Software System Security

POOJA PREMNATH

Unit-2

Public Key Cryptography

Primes - Primality Testing - Factorization - Euler's Totient Function, Fermat's and Euler's Theorem - Chinese Remainder Theorem - Exponentiation and Logarithm - Public Key Cryptography and Message Authentication : Secure Hash Function - HMAC - RSA - Diffie-Hellman - Elliptic Curve arithmetic - elliptic key cryptography.

* Prime Numbers and Primality Testing

→ Prime numbers - has only 2 divisors, 1 and the no. itself.

→ Any integer $a > 1$, can be factored in a unique way as

$$a = p_1^{a_1} * p_2^{a_2} * \cdots p_{p_1}^{a_1}$$

where $p_1 < p_2 \cdots p_t$ are prime numbers

⇒ called the Fundamental Theorem of Arithmetic

* Fermat's Theorem

→ If p is prime and 'a' is a positive integer not divisible by p

then $$\boxed{a^{p-1} = 1 \pmod p}$$

an alternative form is: $$\boxed{aP = a \pmod p}$$

eg1 Find $2^{16} \bmod 17$

By Fermat's Theorem : $a^{p-1} = 1 \bmod p$

here $a = 2$

$p = 17$

$\Rightarrow 2^{17-1} = 1 \bmod 17$

$\therefore \boxed{2^{16} \bmod 17 = 1}$

eg2 Find $2^{50} \bmod 17$

$= ((2^{16})^3 . 2^2) \bmod 17$

$= (2^{16})^3 \bmod 17 . \ 2^2 \bmod 17$

$= 1 . 4 \bmod 17$

→ from prev Q

$= 4$

eg3 $4^{532} \bmod 11$

By Fermat's Theorem $a^{p-1} = 1 \bmod p$

11 is prime

11 does not divide 4

$\Rightarrow a^{11-1} = 1 \bmod 11$

$\Rightarrow 4^{10} = 1 \bmod 11$

$$4^{537} \bmod 11$$

$$= (4^{10})^{53} \cdot 4^{7} \bmod 11$$

$$= ((4^{10})^{53} \bmod 11) \cdot (4^{7} \bmod 11)$$

$$= 1 \cdot 16 \bmod 11$$

$$= 5$$

eg4 Find $3^{201} \bmod 11$ using Fermat's little theorem

Ans By Fermat's little theorem:

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

11 is prime

11 doesn Bot divide 3 $\quad a = 3$

$$p = 11$$

$$\Rightarrow \boxed{3^{10} = 1 \bmod 11}$$

$$3^{201} = ((3^{10})^{20} \cdot 3^{1}) \bmod 11$$

$$= ((3^{10})^{20} \bmod 11) \cdot (3^{1} \bmod 11)$$

$$= 1 \cdot 3$$

$$= 3$$

eg5 using Fermat's Theorem, find $4^{225} \bmod 13$.

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

$$a = 4$$

$$p = 13$$

$$\Rightarrow \boxed{4^{12} = 1 \bmod 13}$$

$4^{12} = 1 \bmod 13$

$4^{225} \bmod 13 = \left((4^{12})^{18} \cdot 4^9 \right) \bmod 13$

$= \left((4^{12})^{18} \bmod 13 \right) \cdot \left(4^9 \bmod 13 \right)$

$= 1 \cdot 4^9 \bmod 13$

$4^9 \bmod 13 = 12$

$\Rightarrow$

1
18
12
136
80
216

Euler's Totient Function - $\phi(n)$

→ This function, written as $\phi(n)$, is defined as the no. of positive integers less than n and relatively prime to n.

eg. $\phi(5) = 4$ $\{1, 2, 3, 4\}$ are relatively prime to 5.

Criteria	Formula.
(i) n is prime	$\phi(n) = n-1$
(ii) $n = p \times q$ p & q are prime	$\phi(n) = (p-1) \times (q-1)$
(iii) $n = a \times b$ either a or b is composite both a & b are composite	$\phi(n) = n \times \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots$ p_1, p_2 are prime numbers

eg6 Using Femat's little Theorem solve

$$\left((5555)^{2222} + (2222)^{5555} \right) \bmod 7$$

Step1 divide 5555 & 2222 by 7 to find the remainders

$5555 \bmod 7 = 4$

$2222 \bmod 7 = 3$

$\Rightarrow \left((4)^{2222} + (3)^{5555} \right) \bmod 7$

$\Rightarrow$ Use the rule : $a^n + b^n$ ⇒ is always divisible by $(a+b)^n$

$\Rightarrow \left((2^2)^{1111} + (3^5)^{1111} \right) \bmod 7$

$a^n + b^n$

$\Rightarrow \left((2^2+35)^{1111} \right) \bmod 7$

$\Rightarrow (259)^{1111} \bmod 7$

$259 \bmod 7$

$= 0$

⇒ The remainder is 0.

