UNIT-3
Asymmetric Ciphers

Number Theory:

Prime Number: A prime number is a number (>1) which is divisible by 1 and itself. For e.g, 2, 3, 5, 7...

Primality Testing: A primality testing is an algorithm to test whether a given number is prime or not.

Miller-Rabin Primality Testing: [Imp]

It is used to test primality of large numbers. To test whether a given number 'n' is prime or not, Miller-Rabin algorithm works as follows:

1. Write $n-1 = 2^k m$, where m is odd.
2. Choose a random number a; $1 \le a \le n-1$.
3. Compute $b = a^m \bmod n$.
4. If $b \equiv 1 \pmod n$ then return Prime.
5. For $i=0$ to $k-1$
   do if $b \equiv -1 \pmod n$ then return Prime.
   else $b = b^2 \bmod n$.
6. Return Composite.

Q. Determine whether the integer 17 is prime or not using Miller-Rabin algorithm.

Soln:
$n = 17$

$n-1 = 16 = 2^4 * 1$

$k=4$ & $m=1$

$a \rightarrow (1-16)$; $a=5$ ← randomly taken any number between 1 and 16

$b = a^m \bmod n = 5^1 \bmod 17 = 5$

$b \equiv 1 \pmod n \Rightarrow 5 \equiv 1 \pmod{17}$ which is false.

If it's true here then declare it as prime and end.

So, $i=0$ to $k-1$ (i.e, 0 to 3)

$i=0$

$b=5$

$\boxed{b \equiv -1 \pmod n \Rightarrow (b+1) \bmod n = 0}$

$5+1=6 \bmod 17 = 6$

$b = b^2 \bmod n = 25 \bmod 17 = 8$

$i=1$

$b=8$ $\quad 8+1=9 \bmod 17 = 9$

$b = b^2 \bmod n = 64 \bmod 17 = 13$

$i=2$

$b=13$ $\quad 13+1=14 \bmod 17 = 14$

$b = 13^2 \bmod 17 = 169 \bmod 17 = 16$

$i=3$

$b=16$ $\quad 16+1=17 \bmod 17 = 0$

$\therefore$ 17 is prime.

⊛. Fermat's Theorem: [Imp].

Fermats theorem states that: if p is prime and a is a positive integer not divisible by p, then $a^{p-1} \equiv 1 \pmod p$.

E.g. $a=3, p=5$ then $3^4 \equiv 1 \pmod 5$.

Alternatively, $a^p \equiv a \pmod p$

E.g. $a=3, p=5$ then $3^5 \equiv 3 \pmod 5$.

Note: The first form of theorem requires that 'a' be relatively prime to p, but second form does not.

⊛. Euler's Totient Function: [Imp].

It is defined as the number of positive integer less than n, which are relatively prime to n. It is denoted by $\phi(n)$.

E.g. $\phi(10) = ?$

Here, $n = 10$

Numbers less than 10 are: $\{1,2,3,4,5,6,7,8,9\}$

Now, Numbers relatively prime to 10 are: $\{1,3,7,9\}$

If GCD of any two numbers is 1, then they are relatively prime. Here (10,1), (10,3), (10,7) & (10,9) are relatively prime.

$\therefore \phi(10) = 4$

Note: If n is the prime number then, $\phi(n) = n-1$.

E.g. $\phi(7) = 7-1 = 6$.

Let p and q are two prime numbers such that $p \neq q$ and $n = pq$, then $\phi(n) = (p-1)(q-1)$.

E.g. $\phi(15) = ?$

Here, $15 = 3 \times 5$

$$\phi(15) = (3-1)(5-1) = 2 * 4 = 8$$

co-prime integers means integers having only one common factor. For e.g. $10 = 2 \times 5 \times 1$, $3 = 3 \times 1$

⊗. Euler's Theorem: [Imp]

Euler's theorem states that if 'a' and 'n' are co-prime integers then, $a^{\phi(n)} \equiv 1 \pmod{n}$.

Alternatively, $a^{\phi(n)+1} \equiv a \pmod{n}$

where, $\phi(n)$ is Euler's totient function.

