# Public Key Algorithms

## Number theory concepts:

- Hash algorithms are irreversible transformation.
- Secret key Algorithms encrypt block of data in reversible Way.

## Public Key Algorithm:

- RSA and ECC, Which do encryption and digital signature.
- Elgamal and DSS, Whic do digital signature.
- Diffie Hellman: establish a shared secret.
- Zero Knowledge proof systems, which do Authentication.

All public key algorithms have in common pair of keys one secret and one public

## Modular Arithmetic

- Most public key Algorithm based on modular arithmetic.
- It use the no. negative integer (less than +ve n) to perform ordinary arithmetic operations such as addition & multiplication.
- The result is said to be mod n.
- X mod n means the remainder of X when divided by n.

### [1] Modular Addition

When we use mod 10 Additio the result is already between 0 and 9
e.g. 5+5=0 3+9=22+2=49+9=8

# Number Theory

- Mathematical op. to understand RSA and how it works.
- Introduction to Modular Arithmetic

## Remainder:

If m>n ∴ remainder of m/n is smallest non –ve no. differ. By multible of n.

Ex.1: 10 mod 3 = 1

Ex.2: 3 mod 10 ≡13 mod 10 ≡ -7 mod 10 = 3

∴ 3, 13, -7 are equivalent

## Mod n addition:

For a mod n & b mod n

∴ a + b is the name for mod n sum.

Ex.: 3 mod 10 = 3

13 mod 10 = 3

16 mod 10 = 6

For different names of a and b ; ex.: a + K n & b +Ln

$$(a + K n) + (b + L n) = a + b + (K + L) n = a + b$$

## Mod n multiplication:

Similarly ab is a name for mod n – product.

Again $(a + K n) (b + Ln) = ab + ( aL + Kb + KL) n = ab$

(Note: Exponentiation is a repeated multiplication)

## PRIMES:

- no. is prime iff its divisible by 2 the integers (itself and 1).
  2,3,5,7,11,13,17,19,23,229,31,37,…
- There are ∞ no. of primes - prove :-
  ∴ If you have finite set of primes, multiply them, add 1

So, you can always find another prime. ∴ ∞
Primes do this as no. get bigger (25 primes less than 100)

∴ Density : 1 : 4 in first hundred integers

In 10 digit no.s density : 1 : 23

For 100 digit no.s density : 1 : 230

(Many Cryptographic Algorithms (RSA) require large primes)

Steps: chose RND no., test whether its prime or not.
Note: in RSA We need 2 primes p,q
Chance: 1 : 230
Prime must be odd.
1/e = 0.37

## Euclid's Algorithm:

Used (1) to find gcd (greatest common divisor) of 2 integers
(2) to find multiplicative inverse mod n

Multiplicative inverse: no. * x to get 1

In RSA d,e are inverses

So, we choose one, and calculate the other

Using Euclid's Alg.

→ 2 no.s are relatively prime iff gcd is 1

Ex.: gcd (8,12) = 4

gcd (12,25) = 1 → 12,25 are relatively prime

Note: gcd (x,1) = 1 & gcd (0,x) = x

## Euclid's Algorithm:

To find gcd (x,y) : replace original no.s with smaller that have

same gcd until one of no. is zero – (Repeated)

<x,y> and <x-y,y> have same common divisions

So, Replace x with its remainder when divided by y

(Note: once x is smaller than y, switch and repeat)

∴ (x,y) → (y, remainder of x/y)

Ex.: gcd (408 and 595)

595/408 =1 remainder 187

408/187 = 2 remainder 34

187/34 = 5 remainder 17

34/17 = 2 remainder 0

gcd (408,595) = 17

## Algorithm:

Initial set up:

| | $n$ | $q_n$ | $p_n$ | $u_n$ | $v_n$ |
|---|---|---|---|---|---|
| | -2 | x | 408 | 1 | 0 |
| | -1 | Y | 595 | 0 | 1 |
| Set n b → | 0 | 0 | 408 | 1 | 0 |
| | 1 | 1 | 187 | -1 | 1 |
| | 2 | 2 | 34 | 3 | -2 |
| | 3 | 5 | 17 | -16 | 11 |
| | 4 | 2 | 0 | 35 | -24 |

$R_n = u_n x + v_n y$

(1) Initial Setup: $u_2 = 1, \quad v_{-2} = 0$

$u_{-1} = 0, \quad v_{-1} = 1$

(2) At step n: $u_n = u_{n-2} - q_n u_{n-1}$ 1- 0.1 = 1

$v_n = v_{n-2} - q_n v_{n-1}$

since, $r_4 = 0$, we can read n=3

gcd(408,595) = r3 = 17 = -16 * 408 + 11 * 595

∴ gcd of 2 no.s can be expressed as sum multiple of each.