eg1 $\phi(3) = 4$ $(n-1)$

eg2 $\phi(31) = 30$ $(n-1)$

eg3 $\phi(35) = \phi(7) \times \phi(5)$ $\phi(n) = (p-1) \times (q-1)$

$= 6 \times 4$

$= \underline{24}$

eg4 $\phi(1000)$ $\phi(p^n) = p^n - p^{n-1}$

$n = 1000$

$1000 = 2^3 \times 5^3$

$\phi(n) = n \times \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots$

$= 1000 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$

$= 1000 \times \frac{1}{2} \times \frac{4}{5}$

$\boxed{\phi(1000) = 400}$

eg5 $\phi(7000) \Rightarrow 2^3 \times 5^3 \times 7^1$

$\phi(7000) = 7000 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)$

$= \underline{2400}$

eg6 $\phi(440)$

$440 = 2^3 \times 5 \times 11$

$\phi(440) = 440 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{11}\right)$

$= \overset{80}{\cancel{440}} \times \frac{1}{\cancel{2}} \times \frac{4}{\cancel{5}} \times \frac{\cancel{10}}{\cancel{11}} = \underline{160}$

Euler's Theorem

→ Euler's Theorem states that for every a and n that are relatively prime :

$$a^{\phi(n)} = 1 \pmod{n}$$

(or)

$$a^{\phi(n)+1} = a \pmod{n}$$

or $a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$

eg1 Prove that Euler's theorem holds true for $a=3$ and $n=10$

Ans By Euler's Theorem :

$$3^{\phi(10)} \equiv 1 \bmod 10$$

$$\phi(10) = \phi(2) \times \phi(5)$$
$$= 4$$

$$3^4 = 81 \equiv 1 \bmod 10$$

∴ holds true.

eg2 Solve using Euler's Theorem : $4^{99} \bmod 35$

$a = 4$

$n = 35$

$$\Rightarrow \quad a^{\phi(n)} = 1 \pmod{n}$$

$$4^{\phi(35)} = 1 \bmod 35$$

$$4^{24} = 1 \bmod 35$$

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

* Multiplicative Inverse using Euler's Theorem

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

(1) $8^{-1} \bmod 17$

$= a^{\phi(17)-1} \bmod 17$

$= 8^{15} \bmod 17$

Using Fast Exponentiation

$8^2 \bmod 17 = 13 \bmod 17$

$8^4 \bmod 17 = (8^2)^2 \bmod 17$

$= 13^2 \bmod 17$

$= 169 \bmod 17$

$= 16 \bmod 17$

$8^8 \bmod 17 = (8^4)^2 \bmod 17$

$= 16^2 \bmod 17$

$= +1 \bmod 17$

$8^{15} = 8^8 \cdot 8^4 \cdot 8^2 \cdot 8^1$

$= 1 \times 16 \times 13 \times 8$

$= 1664 \bmod 17$

$= 15$

1664

$\Rightarrow$ $8^{-1} \bmod 17 \equiv 15 \bmod 17$

(2) $5^{-1} \bmod 23$

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

$$5^{-1} \bmod 13 = 5^{21} \bmod 23$$

$$5^{21} \bmod 23$$

$$5^2 \equiv 2 \bmod 23$$

$$5^4 \equiv (5^2)^2 \equiv (2)^2 \equiv 8^4 \bmod 23$$

$$5^8 \bmod 23 = (5^4)^2 \bmod 23$$

$$= 18 \bmod 23$$

$$= 18$$

$$5^{21} = 5^{16} \cdot 5^4 \cdot 5^1$$

$$= (5^8)^2 \cdot 5^4 \cdot 5^1$$

$$= 18^2 \cdot 3 \cdot 5$$

$$= 5120$$

$$5120 \bmod 23 = 14$$

$$\therefore \boxed{5^{21} \bmod 23 \equiv 14 \bmod 23}$$

4) 23 (5
20
3

③ $60^{-1} \bmod 101$

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

$= 60^{100-1} \bmod 101$

$= 60^{99} \bmod 101$

Using fast exponentiation

$60^2 \bmod 101 = 3600 \bmod 101$

$= 65$

41.83

$60^4 \bmod 101 = (60^2)^2 \bmod 101$

$= 65^2 \bmod 101$

$= 84$

$60^8 \bmod 101 = (60^4)^2 \bmod 101$

$= (84)^2 \bmod 101$

$= 87$

$60^{99} = (60^8)^{12} \cdot 60^2 \cdot 60$

$= (87)^{12} \cdot 65 \cdot 60$

⋮

32 mod 101.

