Unit-III
Asymmetric Ciphers

Primality Testing

- A primality testing is an algorithm to test whether a given number is prime or not.
- A **prime number** is a number (>1) which is divisible by 1 and itself. For e.g. 2, 3, 5, 7

Miller-Rabin Primality Testing

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

1. *Write* $\boldsymbol{n-1=2^k m}$, *where* $\boldsymbol{m}$ *is odd.*
2. *Choose a random number* $\boldsymbol{a}$; $1 \leq a \leq n-1$.
3. *Compute* $\boldsymbol{b = a^m \bmod n}$
4. *If* $\boldsymbol{b \equiv 1 (mod\ n)}$ *then return PRIME.*
5. *For* $\boldsymbol{i = 0\ to\ k-1}$
   do
   IF $\boldsymbol{b \equiv -1 (mod\ n)}$ *then return PRIME.*
   ELSE $\boldsymbol{b = b^2 \bmod n}$
6. *Return COMPOSITE.*

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

$n = 17$
$n - 1 = 16 = 2^4 * 1\ ,\ \ k = 4\ \&\ m = 1$
$a \rightarrow (1-16); a = 5$
$b = a^m\ mod\ n = 5^1\ mod\ 17 = 5$
$b \equiv 1 (mod\ n) \Rightarrow 5 \equiv 1 (mod\ 17)$ which is false.
So,
$i = 0\ to\ k-1\ \ i.e.\ i = 0\ to\ 3$

$i = 0$
$b = 5$
$5 + 1 = 6\ mod\ 17 = 6$
$b = b^2\ mod\ n = 25\ mod\ 17 = 8$

$b \equiv -1 (mod\ n) \Rightarrow (b+1)\ mod\ n = 0$

$i = 1$
$b = 8$
$8 + 1 = 9\ mod\ 17 = 9$
$b = b^2\ mod\ n = 64\ mod\ 17 = 13$

$i = 2$
$b = 13$
$13 + 1 = 14\ mod\ 17 = 14$
$b = 13^2\ mod\ 17 = 169\ mod\ 17 = 16$

$i = 3$
$b = 16$
$16 + 1 = 17\ mod\ 17 = 0$

$\therefore$ 17 is prime.

Q. Determine whether the integer 7 is prime or not using Miller-Rabin algorithm.
Sol^n:

$n = 7$
$n - 1 = 6 = 2^1 * 3\ ,\ \ k = 1\ \&\ m = 3$
$a \rightarrow (1 - 6); a = 4$
$b = a^m\ mod\ n = 4^3\ mod\ 7 = 64\ mod\ 7 = 1$
$b \equiv 1(mod\ n) \Rightarrow 1 \equiv 1(mod\ 7)$ which is true. So, 7 is prime.

- ***Two properties of prime number given by Rabin-Miller:***

Property 1:

If p is prime and a is a positive integer less than p, then $a^2\ mod\ p = 1$if and only if either $a\ mod\ p = 1$ or $a\ mod\ p = -1\ mod\ p = p - 1$.

Property 2:

Let p be a prime number greater than 2. We can then write $p - 1 = 2^q k$, with $k > 0\ and\ q$ as odd. Let a be any integer such that $1 < a < p - 1$ then one of the following conditions is true:

- $a^q\ mod\ p = 1$
- One of the number $a^q, a^{2q}, a^{4q}, \ldots\ldots\ldots, a^{2^{k-1}q}$ is congruent to $1\ mod\ p$.

Fermat's Little Theorem

Fermat's theorem states that: if p is prime and a is a positive integer not divisible by p, then

$$\boldsymbol{a^{p-1} \equiv 1(mod\ p)}$$

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

Alternatively,

$$\boldsymbol{a^p \equiv a(mod\ p)}$$

E.g. $a = 3, p = 5$ then $3^5 \equiv 3(mod\ 5)$

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

Euler Totient Function

- denoted by $\phi(n)$.
- It is defined as the number of positive integer less than n, which are relatively prime to 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}
$\therefore \phi(10) = 4$

⇒ ***If p is prime number then,***

$$\boldsymbol{\phi(p) = p - 1}$$

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

⇒ ***Let p and q are two prime numbers such that $p \neq q$ and $n = pq$, then***

$$\boldsymbol{\phi(n) = (p-1)(q-1)}$$

E.g. $\phi(15) = ?$
$15 = 3 \times 5$
$\phi(15) = (3-1)(5-1) = 2 * 4 = 8$

Euler's Theorem

Euler's theorem states that if 'a' and 'n' are co-prime positive integers then,

$$\boldsymbol{a^{\phi(n)} \equiv 1 (mod\ n)}$$

Alternatively,

$$\boldsymbol{a^{\phi(n)+1} \equiv a (mod\ n)}$$

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

E.g.