Note: any 2 no.s x,y are relatively prime iff ux + vy = 1

## Finding Multiplicative Inverses in Modular Arithmetic

How Euclid's Alg. Can find Multi. Inverse

Ex.: What is the multiplicative Inverse of m mod n

i.e. We want to find u such that : u m mod n = 1

or um = 1 mod n or um + vn = 1

### Steps:

(1) gcd (m,n)
(2) Find u,v provided gcd (m,n) = 1 (m,n Rel. prime)
Note: if m,n not Relat. Prime
∴ m doesn't have a multiplicative inver. Mod n

Could there be more than one u mod n for which um mod n =1

### Answer:

Suppose xm = 1 mod n

Multiply by u : xmu = u mod n

But um = 1 mod n

∴ x = u mod n

∴ there is one multiplicative Inv. Of m mod n

**<u>Summary:</u>** If m, n are relatively prime

We can use Euclid's Alg. To find u ( and v ) such that um + vn = 1 mod n

(u behave like 1/m or $m^{-1}$ or mod n inverse)

If m & n not relat. Prime $m^{-1}$ mod n doesn't exist.

| n | $q_n$ | $p_n$ | $u_n$ | $v_n$ |
|---|---|---|---|---|
| -2 | x | 797 | 1 | 0 |
| -1 | Y | 1047 | 0 | 1 |
| 0 | 0 | 797 | 1 | 0 |
| 1 | 1 | 251 | -1 | 1 |
| 2 | 3 | 47 | 4 | -3 |
| 3 | 5 | 15 | -21 | 16 |
| 4 | 3 | 2 | 67 | -15 |
| 5 | 7 | 1 | -490 | 373 |

∴ 1 = -490 * 197 + 373 * 1047

(A) ∴ 797-1 = -490 mod 1047
= 557 mod 1047

(B) 1047-1 = 373 mod 797
=373

## Chinese Remainder Theorem

Chinese Remainder theorem states if $Z_1, Z_2, Z_3, \ldots Z_k$ are relatively prime and you know that some no. is $x_1$ mod $Z_1$ and $x_2$ mod $Z_2$ … $x_k$ mod $Z_k$

Then you can calculate what number is mod $Z_1, Z_2, Z_3, \ldots Z_k$

Also, if something equals x mod $Z_1, Z_2, Z_3, \ldots Z_k$ , then you can calculate what the no. is mod $Z_1$ , mod $Z_2$ …

$\therefore$ It's easy to convert from one representation to the other.

(A) Standard representation x mod $Z_1, Z_2, Z_3, \ldots Z_k$ {all $Z_i$ R.P.}
(B) Decomposed representation $x_1$ mod $Z_1$ and $x_2$ mod $Z_2$ … $x_k$ mod $Z_k$

**One**: to go from standard to decomposed:

(1) Take no x
(2) Calculate what's mod $Z_i$
(3) Take the remainder as $x_1$ mod $Z_1$
Ex.: if $Z_1 = 7$ $Z_2 = 3$ and $x = 30$
$\therefore$ $\underset{x}{30}$ mod 21 = $\underset{x_1}{9}$ mod 21

**two:** to go from decomposed to standard:

(1) Assume k = 2, we know $x_1$ mod $Z_1$ and $x_2$ mod $Z_2$
And want to find out what's mod $Z_1 Z_2$
In RSA, we call $Z1, Z_2 \longrightarrow p, q$

So, we know that something equal $x_1$ mod p

and something equal $x_2$ mod q

and we want to know what's equal mod p q (call it x)

(2) Since p, q are relatively primes we can use Euclid's Algorithm to find a, b
$a\,p + b\,q = 1$ ; where $a = p^{-1}$ mod q , $b = q^{-1}$ mod p

(3) Multiply this equation by x

$x = x\,a\,p + x\,b\,q$

Since x differs from $x_1$ by multiple of p

And x differs from $x_2$ by multiple of q

Taking both sides mod p q gives:

$x = x_2\,a\,p + x_1\,b\,q \mod p\,q$

**$Z_n^*$**

$Z$ is used as the symbol for the set of all integers

$Z_n$ is the symbol for the set of integer mod n

Ex.: $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$Z_n^*$ is defined as set of mod n integers that are relatively prime to n