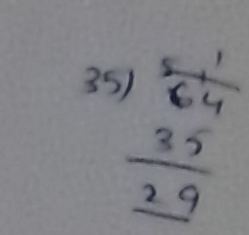
$4^{99} \bmod 35$

$= (4^{24})^4 \cdot 4^3 \bmod 35$

$= ((4^{24})^4 \bmod 35) \cdot (4^3 \bmod 35)$

$= 1 \cdot 4^3 \bmod 35$

$= \underline{\underline{29}}$



eg3 Find $3^{302} \bmod 13$ using Euler's Theorem.

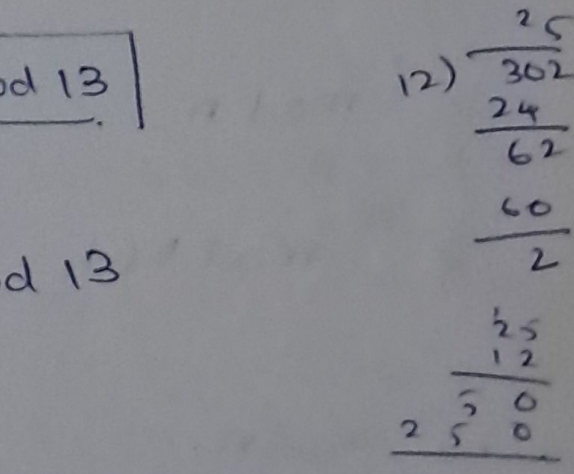
$a = 3$

$n = 13$

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

$a^{\phi(13)} = 1 \bmod 13$

$a^{12} = 1 \bmod 13$ i.e $\boxed{3^{12} = 1 \bmod 13}$



$3^{302} \bmod 13 = ((3^{12})^{25} \cdot 3^2) \bmod 13$

$= 3^2 \bmod 13$

$= \underline{\underline{9}}$

Another algo for primality checking is the Deterministic Primality Algorithm developed by Agrawal, Kayal & Saxena (AKS)

* Primality Testing - Miller Rabin Algorithm

Algorithm

1. Find integers k, q with $k > 0$ and q odd, such that:

$\boxed{n-1 = 2^k q}$

2. Select a random integer a, such that $1 < a < n-1$

3. If $a^q \bmod n = 1$ ⇒ inconclusive.

4. For $j = 0$ to $k-1$ do

   if $a^{2^j q} \bmod n = n-1$ ⇒ inconclusive

   else return composite.

Practically,

$b_0 = a^q \bmod n$

$b_1 = b_0^2 \bmod n$

1 ⇒ comp

-1 ⇒ maybe prime

else: inconclusive

Example Is 561 prime?

$n = 561$

$560 = n-1$

$560 = 2^k \cdot m$ ⇒ $566 = 2^4 \times 35$

$k = 4$

$q = 35$

choose a : let $a = 2$

$b_0 = a^q \bmod n$

$= 2^{35} \bmod 561 = 263$ ⇒ ~~composite~~ inconclusive

see if ±1

1 ⇒ comp

-1 ⇒ may be prime

$b_1 = b_0^2 \bmod n$

$= 263^2 \bmod 561$ ⇒ 166 ⇒ ~~composite~~ inconclusive

$b_2 = b_1^2 \bmod n$

$= 166^2 \bmod 561 = 67$ ⇒ inconclusive

$b_3 = b_2^2 \bmod n = 67^2 \bmod 561 = 1$ ⇒ composite

Distribution of Primes : Primes near n are spaced on the average one every ln(n) integers.

Miller Rabin worked out Examples

(1) Is 561 prime or not when $a = 2$

1. $n-1 = 2^k \cdot q$
2. $a = 2$
3. is $a^q \bmod n = 1 \Rightarrow$ inconclusive
4. for $j = 0$ to $k-1$