$a = 3, n = 10, \phi(10) = 4$ then, $3^4 \equiv 1 (mod\ 10)$ **or** $3^5 \equiv 3 (mod\ 10)$

Primitive Root

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

Q. Is 2 a primitive root of 5?
Sol^n:

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

$2^1\ mod\ 5 = 2$
$2^2\ mod\ 5 = 4$
$2^3\ mod\ 5 = 3$
$2^4\ mod\ 5 = 1$

Here, all values are distinct and consists of integers 1 to 4.
$\therefore$ 2 is primitive root of 5.

Q. Find out whether 3 is primitive root of 7?
Solⁿ:

Here, $a = 3$ and $p = 7$

$3^1 \ mod \ 7 = 3 \ mod \ 7 = 3$
$3^2 \ mod \ 7 = 9 \ mod \ 7 = 2$
$3^3 \ mod \ 7 = 27 \ mod \ 7 = 6$
$3^4 \ mod \ 7 = 81 \ mod \ 7 = 4$
$3^5 \ mod \ 7 = 243 \ mod \ 7 = 5$
$3^6 \ mod \ 7 = 729 \ mod \ 7 = 1$

Here, all values are distinct and consists of integers 1 to 6.

∴ 3 is primitive root of 7.

Q. Is 2 a primitive root of 7?
Solⁿ:

Here, $a = 2$ and $p = 7$

$2^1 \ mod \ 7 = 2$
$2^2 \ mod \ 7 = 4$
$2^3 \ mod \ 7 = 1$
$2^4 \ mod \ 7 = 2$

Repeat

∴ 2 is not primitive root of 7.