E.g. $a=3, n=10, \phi(10)=4$ then,

$$3^4 \equiv 1 \pmod{10} \text{ or } 3^5 \equiv 3 \pmod{10}.$$

⊗. Primitive root: [Imp]

Integer 'a' is said to be a primitive root of prime number 'p' if $a^1 \bmod p, a^2 \bmod p, \ldots\ldots, a^{p-1} \bmod p$ are distinct and consists of integers from 1 to p-1 in some permutation.

E.g. Is 2 a primitive root of 5?

Soln:

Here, $a=2$ and $p=5$

$2^1 \bmod 5 = 2$

$2^2 \bmod 5 = 4$

$2^3 \bmod 5 = 3$

$2^4 \bmod 5 = 1$

Here, all the values are distinct.

$\therefore$ 2 is primitive root of 5.

Discrete Logarithm:

Consider a primitive root 'a' for a prime number 'p'. For any integer p, following relation satisfies;

$$b \equiv r \pmod{p}$$

If we can find a unique exponent such that,

$$b \equiv a^i \pmod{p}$$

Then i is called discrete logarithm of the number b for the base a mod p and denoted as $dlog_{a,p}(b) = i$

E.g., $a=3$ and $p=7$

Suppose $b=8$.

$$8 \equiv 1 \pmod{7}$$

$$8 \equiv 3^0 \pmod{7}$$

$\therefore dlog_{3,7}(8) = 0$.

Public-Key Cryptosystems:

Public-key cryptography is an encryption scheme that uses two mathematically related, but not identical keys: a public key and a private key. The public key is used to encrypt and the private key is used to decrypt, to protect data against unauthorized access or use. A public key cryptosystem must meet the following three conditions:

i) It must be computationally easy to encipher or decipher a message given the appropriate key.

ii) It must be computationally infeasible to derive the private key from the public key.

iii) It must be computationally infeasible to determine the private key from a chosen plaintext attack.

Applications:

i) Digital Signatures: Content is digitally signed with an individuals private key and is verified by the individuals public key. Digitally signing documents and emails offers the following benefits:

↳ Authentication: Since the individuals unique private key was used to apply the signature, recipients can be confident that the individual was the one to actually apply the signature.

↳ Integrity: When the signature is verified, it checks that the contents of the document or message match. Even the slightest change to the original document would cause this check to fail.

ii) Encryption: Content is encrypted using an individuals public key and can only be decrypted with the individuals private key. Security benefits of encryption are as follows:

↳ Confidentiality: Because the content is encrypted with an individuals public key, it can only be decrypted with the individual's private key, ensuring only the intended recipient can decrypt and view the contents.

↳ Integrity: Part of decryption process involves verifying that the contents of the original encrypted message and the new decrypted match, so even the slightest change to the original content would cause the decryption process to fail.

⊛ Distribution of public key: less imp can be escaped

Several techniques have been proposed for the distribution of public keys. All these techniques can be grouped into the following general schemes:

1) Public announcement of public keys: The users distribute public keys to recipients or broadcast to community at large. For Example: Append PGP keys to email messages or post to news groups or email list. It's major weakness is forgery.

2) **Publicly Available directory:** It can obtain greater level of security by registering with a public directory. This scheme is more secure than individual public announcements but still has vulnerabilities.

3) **Public-Key Authority:** It improves security by tightening control over distribution of keys from directory. Users interact with directory to obtain any desired public key securely. It requires real-time access to directory when keys are needed.

4) **Public-Key Certificates:** Certificates allow key exchange without real-time access to public-key authority. A certificate binds identity to public key. It can be verified by anyone who knows the public-key authorities public-key.

③. Distribution of Secret keys: ← less imp can be escaped

1) **Simple Secret Key distribution:** If A wishes to communicate with B, the following procedure is employed;

→A generates a public/private key pair $\{PU_a, PR_a\}$ and transmits a message to B consisting of PU_a and an identifier of A, IDA.

→B generates a secret key, Ks and transmits it to A, encrypted with A's public key.

2) **Simple use of Public-Key Encryption to Establish a Session Key:**

A and B can now securely communicate using conventional encryption and the session key Ks. At the completion of the exchange, both A and B discard Ks. This protocal is insecure against an adversary who can intercept messages and then either relay the intercepted message or substitute another message. Such an attack is known as a man-in-the-middle attack.