   find if $2^{2^j q} \bmod n = n-1 \Rightarrow$ inconclusive
5. return composite

Ans $n = 561$

1. $n-1 = 560 = 2^4 \cdot \underline{35}$

$k = 4$
$q = 35$

2. $a = 2$

3. $a^q \bmod n = 2^{35} \bmod 561$

$2^{560} \equiv 1 \bmod 561$

$= 263$

$= 2^{35} \bmod 561$

$= ((2^{16})^2 \cdot 2^2 \cdot 21) \bmod 561$

$= ((512)^2 \cdot 4 \cdot 1) \bmod 561$

$\Rightarrow$ inconclusive

$2^2 \bmod 561 = 4 \bmod 561$
$= \underline{4}$

$2^4 \bmod 561 = (4)^2 \bmod 561$
$= 16 \bmod 561$
$= \underline{16}$

$2^8 \bmod 561 = 256 \bmod 561$
$= \underline{256}$

$2^{16} \bmod 561 = 512$

4. ● $j = 0$ 8 to $k = 3$ $q = 35$

find $2^{2^0 \cdot 35} \bmod 561$

$2^{2 \cdot 35} \bmod 561$

$2^{4 \cdot 35} \bmod 561$

$2^{8 \cdot 35} \bmod 561$

1048576

(2) Is 29 prime or not? Let $a = 10$

1. $n-1 = 28 = 2^2 \cdot 7$

$u = 2$
$q = 7$

2. Let $a = 10$

3. Find $a^q \bmod n$

$= 10^7 \bmod 29$

~~q div = di~~

dividend ÷ div = q

q × (+1) = div

29x + y = 2^7

$= (10^4 \cdot 10^2 \cdot 10) \bmod 29$

$= (24 \cdot 13 \cdot 10) \bmod 29$

$= 17$

$\neq 1 \Rightarrow$ inconclusive

$10^2 \bmod 29 = 100 \bmod 29$

$= 13$

$10^4 \bmod 29 = (10^2)^2 \bmod 29$

$= (13)^2 \bmod 29$

$= 169 \bmod 29$

$= 24$

4. for $j = 0$ to $k-1$

keep $j = 0, 1$

when $j = 0 \Rightarrow$ $a^{2^j q} \bmod n = a^q \bmod n$

$= 10^7 \bmod 29$

$= 17$

$a^{2^1 \cdot 7} \bmod n = (10^{14}) \bmod 29$

$= (10^7)^2 \bmod 29$

$= (17)^2 \bmod 29$

$= 28$ may be prime or not

Take another value: $a = 12$

$12^7 \bmod 29 = 17$

$12^{14} \bmod 29 = (17)^2 \bmod 29 = 28$ //

Q1 Use Fermat's Theorem to find a no. between 0 and 72 congruent to 9794 modulo 73

Ans $a^{p-1} = 1 \bmod p$

9794 modulo 73 $\equiv$ $9794^{73-1} = 1 \bmod 73$

$= 9794^{72} = 1 \bmod 73$

Q2 Use Fermat's theorem to find x such that $x^{73} = 4 \bmod 37$.

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

remember - always forget the POW on

$p = 37$

$a = x$

$x^{36} = 1 \bmod 37$

$x^{73} \bmod 37 = ((x^{36})^2 \cdot x) \bmod 37$

$= x \bmod 37$

$x^{73} \equiv x \bmod 37$

$x = 4$

* Chinese Remainder Theorem

→ The CRT is used to solve a set of congruent equations with one variable but different moduli which are relatively prime.

Soln: $(a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} \ldots a_n M_n M_n^{-1}) \bmod M$

Example 1 solve the following equations using CRT

$$X \equiv 2 \pmod 3$$

$$X \equiv 3 \pmod 5$$

$$X \equiv 2 \pmod 7$$

Ans Soln:

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

$a_1 = 2$ $\quad m_1 = 3$

$a_2 = 3$ $\quad m_2 = 5$

$a_3 = 2$ $\quad m_3 = 7$

To find: $M_1, M_1^{-1}, M_2, M_2^{-1}, M_3, M_3^{-1}, M$

$$\boxed{M = m_1 \times m_2 \times m_3}$$

$M = 3 \times 5 \times 7 = 105$ $\quad \boxed{M = 105}$

$$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$$

$$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$$

$$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$$

$M_1 = 35$

$M_2 = 21$

$M_3 = 15$

$M_1 \times M_1^{-1} = 1 \bmod m_1$

$M_2 \times M_2^{-1} = 1 \bmod m_2$

$M_3 \times M_3^{-1} = 1 \bmod m_3$

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

$\boxed{M_1^{-1} = 2}$

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

$\boxed{M_2^{-1} = 1}$

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

$\boxed{M_3^{-1} = 1}$

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

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

$$= 233 \bmod 105$$

$\boxed{X = 23}$

Example

$x \equiv 1 \bmod 2$

$x \equiv 1 \bmod 3$

$x \equiv 1 \bmod 4$

$x \equiv 1 \bmod 5$

$x \equiv 0 \bmod 7$

Ans $x \equiv 1 \bmod 4$

$\equiv 1 \bmod (2 \times 2)$

$x \equiv 1 \bmod 2.$

III eq $x \equiv 1 \bmod 6$

$\equiv 1 \bmod (2 \times 3)$

$x \equiv 1 \bmod 2$

$x \equiv 1 \bmod 3$

∴ The required equations are: $x \equiv 1 \bmod 3$

$x \equiv 1 \bmod 4$

$x \equiv 1 \bmod 5$

$x \equiv 1 \bmod 7$

$a_1 = 1 \quad a_2 = 1 \quad a_3 = 1 \quad a_4 = 1$

$m_1 = 3 \quad m_2 = 4 \quad m_3 = 5 \quad m_4 = 7$

$M = m_1 \times m_2 \times m_3 \times m_4$

$\boxed{M = 420}$

$M_1 = \frac{M}{m_1} = \frac{420}{3} = 140$

$M_2 = \frac{M}{m_2} = \frac{420}{4} = 105$

$M_3 = \frac{M}{m_3} = \frac{420}{5} = 84$

$M_4 = \frac{M}{m_4} = \frac{420}{7} = 60$

$M_1 \times M_1^{-1} = 1 \bmod m_1$

$140 \times M_1^{-1} = 1 \bmod 3$

$\boxed{M_1^{-1} = 2}$

$M_2 \times M_2^{-1} = 1 \bmod m_2$

$105 \times M_2^{-1} = 1 \bmod 4$

$\boxed{M_2^{-1} = 1}$

$$M_3 \times M_3^{-1} = 1 \bmod m_3$$

$$84 \times M_3^{-1} = 1 \bmod 5$$

$$\boxed{M_3^{-1} = 4}$$

$$M_4 \times M_4^{-1} = 1 \bmod m_4$$

$$60 \times M_4^{-1} = 1 \bmod 7$$

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} + a_4 M_4 M_4^{-1}) \bmod M$$

$$= ((1)(140)(2) + (1)(105)(1) + (1)(84)(4)) \bmod 420$$

$$= 721 \bmod 420$$

$$= \underline{\underline{301}}$$

Additional problem

$x \equiv 2 \bmod 5$

$x \equiv 3 \bmod 7$

$x \equiv 10 \bmod 11$

* Discrete Logarithms

→ expressions of the form $q^x \bmod p$

For small values of p, it may be easy to find k.

If p is large, the time and effort to find X is very hard.

→ The strength of a one-way function depends on how much time it takes to break it.

Formally, DLP is the problem of determining $1 \leq x \leq p-1$, such that

$$\boxed{\alpha^x \equiv \beta \bmod p}$$

eg1 solve $\log_2 9 \bmod 11$

$$q^x \bmod p \equiv \boxed{\log_q q^x \equiv n \pmod p}$$

here $p = 11$, $g = 2$, $x = 9$

$$\Rightarrow X = g^n \pmod p$$

$$\Rightarrow q = 2^n \bmod 11$$

$$\boxed{n = 6}$$

eg2 Find x in $2^x \pmod 7 = 4$

$$X = g^n \bmod p$$

$p = 7$, $n = x$, $g = 2$

$X = 4$

$$4 = 2^x \bmod 7$$

$$\boxed{X = 2}$$

eg3 What is the discrete logarithm to the base 10 mod 19

for $a = 7$

Ans To find: $\log_{10} 7 \mod 19$

$g = 10$

$x = 7$

$n = ?$

$p = 19$

$$x = g^n \pmod p$$

$$7 = 10^n \mod 19$$

Ans = 12

* Elgamal Encryption System - closely related to Diffie-Hellman

Global Public Elements

$q \rightarrow$ prime no

$\alpha \rightarrow \alpha < q$ and is a primitive root of q

Key Generation

Select private X_A

calculate Y_A : $Y_A = \alpha^{X_A} \bmod q$

Encryption

plaintext = M

select random integer k , $k < q$

Calculate key $K = (Y_A)^k \bmod q$

$C_1 = \alpha^k \bmod q$

$C_2 = KM \bmod q$

cipher text $= (C_1, C_2)$

Decryption

calculate K : $(a)^{X_A} \bmod q$

Plaintext $M = (C_2 K^{-1}) \bmod q$

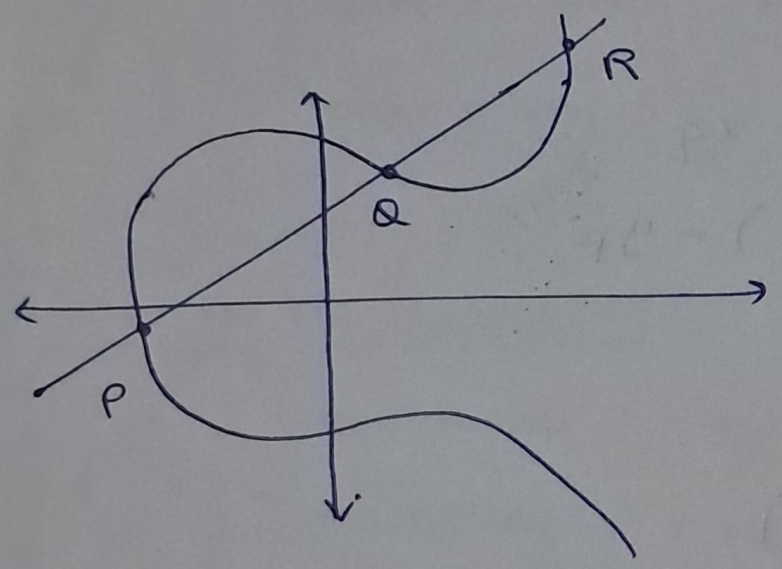
* Elliptic Curve Arithmetic and Elliptic Curve Cryptography