Discrete Logarithm

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

$$b \equiv r(mod \ p)$$

If we can find a unique exponent such that

$$b \equiv a^i(mod \ p)$$

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 $b = 8$

$$8 \equiv 1(mod \ 7)$$
$$8 \equiv 3^0(mod \ 7)$$

∴ $dlog_{3,7}(8) = 0$

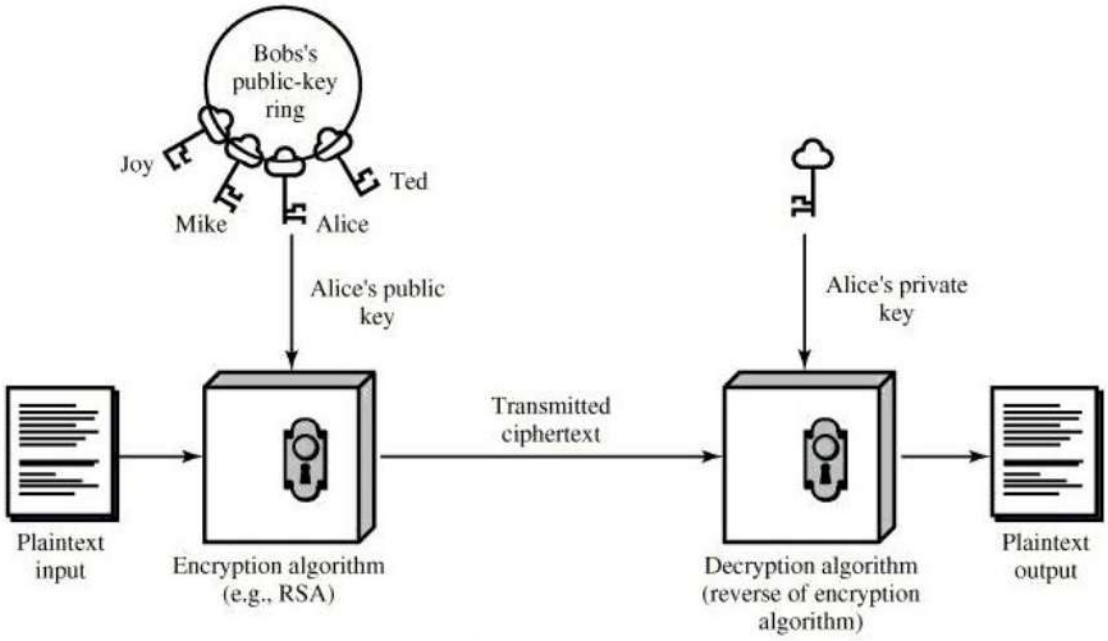
Public-Key Cryptosystems

Asymmetric (Public-key) algorithms rely on one key for encryption and a different but related key for decryption. These algorithms have the following important characteristic:

- It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key.
- Either of the two related keys can be used for encryption, with the other used for decryption.

A public-key encryption scheme has six ingredients:

- ***Plaintext:*** This is the readable message or data that is fed into the algorithm as input.
- ***Encryption algorithm:*** The encryption algorithm performs various transformations on the plaintext.
- ***Public and private keys:*** This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.
- ***Ciphertext:*** This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.
- ***Decryption algorithm:*** This algorithm accepts the ciphertext and the matching key and produces the original plaintext.



(a) Encryption

The essential steps are the following:

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private. As above figure, each user maintains a collection of public keys obtained from others.
3. If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
4. When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

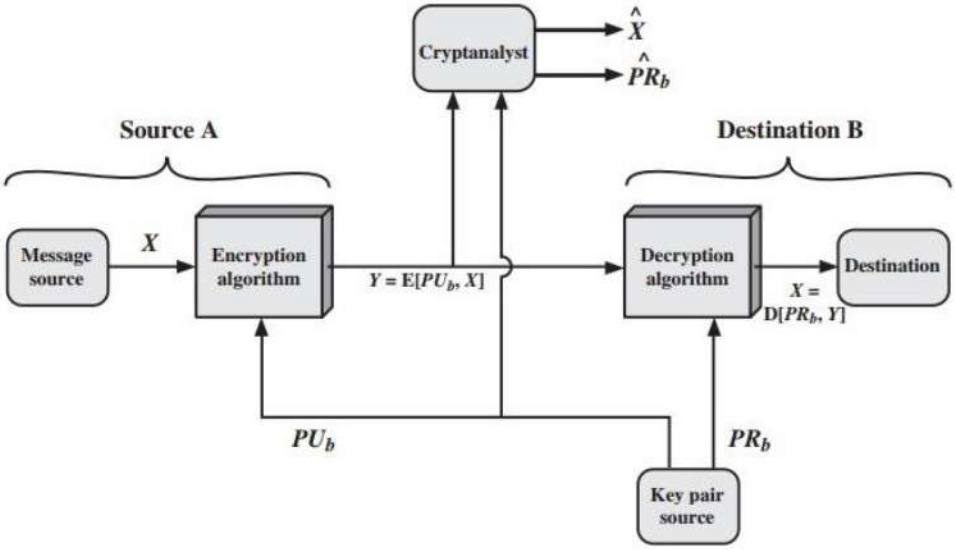
Public-Key Cryptosystem for Secrecy

There is some source A that produces a message in plaintext, $X = [X_1, X_2, \ldots\ldots, X_M]$.The M elements of X are letters in some finite alphabet. The message is intended for destination B. B generates a related pair of keys: a public key, PU_b, and a private key, PR_b. PR_b is known only to B, whereas PU_b is publicly available and therefore accessible by A.

With the message X and the encryption key PU_b as input, A forms the ciphertext $Y = [Y_1, Y_2, \ldots\ldots, Y_N]$:

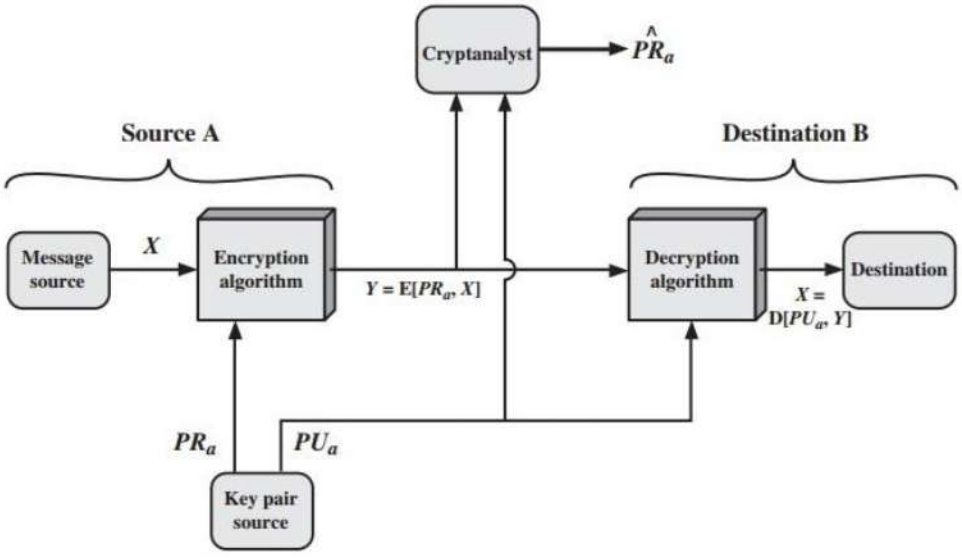
$$Y = E(PU_b, X)$$

The intended receiver, in possession of the matching private key, is able to invert the transformation $X = D(PR_b, Y)$



Public-Key Cryptosystem: Authentication

In this case, A prepares a message to B and encrypts it using A's private key before transmitting it. B can decrypt the message using A's public key. Because the message was encrypted using A's private key, only A could have prepared the message. Therefore, the entire encrypted message serves as a digital signature. In addition, it is impossible to alter the message without access to A's private key, so the message is authenticated both in terms of source and in terms of data integrity. Figure show the use of public-key encryption to provide authentication:



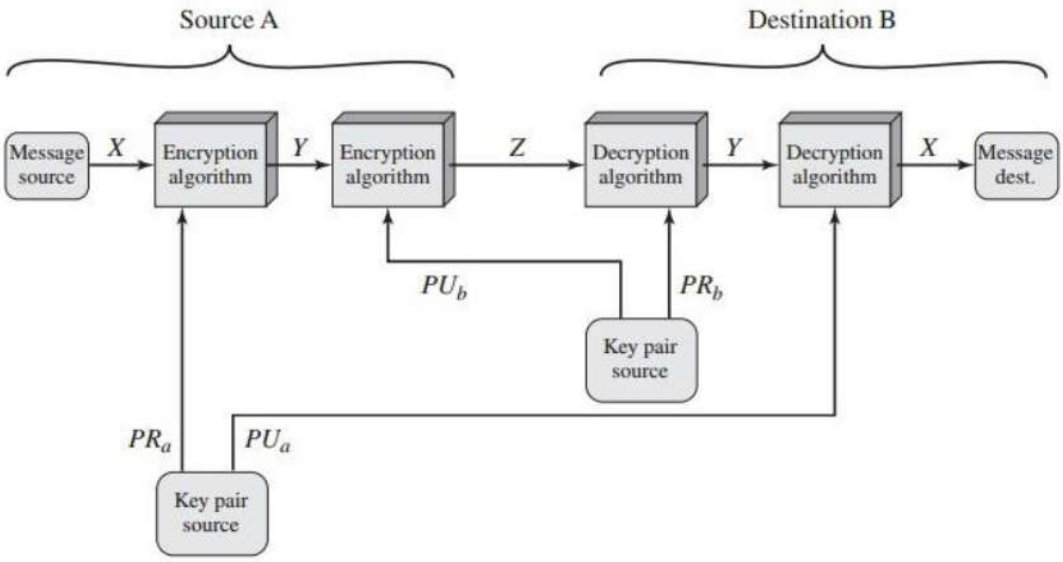
Public-Key Cryptosystem: Authentication and Secrecy

It is, however, possible to provide both the authentication function and confidentiality by a double use of the public-key scheme:

$$Z = E(PU_b, E(PR_a, X))$$

$$X = D(PU_a, D(PR_b, Z))$$

In this case, we begin as before by encrypting a message, using the sender's private key. This provides the digital signature. Next, we encrypt again, using the receiver's public key. The final ciphertext can be decrypted only by the intended receiver, who alone has the matching private key. Thus, confidentiality is provided. The disadvantage of this approach is that the public-key algorithm, which is complex, must be exercised four times rather than two in each communication.



