Unit III

3 Public Key and Management

Syllabus

Public Key Cryptography, RSA Algorithm : Working, Key length, Security, Key Distribution, Deffie-Hellman Key Exchange, Elliptic Curve : Arithmetic, Cryptography, Security, Authentication methods, Message Digest, Kerberos, X.509 Authentication service. Digital Signatures : Implementation, Algorithms, Standards (DSS), Authentication Protocol.

Contents

3.1 Public Key Cryptography

- Diffie and Hellman proposed a new type of cryptography that distinguished between encryption and decryption keys. One of the keys would be publicly known; the other would be kept private by its owner.
- These algorithms have the following important **characteristic.**
  1. It must be computationally easy to encipher or decipher a message given the appropriate key.
  2. It must be computationally infeasible to derive the private key from the public key.
  3. It must be computationally infeasible to determine the private key from a chosen plaintext attack.
- A public key encryption scheme has six ingredients. Fig. 3.1.1 shows public key cryptography. (See Fig. 3.1.1 on next page)

1. **Plaintext :** It is input to algorithm and in a readable message or data.
2. **Encryption algorithm :** It performs various transformations on the plaintext.
3. **Public and private keys :** One key is used for encryption and other is used for decryption.
4. **Ciphertext :** This is the scrambled message produced as output. It depends on the plaintext and the key.
5. **Decryption algorithm :** This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

- 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. This is the public key. The companion key is kept private.
  3. If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
  4. Alice decrypts the message using her private key.
- The public key is accessed to all participants and private key is generated locally by each participant.
- System controls its private key. At any time, a system can change its private key. Fig. 3.1.2 shows the process of public key algorithm.
- A message from source which is in a plaintext $X = (X_1, X_2, \ldots X_m)$. The message is intended for destination which generates a related pair of keys a public key KU_b, and a private key KR_b.
- Private key is secret key and known only to Y_1. With the message X and encryption key KU_b as input, Y_1 forms the ciphertext.