Elliptic Curve Arithmetic

→ An elliptic curve is represented as $E_p(a,b)$, where p is a prime number and a, b are restricted to mod p.

→ The curve is of the form $\boxed{y^2 = x^3 + ax + b}$

→ Elliptic curves are not ellipses but the equations of ECC are described by the calculation of the circumference of the ellipse.



$y = \sqrt{x^3 + ax + b}$ $\quad y = \pm x$

each curve is symmetric about the x-axis ($y = 0$)

O point - called the point at infinity or zero point in which $P + (-P)$ becomes infinity.

Elliptic Curves in Cryptography

Two families of elliptic curves are used:

(i) prime curves over Z_p

(ii) binary curves over $GF(2^m)$

Mathematical Operations

① Addition

To add points: $P(x_p, y_p)$ and $Q(x_q, y_Q)$ to get

$R(x_r, y_r)$

Steps: (i) Find the slope $\lambda = \dfrac{y_q - y_p}{x_q - x_p}$ $\quad P \neq Q$

$\lambda = \dfrac{3x_p^2 + a}{2y_p}$ $\quad P = Q$

a is from $Ep(a, b)$

(ii) Find the sum : $P+Q$ as

$$x_r = \lambda^2 - x_p - x_q$$

$$y_r = \lambda(x_p - x_r) - y_p$$

Negation : if $Q = (x_q, y_q)$

then $-Q = -(x_q, y_q)$

$= (x_q, -y_q)$

Subtraction : $P - Q = (x_p, y_p) - (x_q, y_q)$

$= (x_p, y_p) + (x_p, -y_q \bmod p)$

Multiplication : only scalar multiplication is possible.

Division : only scalar division is possible

*ECC Algorithm → min key size 160, max used = 512

ECC Key Exchange

Global Public Elements -

(i) $E_p(a,b)$ - elliptic curve with parameters a, b & p

(prime no. or an integer of the form 2^m)

(ii) G - point on the elliptic curve

User A Key Generation

private key : n_A $\quad n_A < n$

public key : P_A $\quad P_A = n_A \times G$

User B Key Generation

private key : n_B $\quad n_B < n$

public key : P_B $\quad P_B = n_B \times G$

Secret key for user A

$$k = n_A \times P_B$$

Secret key for user B

$$k = n_B \times P_A$$

ECC Encryption

→ Let the message be M

→ First encode this message M into a point on the elliptic curve.

Let this point be P_m.

→ For encryption, choose a random positive integer k.

The cipher point will be:

$$C_m = \{ kG,\ P_m + kP_B \}$$

P_B → public key of B

P_m → plaintext on curve

→ C_m is sent to the receiver.

ECC Decryption

→ Multiply x coordinate by secret key

$$= kG \times n_B$$

→ subtract this product $(kG \times n_B)$ from the y coordinate of the cipher point.

i.e $P_m + kP_B - (kG \times n_B)$

$P_m + k(n_B \times G) - (kG \times n_B)$

$P_m + kn_B G - kGn_B$

$= P_m$ ⇒ receiver gets the same point

* Message Authentication

→ Message authentication / integrity is a procedure that allows competing parties to verify that their received messages are authentic