$Z_{10}^* = \{1, 3, 7, 9\}$ Note: Ø is missing because gcd(0, 10) = 10

**Multiplication table for $Z_{10}^*$ is**

| | 1 | 3 | 7 | 9 |
|---|---|---|---|---|
| 1 | 1 | 3 | 7 | 9 |
| 3 | 3 | 9 | 1 | 7 |
| 7 | 7 | 1 | 9 | 3 |
| 9 | 9 | 7 | 3 | 1 |

**Observation:**

(1) All answers are either 1, 3, 7 or 9
i.e. if you multiply any 2 no.s in $Z_{10}^*$

(2) each row, column contains all elements of $Z_{10}^*$ with no

Repeat

(3) it's not only for 10, but any no. (say 15)

$Z_{15}^* = \{1, 2, 3, 4, 7, 8, 11, 13, 14\}$

$um + vn = 1$ can be used for encryption & decryption

Now, look at mod 10 addition table it can be used as a scheme for encrypting digits (it maps each decimal digit to a different decimal digit in a way that is reversible).

But it is a cipher (it's actually a Caesar Cipher)

For e.g./ 4's inverse will be 6, because in mod 10 arithmetic

$4 + 6 = 0$ if a secret key were 4, then to

Encrypt we'd add 4 (mod 10)

Decrypt we'd add 6 (mod 10)

e.g./ <u>s</u> <u>a</u> <u>f</u> <u>e</u> = <u>19</u> <u>01</u> <u>06</u> <u>05</u>

to encrypt msg 9: $9 + 4 \bmod 10 = 3$ (cipher)

to decrypt cipher: $3 + 6 \bmod 10 = 10$ (data)

So, for encryption / decryption we can use (6,4), (7,3), …

called Additive inverse.

## (2) Modular Multiplication:

Multiplication by 1, 3, 7, or 9 works as a cipher, because it perform one to one substitution of the digits.

But multiplication by other no.s will not work as a cipher.

e.g./ multiplying by 5 half the no.s would encrypt to 0 and other half would encrypt to 5 i.e.: you will lost information.

Multiplicative inverse: of x (written $x^{-1}$) is the no by which you multiply

x to get 1 (in ordinary arithmetic, x's multiplicative inverse is 1/x)

only the no.s {1, 3, 7, 9} have multiplicative inverse mod 10

for e.g./ 7 is the multiplicative inverse of 3 ($7*3 \bmod 10 = 1$)

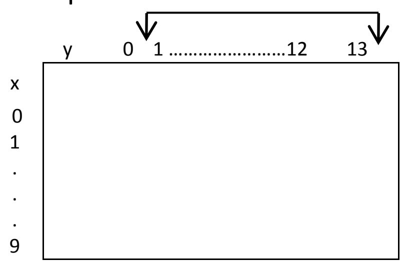
∴ encryption could be performed by multiplying by 3, and

decryption could be performed by multiplying by 7.

## (3) Modular Exponentiation :

e.g./ $4^6$ mod 10 = 4096 mod 10 = 6 mod 10

look at the exponentiation table mod 10




Extra 2 col.s because in exponentiation xy mod n not same as xy+n mod n

e.g./ 31 = 3 mod 10 but 311 = 7 mod 10

Extra 2 col.s because in exponentiation $x^y$ mod n not same as $x^{y+n}$ mod n

e.g./ $3^1$ = 3 mod 10 but $3^{11}$ = 7 mod 10

we stop at $3^{12}$ because $3^{13} = 3^1$ & $3^{14} = 3^2$ & $3^{15} = 3^3$ mod 10

Note: exponentiation by 3 would act as an encryption of the digits, because it rearranges all the digits

In case of 10, the no.s relatively prime to 10 are {1,3,7,9}

∴ Ø(n) = 4

So that the $i^{th}$ col in the above table is the same as the i + $4^{th}$ col {col ≠1 =col ≠5, col ≠2 = col≠ 6, col≠3 = col≠ 7…. So on}

∴ $x^y$ mod n = $x^{(y \bmod \emptyset(n))}$ mod n

e.g. $x^5$ mod 10 = $x^{5mod4}$ mod 10 = $x^1$ mod 10

∴ col 5 = col 1

**encryption / decryption**

Cipher

Col $^m$ = no.(cipher) → (col + Ø (n)) = message

e.g./ col 3, col 7 can be used for encryption, decryption

because 3, 7 are prime numbers & 7 = 3 + Ø (n)

where Ø (n)= no.s {1, 3, 7, 9} relatively prime to 10 → Ø (n) = 4

Note: 2,6 {2, 2+Ø (n)} can't work as crypto system because they are not prime no.s

e.g./ if m = 8 → take col 3 and compative $3^8$ = 2 (Cipher)

decryption → take col7 and compative $7^2$ = 8 (message)

also, $2^7$ = 8 (message) $8^3$ = 8 (Cipher)