Q. Distinguish between conventional and public key encryption.

Sol^n:

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

Applications of Public Key Cryptography

Public-key systems are characterized by the use of a cryptographic algorithm with two keys, one held private and one available publicly. Depending on the application, the sender uses either the sender's private key or the receiver's Public key, or both, to perform some type of cryptographic function. In broad terms, we can classify the use of Public-key cryptosystems into three categories:

- ***Encryption/decryption:*** The sender encrypts a message with the recipient's Public key.
- ***Digital signature:*** The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.
- ***Key exchange:*** Two sides cooperate to exchange a session key. Several different approaches are possible, involving the Private key(s) of one or both parties.

Distribution of Public Keys

Public key can be distributed in 4 ways: Public announcement, Publicly available directory, Public-key authority, and Public-key certificates.

1. ***Public Announcement:*** Here the public key is broadcasted to everyone. Major weakness of this method is forgery. Anyone can create a key claiming to be someone else and broadcast it. Until forgery is discovered can masquerade as claimed user.
2. ***Publicly Available Directory:*** In this type, the public key is stored at a public directory. Directories are trusted here, with properties like Participant Registration, access and allow to modify values at any time, contains entries like {name, public-key}. Directories can be accessed electronically still vulnerable to forgery or tampering.

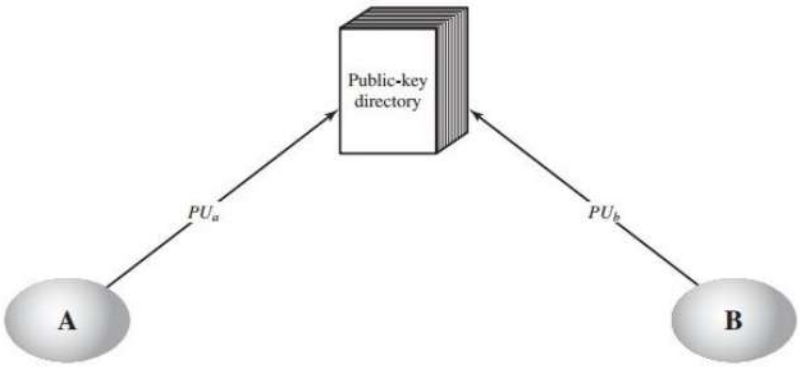


Fig: Public-key publication

3. ***Public Key Authority:*** It is similar to the directory but, improve security by tightening control over distribution of keys from directory. It requires users to know public key for the directory. Whenever the keys are needed, a real-time access to directory is made by the user to obtain any desired public key securely.
4. ***Public Certification:*** This time authority provides a certificate (which binds identity to the public key) to allow key exchange without real-time access to the public authority each time. The certificate is accompanied with some other info such as period of validity, rights of use etc. All of this content is signed by the trusted Public-Key or Certificate Authority (CA) and it can be verified by anyone possessing the authority's public-key.

Diffe-Hellman (D-H) Key Exchange

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 prime number and $g < p$ is primitive root of p.
2. User A select random integer $X_A < p$ and computes $Y_A = g^{X_A} mod\ p$.
3. User B select random integer $X_B < p$ and computes $Y_B = g^{X_B} mod\ p$.
4. Each side keeps the X value as private and makes Y value available to each other.
5. User A computes key as $K = (Y_B)^{X_A}\ mod\ p$.
6. User B computes key as $K = (Y_A)^{X_B}\ mod\ p$.

Example

$p = 23, g = 5$

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

Q. Find the result of following operations.

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

Solution:

1. $\mathbf{5^{15}\ mod\ 23}$	2. $\mathbf{19^6\ mod\ 23}$
$\Rightarrow (5^3 * 5^3 * 5^3 * 5^3 * 5^3)\ mod\ 23$ $\Rightarrow (10 * 10 * 10 * 10 * 10)$ $\Rightarrow (10^2 * 10^2 * 10) mod\ 23$ $\Rightarrow (8 * 8 * 10)$ $\Rightarrow (64 * 10)\ mod\ 23$ $\Rightarrow (18 * 10)$ $\Rightarrow 180\ mod\ 23$ $\Rightarrow 19$	$\Rightarrow (19^2 * 19^2 * 19^2)\ mod\ 23$ $\Rightarrow (16 * 16 * 16)$ $\Rightarrow (16^2 * 16)\ mod\ 23$ $\Rightarrow (3 * 16)$ $\Rightarrow 48\ mod\ 23$ $\Rightarrow 2$