→ Message integrity means that a message has not been tampered with or altered

* Message Authentication without Message Encryption

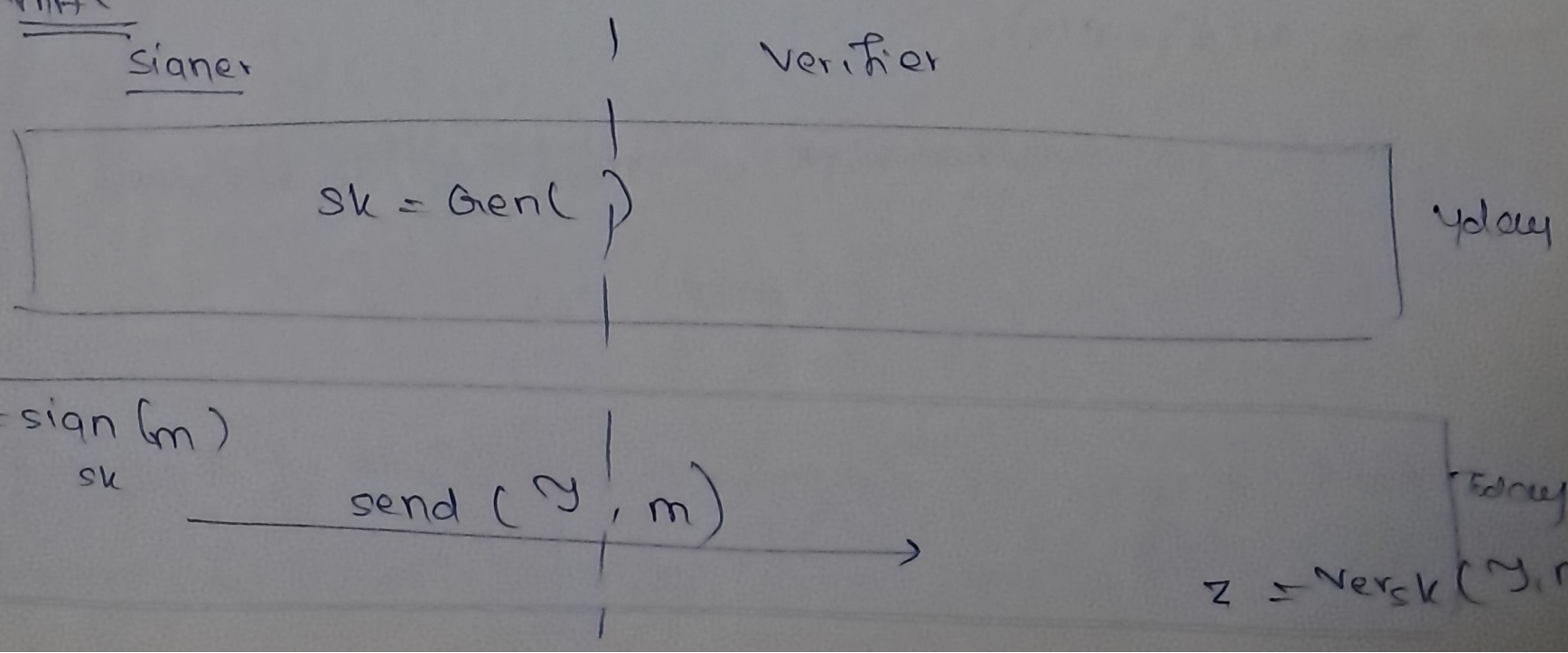
→ Message authentication does not rely on encryption

→ An authentication tag is generated and appended to each msg. for transmissions.

→ It is possible to just send the msg w/o encryption and read it at the destination

→ It is also possible to combination authentication & confidentiality in a single algorithm by encrypting a msg + its auth tag.

* MAC



* Secure Hash Function

→ important for not only message authentication but also digital signatures.

→ Such hash fns. should have the following properties

1. H can be applied to a block of data of any size
2. H produces a fixed-length output
3. H(x) is easy to compute for any x.
4. For any given code h, it is computationall ~~to~~ infeasible to find x such that H(x) = h.

called one-way / pre-image resistant

5. For an given block x, it is computationally infeasible to find $y \neq x$ with (H(x) = Hy)

called second pre-image resistant or weak collision resistant

6. It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).

called collision resistant or strong collision resistant

* HMAC → mandatory to implement mnc for IP Security

Let

b = no. of bits in a block

k = secret key

$k+$ = k with zeroes padded to the left so that the result is b bits in length

ipad = 00110110 (36 in hexadecimal)

opad = 5C in hex

Steps

1. Append zeros to the left of k to create a b-bit string $k+$

2. XOR $k+$ with i-pad to produce S_i

3. Append M with S_i

4. Apply H to the stream generated in Step 3

5. XOR $k+$ with opad to produce S_o

6. Append S_o w/ result from 4

7. Apply H to the stream generated in step 6 and output the result

* RSA Algorithm

1. Select 2 large primes p and q
2. compute $n = p \times q$
3. Compute Euler Totient Function: $\phi(n) = (p-1) \times (q-1)$
4. Select an integer e such that $\gcd(e, \phi(n)) = 1$
5. Private key calculate d: $de \bmod \phi(n) = 1$
6. Public Key $= (e, n)$

   Private Key $= (d, n)$
7. Encryption $= c = m^e \bmod n$

   Decryption $= m = c^d \bmod n$

Example)