Next: RSA

**Euler's Totient Function Ø (n)**

Ø (n) : n$\underline{o}$. of elements in Ø (n)

Ex.: Ø (10) = 4 since $Z_{10}^{*}$ = {1,3,7,9}

a) Given n, can we calculate Ø (n) ?
   Suppose n is prime what is Ø (n) ? easy
   $Z_n^{*}$ = {1, 2, 3, … n-1} → Ø (n) = n-1

b) What is Ø (n) when n = $p^{\alpha}$ where p is prime and $\alpha$ >Ø ?
   - only multiple of p are not relatively prime to $p^{\alpha}$
   (ex.: in p = 7 ∴ $p^{th}$ = 7, 14, 21, …) .
   - there is $p^{\alpha - 1}$ $p^{th}$ less than $p^{\alpha}$
   ∴ Ø ($p^{\alpha}$) = $p^{\alpha}$ - $p^{\alpha-1}$ = (p – 1). $p^{\alpha-1}$

c) What is Ø(n) when n = p q and p & q are relatively prime ?
   = Ø(p). Ø(q) → prove : Chinese theorem

**Euler's Theorem**

(1) For all a in $Z_n^{*}$, $a^{Ø(n)}$ = 1 mod n
(2) For all a in $Z_n^{*}$, any integer k : $a^{kØ(n) + 1}$ = a mod n
   Proof:
   $a^{kØ(n) + 1}$ = $a^{kØ(n)}$ a = $a^{Ø(n) k}$ a = $1^{k}$ . a = a
   ∴ Paging any number m to gets m back mod n,
   Only work if m in $Z_n^{*}$ (i.e. m relatively prime to n)
   In RSA, where n is a product of 2 prime n$\underline{o}$.s,
   $m^{kØ(n) + 1}$ = m mod n, even if m is not relatively prime to n
   ∴ $m^{kØ(n) + 1}$ = m mod n for all m in $Z_n$ (not just for m in $Z_n^{*}$)

9 is its own inverse. And 1 is its own inverse.

∴ encryption : multiply by x → cipher
decryption : multiply by $x^{-1}$ → get back to msg.
e.g.: m = 9 → encrypt : 9 * 7 mod 10 = 63 mod 10 = 3
decrypt : 3 * 3 mod 10 = 9 mod 10 = 9 (back to msg.)
Now, what if n was a 100 digit no. how would we able to find multiplicative inverse ? we can't use brute force search, but there is an Algorithm that will find inverse mod n. it is known as Euclid's Algorithm:
Given x, n → it finds the no. y such that x . y mod n = 1

Question1: What's special about no.s {1, 3, 7, 9} ? why they are the only ones ?

The answer that those no.s are relatively prime to n(10)

i.e. gcd = 1 (e.g./ the no. that divides both 9, 10 is 1)

In general, when you are working with n, all the no.s that are relatively prime to n will have multiplicative inverse.

Question2: How many no.s less than n are relatively prime to n ?

Ø(n) : Totient function tell (total + quotient): if n is prime, then all the integers {1, 2,…n} are relatively prime to n.

*i*.e. Ø(n) = n – 1. More over if 2 primes, say p, q then there are

(p-1)(q-1) no.s relatively prime to n

∴ Ø(n) = (p-1)(q-1) why is that ?

Well; there are n = pq total no.s in {0, 1, 2, … n-1}, and we want to exclude those no.s that aren't relatively prime to n

Those are the no.s that either multiples of p or of q.

There are p multiple of q less than pq and q multiple of p less than pq.

∴ Those are p + q – 1 no.s less than pq that aren't relatively prime to pq (we can't count Ø twice) → Ø (pq) = pq – (p + q – 1) = (p -1) (q – 1)

e.g. / p =3, q = 7 → Ø (n) = 12 → 12 no.s less than n are relatively prime to 21 = (pq)

1, 2, ~~3~~, 4, 5, ~~6~~, ~~7~~*, 8, ~~9~~, 10, 11, ~~12,~~ 13, ~~14~~*, ~~15~~, 16, 17, 18, ~~19~~, 20, ~~21~~

Note: more over if n is prime no. → Ø (n) = n – 1 (relatively prime to n)