10/10/23 UNIT: 3

MATHAMETICS OF ASYMMATRIC KEY CRYPTOGRAPHY AND ALGORITHM.

Encryption:
key in public
→ anyone can access

Message Authardic code
↓
Private key

Decryption:
→ Private key.

- prime numbers
- log
- exponentiation
- prime factor

} Mathemetical term used in Asymmatric key cryptography

Primality testing:

* Format's theorem
* Miller Robin Algorithm.

Fermat's theorem: [carmichael theorem]

$$a^{n-1} \equiv 1 \bmod n.$$

$$a^{n-1} \bmod n \equiv 1 \bmod n$$

When we take a maximum numbers between 1 & n then only the Fermat's theorem is highly accuracy.

If 'n=7'

$a = 2$.

$$2^{7-1} \bmod 7 \equiv 1 \bmod 7$$

$$2^6 \bmod 7 \equiv 1 \bmod 7$$

$$64 \bmod 7 \equiv 1 \bmod 7$$

$$1 \equiv 1$$

so, the given number is a prime number.

MILLER ROBIN ALGORITHM:

step (i) $n-1 = 2^s \times d$

s -> any value (+ve)

d -> odd number (+ve)

step (ii) $x \equiv a^d \bmod n$

a value can be between

$2 \leq a \leq n-2$.

step (iii) $x \equiv \pm 1 \bmod n$

$n = 7$. $\quad s = 1, d = 3, n = 7$

Step 1: $7 - 1 = 2^1 \times 3$

$b = 2 \times 3$

$b = b_{//}$

Step 2: $x = a^d \bmod n$ $\quad 2 \le a \le 7-2$

$a = 3$ $\quad 2 \le a \le 5$

$x = 3^3 \bmod n$

$x = 27 \bmod 7$

$x = b$

Step 3: $b \equiv \pm 1 \bmod n$

$b \equiv \pm 1 \bmod 7$

$b \equiv -1 \bmod 7$

$b = b_{//}$

11/10/23

Format's Factorization:

$n = t^2 - s^2$

$s^2 = t^2 - n$

$s = \sqrt{t^2 - n}$

$t = \sqrt{n} + 1$

$n = 809009$ $\quad \Rightarrow t = \sqrt{n} + 1$

$= 899 + 1$

$= 900.$

$S = \sqrt{810000 - 809009}$

$S = \sqrt{991}$

$S = 31.5$

not a perfect square.

$t = \sqrt{n} + 2$

$= 901$

$S = \sqrt{811801 - 809009}$

$S = \sqrt{2792}$

$S = 53.$ It is not a perfect square.

$t = \sqrt{n} + 3$

$= 902$

$S = \sqrt{813,604 - 809009}$

$S = \sqrt{4595}$

$S = 68$

$t = \sqrt{n} + 4$

$= 903$

$S = \sqrt{815409}$

$S = \sqrt{6400}$

$S = 80$

$n = 810000 - 992.25$

$n =$

$t = \sqrt{n} + 5$

$t = 904$

$S = \sqrt{817216}$

$S = \sqrt{8207}$

$S = 90.5$

$t = \sqrt{n} + 6$

$= 905$

$S = \sqrt{819025}$

$S = \sqrt{10016}$

$S = 100$

$t = \sqrt{n} + 7$

$= 906$

$S = \sqrt{820836}$

$S = \sqrt{11827}$

$S = 108.7$

13/10/2023:

Euler's theorem:

$a^{\phi(n)} \equiv 1 \bmod n$.

$n = pq$

$\phi(n) = \phi(pq) = \phi(p) * \phi(q)$

$= (p-1) \times (q-1)$

$\phi(21) = \phi(7) \times \phi(3)$

$\phi(n) = (7-1) \times (3-1)$

$= 6 \times 2$

$\phi(21) = 12.$

$\phi(12) = \phi(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11)$

~~$\phi(12)$~~ gcd $(1, 12) = 1$ ✓

gcd $(2, 12) = 2$

gcd $(3, 12) = 3$

gcd $(4, 12) = 4$

gcd $(5, 12) = 1$ ✓

gcd $(6, 12) = 6$

gcd $(7, 12) = 1$ ✓

gcd $(8, 12) = 4$

gcd $(9, 12) = 3$

gcd $(10, 12) = 2$

gcd $(11, 12) = 1$ ✓

~~gcd~~

~~$\phi(12) = 6$~~

$\phi(12) = 4$

Euler's totient function:

$\phi(n)$

$n = 4$

$\phi(n) = 3, 2, 1$

gcd (x, 4) = 1

$\phi(4) = 2$.

gcd (1, 4) = 1

gcd (2, 4) = 2

gcd (3, 4) = 1

ϕ (prime) = P - 1

$\phi(3) = 3 - 1$

$\phi(3) = 2$

$\phi(37) = 37 - 1$
$= 36$.

$\phi(5) = 4, 3, 2, 1$.

gcd (1, 5) = 1

gcd (2, 5) = 1

gcd (3, 5) = 1

gcd (4, 5) = 1

~~gcd (5, 5)~~

$\phi(55) = 5 - 1$
$= 4$.

EXPONENTIATION AND LOGARITHM:

Exponentiation $y = a^x \Rightarrow$ logarithm $x = \log_a y$

Discrete logarithm

$g^x \bmod p$

primitive root.