$$Y = (Y_1, Y_2, Y_3 \ldots . Y_n)$$

$$Y = E_{KU_b}(X)$$

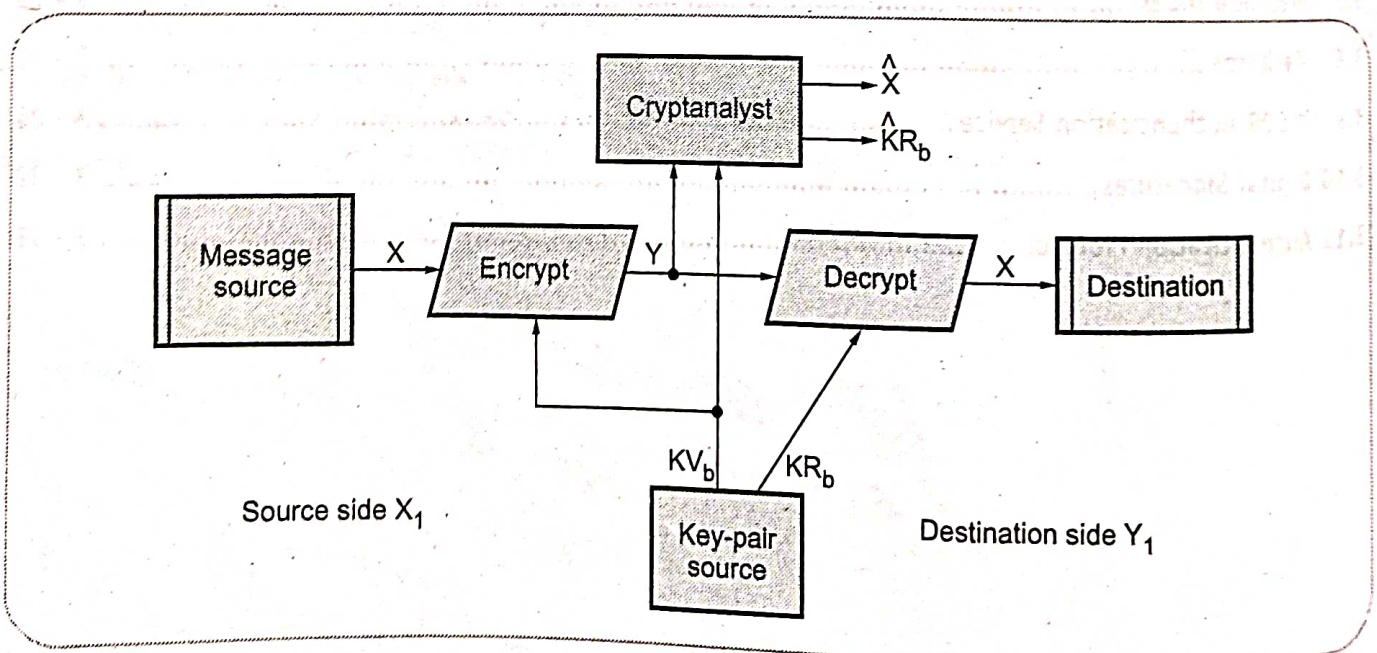


Fig. 3.1.2 Public key cryptosystem secrecy

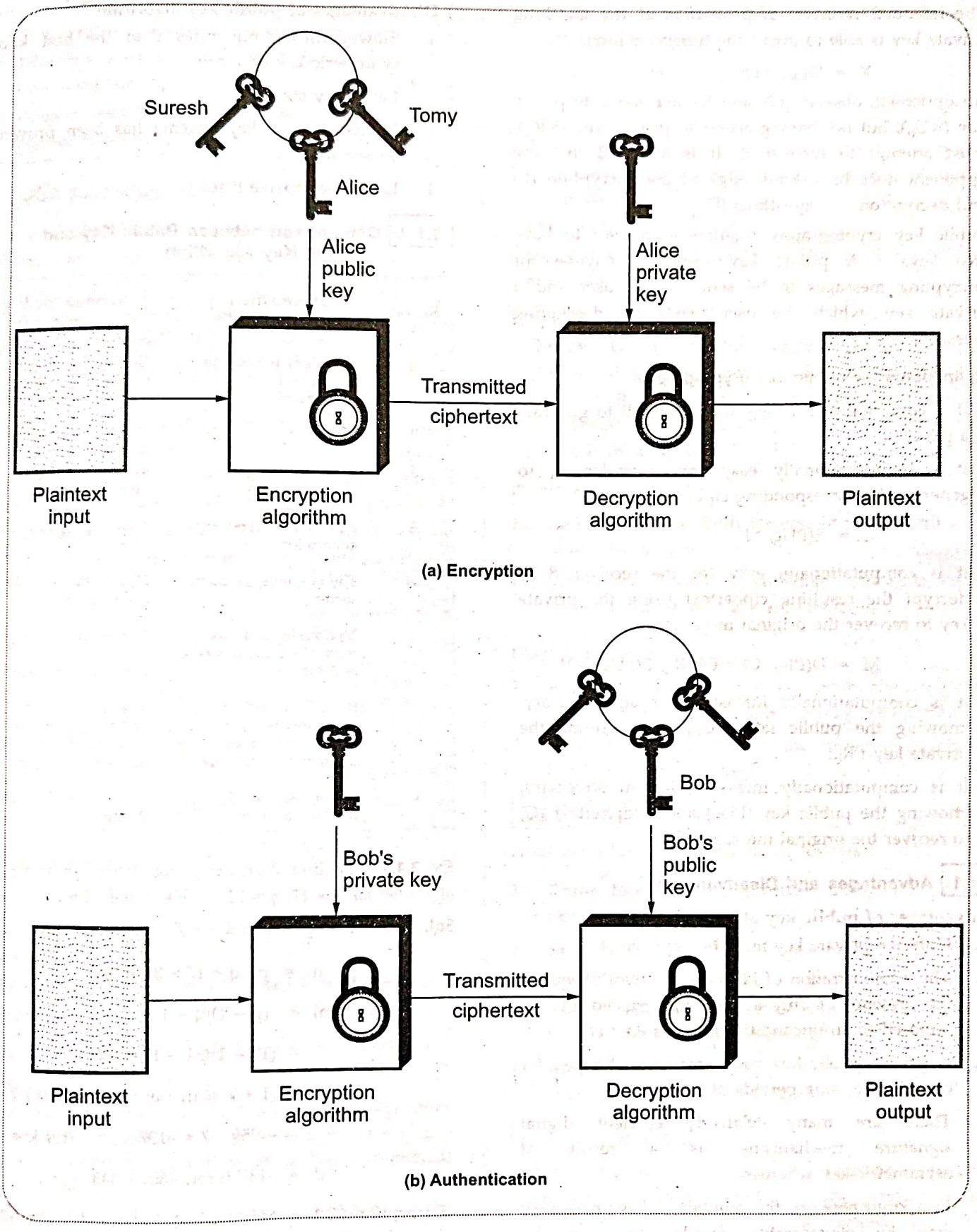


Fig. 3.1.1 Public key cryptography

- The intended receiver, in possession of the matching private key is able to invert the transformation.

$$X = D_{KR_b}(Y)$$

- An opponent, observing Y and having access to public key (KU_b), but not having access to private key (KR_b), must attempt to recover X. It is assumed that the opponent does have knowledge of the encryption (E) and decryption algorithms (D).
- Public key cryptography requires each user to have two keys : A public key used by anyone for encrypting messages to be sent to that user and a private key, which the user needs for decrypting messages.

Requirements for public key cryptography

1. It is computationally easy for a party B to generate a pair.
2. It is computationally easy for a sender A, to generate the corresponding ciphertext :

$$C = E(PU_b, M)$$

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message :

$$M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$$

4. It is computationally infeasible for an adversary, knowing the public key (PU_b) to determine the private key PR_b.
5. It is computationally infeasible for an adversary, knowing the public key (PU_b) and a ciphertext (C) to recover the original message (M).

3.1.1 Advantages and Disadvantages

- **Advantages of public key algorithm**
  1. Only the private key must be kept secret.
  2. The administration of keys on a network requires the presence of only a functional trusted TTP as opposed to an unconditionally trusted TTP.