1. Show key generation when $p = 17$, $q = 11$, $e = 7$

$n = 187$

$\phi(n) = 160$

d: $de \bmod \phi(n) = 1$

$d(7) \bmod (160) = 1$

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

$7^{-1} \bmod 160$

$7^{-1} \bmod 160$

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

$7^{63} \bmod 160$

$7^{63} = (7^8)^7 \cdot 7^4 \cdot 7^2 \cdot 7$

$7^2 \bmod 160 = 49$

$7^4 \bmod 160 = (49)^2 \bmod 160 = 1$

$7^8 \bmod 160 = 1 \bmod 160 = 1$

$7^{63} \bmod 160 = (1)^7 \cdot 1 \cdot 49 \cdot 7 \bmod 160$

$d = \underline{23}$

$\phi(160)$

$= 160 \times \frac{4}{5} \times \frac{1}{2}$

$= \underline{64}$

$2 \mid 160$
$2 \mid 80$
$2 \mid 40$
$2 \mid 20$
$2 \mid 10$
5

5×2^5

$80 \times \frac{4}{5} = 64$

public = {7, 187}
private = {23, 187}

Example 2

Find the private and public key when $p = 13$, $q = 23$, $e = 5$

$n = p \times q = 299$

$\phi(n) = 298$

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

$= 5^{-1} \bmod 298$

* Diffie-Hellman Algorithm

→ used to generate a private shared key in symmetric algorithms, not meant as an encryption algorithm

→ works on the effectiveness of computing discrete logarithms

→ asymmetric encryption is used to calculate a key at the sender and receiver side.

Steps

1. Assume a prime number q.

2. Select α such that

$\alpha \Rightarrow$ primitive root of q (if a is a primitive root of p then $\{a^1 \bmod p, a^2 \bmod p \dots a^{p-1} \bmod p\}$ result in $\{1, 2, 3 \dots p-1\}$)

$\alpha < q$

3. Assume $X_A \Rightarrow$ private key of user A

$X_A < q$

4. Calculate $Y_A \Rightarrow$ public key of user A

$$Y_A = \alpha^{X_A} \bmod q$$

5. Assume $X_B \Rightarrow$ private key of user B

$X_B < q$

6. Calculate $Y_B \Rightarrow$ public key of user B

$$Y_B = \alpha^{X_B} \bmod q$$

Key Generation

user A

$$K = (Y_B)^{X_A} \bmod q$$

user B

$$K = (Y_A)^{X_B} \bmod q$$

Man-in the-middle Attack on Diffie Hellman

Consider Darth to be an adversary

1. Darth generates 2 random private keys X_{D1} and X_{D2} and computes the corresponding public keys.

2. Alice transmits Y_A to Bob

3. Darth intercepts Y_A and transmits Y_{D1} to Bob. Darth calculates $K = (Y_A)^{X_{D2}} \bmod q$

4. Bob receives Y_{D1} and calculates $r_1 = (Y_{D1})^{X_B} \bmod q$

5. Bob transmits Y_B to Alice

6. Darth intercepts Y_B and transmits Y_{D2} to Alice. Darth calculates it as $r_1 = (Y_B)^{X_{D1}} \bmod q$

7. Alice receives Y_{D2} and computes $r_2 = (Y_{D2})^{X_A} \bmod q$

At this point

Bob, Darth $= K_1$

Alice, Darth $= r_2$

→ Diffie Hellman Example

(1) $q = 11$ $\quad x_A = 3$

$\alpha = 7$ $\quad x_B = 5$

private key of A = $x_A = 3$

public key of A = $\alpha^{x_A} \bmod q$

$= 7^3 \bmod 11$

$y_A = 2$

$11 \overline{)343}$ (31) 33, 13, 11, 2

private key of B = $x_B = 5$

public key of B = $\alpha^{x_B} \bmod q$

$= 7^5 \bmod 11$

$y_B = 10$

exchange public keys

Key Generation

A

$K = (y_B)^{x_A} \bmod q$

$2^3 \bmod 11$

$10^3 \bmod 11$

$= 10$

B

$(y_A)^{x_B} \bmod q$

$10^5 \bmod 11$

$2^5 \bmod 11$

$= 10$

(2) Find the key when $q = 23$

$\alpha = 5$

$X_A = 3$

$X_B = 7$

$X_A = 3$

$X_B = 7$

$Y_A = \alpha^{X_A} \bmod q$

$= 5^3 \bmod 23$

$= 125 \bmod 23$

$= 10$

$Y_A = \alpha^{X_A} \bmod q$

$= 5^3 \bmod q$

$= 5^3 \bmod 23$

$= 10$

$Y_B = \alpha^{X_B} \bmod q$

$= 5^7 \bmod 23$

$= 17$

Key generation

A

$K = (Y_B)^{X_A} \bmod q$

$= (17)^3 \bmod 23$

$= 14$

B

$(Y_A)^{X_B} \bmod q$

$(10)^7 \bmod 23$

$= 14$