⊛. Diffe-Hellman (D-H) Key Exchange: [Imp]

Diffe-Hellman key exchange is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communication channel.

Steps:

1. Generate two global public elements p and g, where p is the prime number and $g<p$ is primitive root of p.
2. User A select random integer $X_A<p$ and computes $Y_A = g^{X_A} \bmod p$.
3. User B select random integer $X_B<p$ and computes $Y_B = g^{X_B} \bmod p$.
4. Each side keeps the value X as private and makes value Y available to eachother.
5. User A computes key as $K = (Y_B)^{X_A} \bmod p$.
6. User B computes key as $K = (Y_A)^{X_B} \bmod p$.

Example:

$p = 23$, $g = 5$

User A	User B
$X_A<p$, so user A chooses the secret integer $X_A=6$. $Y_A = g^{X_A} \bmod p$ $= 5^6 \bmod 23$ $= 8$ User A sends the value of Y_A to user B. $K = (Y_B)^{X_A} \bmod p$ $= 19^6 \bmod 23$ $= 2$	$X_B<p$, so user B chooses the secret integer $X_B=15$. $Y_B = g^{X_B} \bmod p$ $= 5^{15} \bmod 23$ $= 19$ User B sends the value of Y_B to A. $K = (Y_A)^{X_B} \bmod p$ $= 8^{15} \bmod 23$ $= 2$

Q. Find the result of following operations.

1. $5^{15} \bmod 23$
2. $19^6 \bmod 23$

Solution:

1). $5^{15} \bmod 23$ 3 is smallest power which can divide 15 and just greater than 23.

$\Rightarrow (5^3 * 5^3 * 5^3 * 5^3 * 5^3) \bmod 23$

$\Rightarrow (10 * 10 * 10 * 10 * 10)$ values after mod 23

$\Rightarrow (10^2 * 10^2 * 10) \bmod 23$

$\Rightarrow (8 * 8 * 10)$

$\Rightarrow (64 * 10) \bmod 23$

$\Rightarrow (18 * 10)$

$\Rightarrow 180 \bmod 23$

$\Rightarrow 19$

2). $19^6 \bmod 23$

$\Rightarrow (19^2 * 19^2 * 19^2) \bmod 23$

$\Rightarrow (16 * 16 * 16)$

$\Rightarrow (16^2 * 16) \bmod 23$

$\Rightarrow (3 * 16)$

$\Rightarrow 48 \bmod 23$

$\Rightarrow 2$

Q. Consider a Deffie-Hellman scheme with a common prime $p=11$ and a primitive root $g=2$.

i) Show that 2 is a primitive root of 11.

ii) If user A has public key $Y_A = 9$, what is A's private key X_A?

iii) If user B has public key $Y_B = 3$, what is shared key K, shared with A?

Solution:

i) Here, $p = 11$ & $g = 2$

$2^1 \bmod 11 = 2 \bmod 11 = 2$

$2^2 \bmod 11 = 4 \bmod 11 = 4$

$2^3 \bmod 11 = 8 \bmod 11 = 8$

$2^4 \bmod 11 = 16 \bmod 11 = 5$

$2^5 \bmod 11 = 32 \bmod 11 = 10$

$2^6 \bmod 11 = 64 \bmod 11 = 9$

$2^7 \bmod 11 = 128 \bmod 11 = 7$

$2^8 \bmod 11 = 256 \bmod 11 = 3$

$2^9 \bmod 11 = 512 \bmod 11 = 6$

$2^{10} \bmod 11 = 1024 \bmod 11 = 1.$

Here all values are distinct.
So, 2 is a primitive root of 11.

ii) User A's public key $Y_A = 9$

A's private key $X_A = ?$

We have,

$Y_A = g^{X_A} \bmod p.$

$9 = 2^{X_A} \bmod 11$

From this equation,

$X_A = 6$, because $2^6 \bmod 11 = 9$.

$\therefore$ A's private key $X_A = 6$.

iii) B's public key $Y_B = 3$

Now,

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

$= 3^6 \bmod 11$

$= 729 \bmod 11$

$= 3$

$\therefore$ Shared key $K = 3$.

