmod 7$

$= 2^5 \bmod 7$

$= 4$

$M_2^{-1} \longrightarrow Z_{13}$

$= 84^{-1} \bmod 13$

$= 84^{11} \bmod 13$

$= (6)^{11} \bmod 13$

$= (6^3 \bmod 13) \times (6^3 \bmod 13) \times (6^5 \bmod 13) \times 36 \bmod 13$

$= (8 \times 8 \times 8) \bmod 13 \times 10$

$= (5 \times 10) \bmod 13$

$= 11$

(iv) $(3 \times 156 \times 4 + 3 \times 84 \times 11) \bmod 1092$

$= 4644 \bmod 1092$

$= 276$

eg: $X \equiv 2 \bmod 7$
$X \equiv 3 \bmod 9$

(i) 63

(ii) $M_1 = 9 \quad M_2 = 7$

(iii) $9^{-1} \bmod 7$
$= 9^5 \bmod 7$
$= 2^5 \bmod 7$
$= 4$

$7^{-1} \bmod 9$
$= 7^7 \bmod 9$
$= 7$
$=$

(iv)

Asymmetric Key Encryption

- Knapsack Crypto System / Knapsack Algo

(i) n bit message

(ii) choose a super increasing vector

(iii) choose a number q such that
$q > \sum a$
$1 \leq i \leq n$

$a_i > \sum a_n$
$1 \leq n \leq i-1$

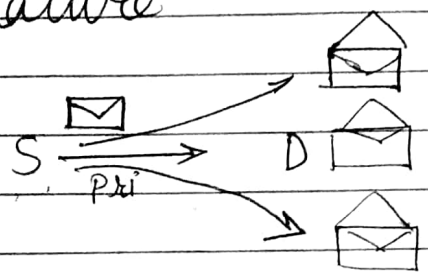
(iv) select r such that
$\gcd(q, r) = 1$
r is multiplier

(v) Compute vector
$B_i = [b_1 \; b_2 \; \ldots \; b_n]$
$b_i = a_i r \bmod q$ ← public key

(vi) Knapsack sum (x[1, 2, ..., k], b[1, 2, ..., k]){

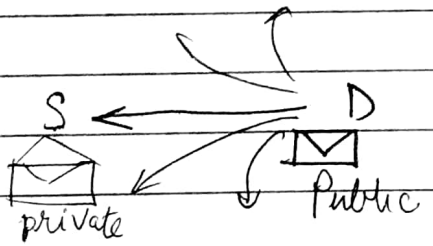
```
    s ← 0
    for (i=1 to k){
        s ← s + b_i × x_i.
    }
    Return s
}
```

Signature



opened with public key

All having public key can decrypt



Signed using public key and can be decrypted only by ~~sender's~~ private key

~~Tracing~~

~~(1) 10010.~~

eg: Super increasing tuple :

3, 5, 15, 25, 54, 110, 225

q = 439

r = 10

n = 10010000

C = 280

NOTE:

|SIT| = |n|

Another eg: ~~P = 280~~

~~B =~~ $B = \{10, 20, 40, 80, 48\}$

$q = 101$

$r = 10$

$n = 10010$

$P = 10 \times 1 + 20 \times 0 + 40 \times 0 + 80 \times 1 + 48 \times 0$

$= 10 + 80$

$= 90$

Decryption

(i) Compare r^{-1} of r in modulo of q

(ii) $C'_{P.T.} = C \cdot r^{-1} \bmod q$

(iii)
```
Inv_Knapsack (c', a[1,2,...k]){
    for (i=k to 1){
        if c >= a_i {
            x_i ← 1
            c' = c' - a_i
        }
        else {
            x_i ← 0
        }
    }
    return x[1,...,k]
}
```

Using extended Euclidian Algorithm

x: 3, 5, 15, 25, 54, 110, 225

$q = 439$

$c = 280$

$r = 10$

(i) x^{-1} in Z_{439}

q	x_1	x_2	r	t_1	t_2	t
	439	10		0	1	-43
43	10	9	9	1	-43	44
1	9	1	1	-43	44	
9	1	0	0	44		

$x^{-1} = 44$

(ii) $c' = 280 \cdot 44 \bmod 439$

$= 28$

(iii) Inv-Knapsack (28, a)

$28 \geq 225$ ✗ $x_i = 0$

$28 \geq 110$ ✗ $x_i = 0$

$28 \geq 54$ ✗ $x_i = 0$

$28 \geq 25$ ✓

$c' = 3$ $x_i = 0$

$3 \geq 15$ ✗ $x_i = 0$

$3 \geq 5$ ✗ $x_i = 0$

$3 \geq 3$ ✓ $x_i = 1$

1000000

~~10, 20, 40, 8~~

1, 2, 4, 8, 25

$q = 101$

$r = 10$

$c = 90$

(i) r^{-1} in Z_{101}

10	101	10	1	0	1	-10
10	10	1	0	1	-10	-101
	1	0		-10		

$r^{-1} = 91$

(ii) $c' = 90 \times 91 \bmod 101$

$\equiv 9$

(iii) 10010

Extended Knapsack Algorithm

You can repeat Super increasing tuple but the P.T. format must

- Inverse not available
- Bits must be in multiple of S.I.T.