$2^x \bmod 7 = 4$

where, x = 2, 5, etc..

order of group

$G_1 = \langle Z_{21}^*, \times \rangle$

$\phi(21) = \phi(3) \times \phi(7)$

$\phi(p) = p-1$

$3-1=2, \quad 7-1=6$

$= \phi(2) \times \phi(6)$

$= \phi(12)$

$f(21) = \phi(12)$

$\phi(10) = \phi(2) \times \phi(5)$

$= \phi(1) \times \phi(4)$

$= \phi(4)$

$f(10) = \phi(4)$

order of elements

$G_1 = \langle Z_{10}^*, \times \rangle$

$\phi(10) = \phi(2) \times \phi(5)$

$\phi(p) = p-1$

$\phi(10) = \phi(1) \times \phi(4)$

$= \phi(4)$

$f(10) = \phi(4)$

primitive roots.

$G = \langle Z_7^*, \times \rangle$

$|G| = \phi(7) = \phi(1) \times \phi(6)$

$= 6$

$f(7) = 6$

	i=1	2	3	4	5	6
a=1	x=1	1	1	1	1	1
a=2	2	4	1	2	4	1
a=3	3	2	6	4	5	1
a=4	4	2	1	4	2	1
a=5	5	4	6	2	3	1
a=6	6	1	6	1	6	1

1) $\log_2 9 \bmod 11 \Rightarrow g^x \bmod p$

$p=11, \quad g=2, \quad x=9:$

$\log_g x \equiv n \pmod p$

$\log_2 9 \equiv g^n \pmod p$

$x \equiv g^n \pmod p$

$9 \equiv 2^n \pmod{11} \quad n=1, 2, 3, 4, \ldots$

$9 \equiv 2^6 \pmod{11}$

$9 \equiv 64 \bmod 11$

(1) $4 = 3^x \bmod 7$

$4 = 81 \bmod 7$

$4 = 4$

(2) $6 = 5^x \bmod 7$

$6 = 5^3 \bmod 7$

$6 = 125 \bmod 7$

$6 = 6$

⇒ Chinese Remainder:

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_3 \pmod{m_3}$

$x = a_1 m_1 m_1^{-1} + a_2 m_2 m_2^{-1} + a_3 m_3 m_3^{-1} \bmod M$

Eg: $x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

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

$m_1 = 3$, $m_2 = 5$, $m_3 = 7$

$M = m_1 \times m_2 \times m_3$

$= 3 \times 5 \times 7$

$\boxed{M = 105}$

$M_1 = M / m_1 = 35$

$M_2 = M / m_2 = 21$

$M_3 = M / m_3 = 15$

$M_1^{-1} \bmod m_1 = 35^{-1} \bmod 3$

$= 2.$

$M_2^{-1} \bmod m_2 = 21^{-1} \bmod 5$

$= 1$

$M_3^{-1} \bmod m_3 = 15^{-1} \bmod 7$

$= 1$

$x = (2 \times 35 \times 2) + (3 \times 21 \times 1) + (2 \times 15 \times 1) \bmod 105$

$= 140 + 63 + 30 \bmod 105$

$= 233 \bmod 105$

$\boxed{x = 23}$

Diffie-Hellman key exchange: [25/10/2023]

common key P

prime Number

Alice	Bob.
a → private key	b → private key.
$x = G^a \bmod p$	$y = G^b \bmod b$
y	key exchange take place. x
Generated secret key	
$k_a = y^a \bmod p$	$k_b = x^b \bmod p$

$k_a = k_b$.

① $P = 23$, $G = 9$, $a = 4$, $b = 3$.

$x \Rightarrow 9^4 \bmod 23$

$\Rightarrow 6561 \bmod 23$

$\Rightarrow 6$

$y \Rightarrow 9^3 \bmod 23$

$\Rightarrow 729 \bmod 23$

$\Rightarrow 16$

$k_a = y^a \bmod 23$

$\Rightarrow 16^4 \bmod 23$

$\Rightarrow 9$

$k_b = b^3 \bmod 23$

$= 9$

$k_a = k_b$

ELGAMAL CRYPTO SYSTEM:

* Bob generates public, private keys
* Choose large-q of G from Fq (cyclic group) g and a gcd (a, q) = 1
* computes $h = g^a$.

publishes F, $h = g^a$, q, g as public key

a = private key.

* Alice encryptes using Bob's public key

select k from Fq gcd (k, q) = 1

computes, $S = h^k = g^{ak}$

g^{ak} = Bob decrypt = g^{ak}.

26/10/2023.

RSA Algorithm:

p = 3, q = 11

n = pq

n = 33

$\phi(n) = (p-1)(q-1)$

$\phi(n) = (2)(10) = 20$

$e = 1 < e < \phi(n)$

↓ e = 7

public key.

Private key

↑

$d = e^{-1} \bmod \phi(n)$

$= 7^{-1} \bmod (20)$

$\boxed{d = 3}$ $7 \times 3 = 21$, $21 \bmod 20$

Encryption:

encryption = $C = m^e \bmod n$

plain text or message ← $m = c^d \bmod n$ ↳ decryption

$m = 2$

$c = 2^7 \bmod 33$

$m = 29^3 \bmod 33$