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, $p = 11$ & $g = 2$

$2^1 \ mod\ 11 = 2 \ mod\ 11 = 2$
$2^2 \ mod\ 11 = 4 \ mod\ 11 = 4$
$2^3 \ mod\ 11 = 8 \ mod\ 11 = 8$
$2^4 \ mod\ 11 = 16 \ mod\ 11 = 5$
$2^5 \ mod\ 11 = 32 \ mod\ 11 = 10$
$2^6 \ mod\ 11 = 64 \ mod\ 11 = 9$
$2^7 \ mod\ 11 = 128 \ mod\ 11 = 7$
$2^8 \ mod\ 11 = 256 \ mod\ 11 = 3$
$2^9 \ mod\ 11 = 512 \ mod\ 11 = 6$
$2^{10} \ mod\ 11 = 1024 \ mod\ 11 = 1$

Here all values are distinct and consists of integers 1 to 10 (i.e. 1 to $p - 1$). Hence, 2 is a primitive root of 11.

ii) User A's public key $Y_A = 9$
A's private key X_A =?
We have,

$Y_A = g^{X_A} mod\ p$
$9 = 2^{X_A} \ mod\ 11$

From this equation,

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

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

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

$K = (Y_B)^{X_A} \ mod\ p$
$= 3^6 \ mod\ 11$
$= 729 \ mod\ 11$
$= 3$

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

Man-In-Middle Attack

A man-in-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.

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}. [$Y_{D1} = g^{X_{D1}} mod\ p$ & $Y_{D2} = g^{X_{D2}} mod\ p$].
2. Alice transmits Y_A to Bob.
3. Darth intercepts Y_A and transmits Y_{D1} to Bob. Darth also calculates $K_2 = (Y_A)^{X_{D2}}\ mod\ p$.
4. Bob receives Y_{D1} and calculates $K_1 = (Y_{D1})^{X_B}\ mod\ p$.
5. Bob transmits Y_B to Alice.
6. Darth intercepts Y_B and transmits Y_{D2} to Alice. Darth calculates $K_1 = (Y_B)^{X_{D1}}\ mod\ p$.
7. Alice receives Y_{D2} and calculates $K_2 = (Y_{D2})^{X_A}\ mod\ p$.

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 $X_A = 5$.

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

Let Bob's private key $X_B = 3$.

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

1. Darth's two private keys: Let $X_{D1} = 6$ & $X_{D2} = 9$
   Darth calculates $Y_{D1} = g^{X_{D1}}\ mod\ p = 2^6\ mod\ 11 = 9$ and $Y_{D2} = g^{X_{D2}}\ mod\ p = 2^9\ mod\ 11 = 6$.
2. Alice transmits $Y_A = 10$ to Bob.
3. Darth intercepts Y_A and transmits $Y_{D1} = 9$ to Bob. And Darth calculates $K_2 = (Y_A)^{X_{D2}}\ mod\ p = 10^9\ mod\ 11 = 10$.
4. Bob receives $Y_{D1} = 9$ and calculates $K_1 = (Y_{D1})^{X_B}\ mod\ p = 9^3\ mod\ 11 = 3$.
5. Bob transmits $Y_B = 8$ to Alice.
6. Darth intercepts Y_B and transmits $Y_{D2} = 6$ to Alice. And Darth calculates $K_1 = (Y_B)^{X_{D1}}\ mod\ p = 8^6\ mod\ 11 = 3$.
7. Alice receives $Y_{D2} = 6$ and calculates $K_2 = (Y_{D2})^{X_A}\ mod\ p = 6^5\ mod\ 11 = 10$.

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

RSA (Rivest Shamir Adleman) Algorithm

- RSA algorithm is public key cryptography i.e. it works on two different keys i.e. 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.

Algorithm

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 $ed \equiv 1(mod\ \phi(n))$.
6. Public key is $\{e, n\}$.
7. Private key is $\{d, n\}$.