eg: $a = [17, 25, 46, 94, 201, 400]$ } Σ

$pt = 101010$

$q = 787 > 783$ take prime for ease

$r = 15$

$b = 255, 375, 690, 623, 654,$

~~$17 \times 1 + 46 \times 1 + 201 \times 1$~~ $= 1599$

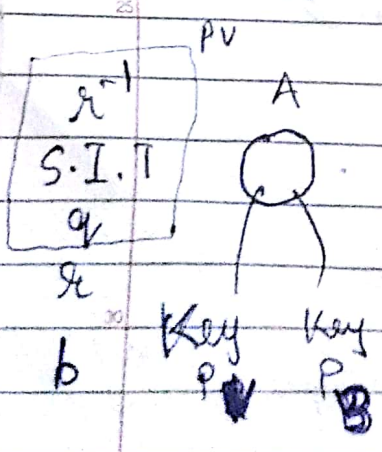
~~$c = 264$~~ $c = 255 + 690 + 3015 = 3960$

- r^{-1} in $\mathbb{Z}_{787}$

52	787	15	7	0	1	−52
2	15	7	1	1	−52	105
7	7	1	0	−52	105	
	1	0		105		

(i) $r^{-1} = 105$

(ii) ~~175~~ ~~264~~



RSA Algorithm

Key generation

{ → select two large prime p & q such that $p \neq q$

→ $n \leftarrow p \times q$

→ $\phi(n) \leftarrow (p-1)(q-1)$

→ ~~set~~ select e such that $1 < e < \phi(n)$ & e is co-prime to $\phi(n)$

→ $d \leftarrow e^{-1} \bmod \phi(n)$

→ public key $\leftarrow (e, n)$

→ private key $\leftarrow$ ~~to~~ d

Encryption

{

$CT = PT^e \bmod n$

}

Decryption

{

$PT = CT^d \bmod n$

eg: $p \rightarrow 11$

$q \rightarrow 17$

$n = 187$

$\phi(n) = 10 \times 16 = 160$

$e \leftarrow 7$

e^{-1} in $\mathbb{Z}_{160}$

160 7

:

$d = 23$

public key : (7, 187)

private key : (23)

Camlin Page
Date / /

PT = 88

$\therefore CT = 88^7 \bmod 187$

$= 88\ (77)^3 \times 88 \bmod 187$

$= (66 \times 88) \% 187$

$= 11$

CT = 11

$PT = 11^{23} \bmod 187$

$11^5 \times 11^5 \times 11^5 \times 11^5 \times 11^3 = (44)^4 \times (11)^3$

$= 55 \times 22$

$(44)^4 = 88$

$e \times d \bmod 160 = 1$

$(7 \times 23) \% 160 = 1$

161
321

eg: p = 11 PT = 88
q = 3

PRIMALITY TESTING

- Miller-Rabin (a, n)

```
{
Find m and k such that
      n-1 = m × 2^k
T ← a^m mod n   (a=2)
if (T = ±1) return "a prime"
for (i ← 1 to k-1){
      T ← T^2 mod n
      if (T = +1) return "a composite"
      if (T = -1) return "a prime"
}
return "a composite"
}
```

- ~~Working~~ Proof of RSA

$$P_1 = C^e \bmod n$$
$$= (p^d \bmod n)^e \bmod n$$
$$= p^{ed} \bmod n$$

$e \leftarrow \phi(n) + 1$

d

$ed = k\phi(n) + 1$

$$= p^{k\phi(n)+1} \bmod n$$
$$= p \quad \text{(Using extended euclidean Algo)}$$

Miller-Rabin

561 =

560 = ~~28 x 2 x 2 x 2 x 5~~

= 28 x 2 x 5 x 2

= ~~35~~ x 2^4.

m = 35

k = 4

T ← 2^{35} mod 561

= $(2^{11} \text{ mod } 561)^3 (4 \text{ mod } 561)$

= 206 x 4 mod 561

T = 263 ~~mod 561~~ mod 561

263 ≠ ±1

i = 1 ~~to~~ 3

i	
1	$T = 263^2 \text{ mod } 561 = 166$
2	$T = 166^2 \text{ mod } 561 = 67$
3	$T = 67^2 \text{ mod } 561 = 1$ ~~co~~ Thus, composite

29

~~28 x 2~~

29 k = 0 k = ~~2~~

m = ~~28~~ m = 7

2 x 2 x 7

$T \leftarrow 2^r \bmod 29$

$T \leftarrow 12 \neq \pm 1$ ✗

$i = 1 \quad 144 \bmod 29 = 28 \bmod 29$

$= -1$

61

$60 = 15 \times 4$

$m = 15$

$k = 2$

$2^{15} \bmod 61$

$= 11$

$i = 1 \quad 121 \bmod 61$

-1

133

$132 = 2^5 \times 2^2 \times 3 \times 11 =$

$= m = 33 \quad 33 \times 2^2$

$2^{33} \bmod 133$

- Fast modulation

```
c = 0; f = 1
for (i = k down to 0)
    do  c ← 2c
        f ← (f × f) mod n
    if b_i = 1
        then
            c ← c + 1
            f ← (f × a) mod n
return f
```

$a^b \bmod n$

(1) $7^{560} \bmod 561$

b =	1	0	0	0	1	1	0	0	0	0
c	1	2	4	8	17	35	70	140	280	560
f	7	49	157	526	160	241	298	166	67	1

(2) $11^{290} \bmod 402$

1 1 0 0 1 0 0

	1	0	0	1	0	0	0	1	0
c	1	2	4	9	18	36	72	145	290
f	11	121	169	209	265	277	349	347	211

Camlin Page
Date / /

~~Fro~~ To implement RSA cryptosystem which # will you take as p and q and which # will you take as. Verify using MR primality test as well as e must follow the rule of RSA cryptosystem. ~~msg~~ = 88

#: 109, 101, 127, 49, 55, 57, 439, 237