⊛. Man-In-The-Middle Attack: [Imp]

i.e., spying or monitoring

A man-in-the-middle attack is a form of eavesdropping where communication between two users is monitored and modified by an unauthorized party. Generally, the attacker actively eavesdrops by intercepting public key message exchanged and retransmit the message while replacing the requested key with his own.

question maybe asked as this, or whatever but always ~~but~~ we write this theory of man-in-middle attack

> Q. How Man-In-Middle attack is possible in Deffie-Hellman Algorithm?
>
> OR
>
> Q. What do you mean by Man-In-Middle attack? Is man in middle attack possible in Diffe-Hellman algorithm for key exchange? How?

Diffie-Hellman key exchange is insecure against a man-in-the-middle attack. Suppose Alice and Bob wish to exchange keys and Darth is adversary. The attack proceeds as follows:

1. Darth prepares for attack by generating two random private key's X_{D1} & X_{D2} and then computing the corresponding public keys Y_{D1} & Y_{D2}. [$Y_{D1} = g^{X_{D1}} \bmod p$ & $Y_{D2} = g^{X_{D2}} \bmod p$].
2. Alice transmits Y_A to Bob.
3. Darth intercepts Y_A and transmits Y_{D1} to Bob. Darth also calculates $K_2 = (Y_A)^{X_{D2}} \bmod p$.
4. Bob receives Y_{D1} and calculates $K_1 = (Y_{D1})^{X_B} \bmod p$.
5. Bob transmits Y_B to Alice.
6. Darth intercepts Y_B and transmits Y_{D2} to Alice. Darth calculates $K_1 = (Y_B)^{X_{D1}} \bmod p$.
7. Alice receives Y_{D2} and calculates $K_2 = (Y_{D2})^{X_A} \bmod p$.

At this point, Bob and Alice think that they share a secret key but instead Bob and Darth share secret key K_1 and Alice and Darth share secret key K_2.

Example: Let $p=11$ & $g=2$.

Let Alice's private key $X_A=5$.

$$Y_A = g^{X_A} \bmod p = 2^5 \bmod 11 = 10$$

Let Bob's private key $X_B=3$

$$Y_B = g^{X_B} \bmod p = 2^3 \bmod 11 = 8$$

1. Darth's two private keys:

Let $X_{D1}=6$ & $X_{D2}=9$.

Darth calculates $Y_{D1} = g^{X_{D1}} \bmod p = 2^6 \bmod 11 = 9$

& $Y_{D2} = g^{X_{D2}} \bmod p = 2^9 \bmod 11 = 6$.

2. Alice transmits $Y_A=10$ to Bob.
3. Darth intercepts Y_A and transmits $Y_{D1}=9$ to Bob. And Darth calculates $K_2 = (Y_A)^{X_{D2}} \bmod p = 10^9 \bmod 11 = 10$.
4. Bob receives $Y_{D1}=9$ and calculates $K_1 = (Y_{D1})^{X_B} \bmod p = 9^3 \bmod 11 = 3$.
5. Bob transmits $Y_B=8$ to Alice.
6. Darth intercepts Y_B and transmits $Y_{D2}=6$ to Alice. And Darth calculates $K_1 = (Y_B)^{X_{D1}} \bmod p = 8^6 \bmod 11 = 3$.
7. Alice receives $Y_{D2}=6$ and calculates $K_2 = (Y_{D2})^{X_A} \bmod p = 6^5 \bmod 11 = 10$.

Here Bob and Darth share secret key $K_1=3$ and Alice and Darth share secret key $K_2=10$.

⊛. RSA (Rivest Shamir Adleman) Algorithm: [Imp]

→ RSA algorithm is public key cryptography. i.e, it works on two different keys: public key and private key.

→ The public key can be known to everyone and is used for encrypting message. Message encrypted with the public key can only be decrypted using the private key.

RSA key generation:

1. Choose two distinct large prime numbers p and q.
2. Compute $n = pq$, n is used as modulus for both public and private keys.
3. Compute the totient: $\phi(n) = (p-1)(q-1)$.
4. Choose an integer e such that $1 < e < \phi(n)$ and e and $\phi(n)$ are co-prime.
5. Compute d to satisfy $ed \equiv 1 \pmod{\phi(n)}$.
6. Public key is $\{e, n\}$.
7. Private key is $\{d, n\}$.