Encryption:

$c = m^e \ mod\ n$

Decryption:

$m = c^d \ mod\ n$

Example

$p = 5$ & $q = 19$

$n = pq = 5 * 19 = 95$

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

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

$\therefore e = 5$

Calculate d by using;

$ed \equiv 1(mod\ \phi(n))$

$5 * d \equiv 1(mod\ 72)$

$5 * 29 \equiv 1(mod\ 72)$

$\therefore d = 29$

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

Consider $m = 19$

Encryption:

$c = m^e \ mod\ n$

$= 19^5 \ mod\ 95$

$= 19$

Decryption:

$m = c^d \ mod\ n$

$= 19^{29} \ mod\ 95$

$= 19$

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;
$ed \equiv 1(mod\ \phi(n))$
$3 * d \equiv 1(mod\ 3016)$
$3 * 2011 \equiv 1(mod\ 3016)$
$\therefore d = 2011$

So, the public key is $\{e, n\} = \{3, 3127\}$ and the private key is $\{d, n\} = \{29, 95\}$.

Let us assume "HI" $= 89$

Encryption:

$c = m^e\ mod\ n$
$= 89^3\ mod\ 3127$
$= 1394$

Decryption:

$m = c^d\ mod\ n$
$= 1394^{2011}\ mod\ 3127$
$= 89$

Security approaches of RSA algorithm

Four possible security approaches to attacking the RSA algorithm are as follows:

- ***Brute force:*** This involves trying all possible private keys.
- ***Mathematical attacks:*** There are several approaches, all equivalent in effort to factoring the product of two primes.
- ***Timing attacks:*** These depend on the running time of the decryption algorithm.
- ***Chosen ciphertext attacks:*** This type of attack exploits properties of the RSA algorithm.

The defense against the brute-force approach is the same for RSA as for other cryptosystems, namely, to use a large key space. Thus, the larger the number of bits in d, the better. However, because the calculations involved, both in key generation and in encryption/decryption, are complex, the larger the size of the key, the slower the system will run.

Elgamal Cryptographic System

- It is a 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 $y = g^x \ mod \ p$.
- 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 $C_1 = g^k \ mod \ p$
- Compute $C_2 = m \times y^k \ mod \ p$

Decryption:

Decrypt message by computing following;

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

Example

Key generation:

- Let $p = 23 \ and \ g = 7$.
- Choose private key $x = 9$
- $y = g^x \ mod \ p = 7^9 \ mod \ 23 = 15$
- Public key: $(p, g, y) = (23, 7, 15)$

Encryption:

- Let $m = 20$
- Pick a random number $k = 3$
- $C_1 = g^k \ mod \ p = 7^3 \ mod \ 23 = 21$
- $C_2 = m \times y^k \ mod \ p = 20 \times 15^3 \ mod \ 23 = 18$
- Send $(C_1, C_2) = (21, 18)$ as a ciphertext.

Decryption:

$$m = C_2 \times {C_1}^{-x} \ mod \ p = \frac{C_2}{{C_1}^x} mod \ p = \frac{18}{21^9} mod \ 23 = 20$$

Q. Given the prime number p = 17 and the primitive root g = 6, private key of sender with X=5 and random integer K = 10, show encryption and decryption process for the message m = 13 using Elgamal cryptosystem.

Solution:

Key generation:

- Given, $p = 17$ *and* $g = 6$
- Private key $x = 5$
- $y = g^x \, mod \, p = 6^5 \, mod \, 17 = 7$
- Public key: $(p, g, y) = (17, 6, 7)$

Encryption:

- Given, $m = 13$
- Pick a random number $k = 10$
- $C_1 = g^k \, mod \, p = 6^{10} \, mod \, 17 = 15$
- $C_2 = m \times y^k \, mod \, p = 13 \times 7^{10} \, mod \, 17 = 9$
- Sender sends $(C_1, C_2) = (15, 9)$ as a ciphertext.

Decryption:

Receiver receives $(C_1, C_2) = (15, 9)$ from sender.

$$m = C_2 \times {C_1}^{-x} \, mod \, p = \frac{C_2}{{C_1}^x} mod \, p = \frac{9}{15^5} mod \, 17 = 13$$

Receiver has now decrypted the message and received: 13

Please let me know if I missed anything or anything is incorrect.

poudeljayanta99@gmail.com