Encryption:

$$c = m^e \bmod n.$$

Decryption:

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

Example: $p = 5$ & $q = 19$ (let).

$$n = pq = 5*19 = 95$$

$$\phi(n) = (5-1)(19-1) = 4*18 = 72$$

integer greater than 1 (i.e, start from 2) and smaller than 72 & having only one common factor.
$72 = 2\times2\times2\times2\times2\times2\times1$
$5 = 5\times1$

Choose e, such that $1 < e < 72$ and co-prime to 72.

$$\therefore e = 5$$

Calculate d by using;

$$ed \equiv 1 \pmod{\phi(n)}$$

$$5*d \equiv 1 \pmod{72}$$

$$5*29 \equiv 1 \pmod{72}$$

$$\therefore d = 29.$$

So, the public key is $\{e, n\} = \{5, 95\}$ and the private key is $\{d, n\} = \{29, 95\}$.

Consider $m = 19$.

Encryption:

$$c = m^e \bmod n$$
$$= 19^5 \bmod 95$$
$$= 19$$

Decryption:

$$m = c^d \bmod n$$
$$= 19^{29} \bmod 95$$
$$= 19$$

Q. In a RSA system, a user has chosen the primes 53 and 59 to create a key pair. Now show that the generation of public key pair (e,n) and private key pair (d,n). Show encryption and decryption process for the message "HI".

Solution:

Given, $p=53$, $q=59$

$n=pq=53*59=3127$

$\phi(n)=(53-1)(59-1)=3016$

Choose e, such that $1<e<3016$ and co-prime to 3016.

$\therefore e=3$.

Calculate d by using;

$ed \equiv 1 (\text{mod } \phi(n))$

$3*d \equiv 1 (\text{mod } 3016)$

$3*2011 \equiv 1 (\text{mod } 3016)$

$\therefore d=2011$

large no. like this भए सजिलोको लागि यसरी गर्ने. $\frac{3016}{3}=1005.33=1005$
Now check if $3*1005 \equiv 1 (\text{mod } 3016)$.
Here it is false, so, we ~~keep on~~ proceed as;
$1005.33 \times 2 = 2010.66 = 2011$.
Now again check if it satisfies.

So, the public key is $\{e,n\}=\{3,3127\}$ and the private key is $\{d,n\}=\{2011,3127\}$

Let us assume "HI" = 89.

Encryption:

$c = m^e \text{ mod } n$

$= 89^3 \text{ mod } 3127$

$= 1394$

Decryption:

$m = c^d \text{ mod } n$

$= 1394^{2011} \text{ mod } 3127$

$= 89$

⊛. Elgamal Cryptographic System:

→ It is public-key cryptosystem.

→ It has three steps: key generation, encryption and decryption.

Key Generation:

→ Select a large prime number p and g, where g is the primitive root of p.

→ Choose $x \in [1, p-1]$ and compute $y = g^x \text{ mod } p$.

→ Private key $= x$

→ Public key $= (p, g, y)$.

Encryption:

Encrypt m as a pair of integer (C_1, C_2).

→ Pick a random integer $k \in [1, p-2]$.

→ Compute $C_1 = g^k \bmod p$

→ Compute $C_2 = m \times y^k \bmod p$.

Decryption:

$$m = C_2 \times C_1^{-x} \bmod p.$$

Example: Let $p = 23$ and $g = 7$.

Key generation:

→ Choose private key $x = 9$.

→ $y = g^x \bmod p = 7^9 \bmod 23 = 15$

→ Public key: $(p, g, y) = (23, 7, 15)$

Encryption:

→ Let $m = 20$

→ Pick a random number $k = 3$

→ $C_1 = g^k \bmod p = 7^3 \bmod 23 = 21$

→ $C_2 = m \times y^k \bmod p = 20 \times 15^3 \bmod 23 = 18$

→ Send $(C_1, C_2) = (21, 18)$ as a ciphertext.

Decryption:

$$m = C_2 \times C_1^{-x} \bmod p$$

$$= 18 \times \frac{1}{21^9} \bmod 23$$

$$= 20$$