  3. A private/public key pair remains unchanged for considerable long periods of time.
  4. There are many relatively efficient digital signature mechanisms as a result of asymmetric-key schemes.
  5. In a large network the number of keys necessary may be considerably smaller than in the symmetric-key scenario.
- **Disadvantages of public key algorithm**
  1. Slower throughput rates than the best known symmetric-key schemes.
  2. Large key size.
  3. No asymmetric-key scheme has been proven to be secure.
  4. Lack of extensive history.

3.1.2 Comparison between Public Key and Private Key Algorithm

Sr. No.	Symmetric key cryptography	Asymmetric key cryptography
1.	Same key is used for encryption and decryption.	One key for encryption and other key for decryption.
2.	Very fast.	Slower.
3.	Key exchange is big problem.	Key exchange is not a problem.
4.	Also called **secret key** encryption.	Also called **public key** encryption.
5.	The key must be kept secret.	One of the two keys must be kept secret.
6.	The sender and receiver must share the algorithm and the key.	The sender and receiver must each have one of the matched pair of keys.
7.	Size of the resulting encrypted text is usually same as or less than the original clear text size.	Size of the resulting encrypted text is more than the original clear text size.
8.	Cannot be used for digital signatures.	Can be used for digital signature.

Ex. 3.1.1 *Perform encryption and decryption using RSA algorithm for p = 17, q = 11, e = 7 and M = 2.*

Sol. : P = 17 q = 31 and e = 7

$$n = p \times q = 17 \times 31 = 527$$

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

$$= (17 - 1)(31 - 1) = 480$$

$$d = (1 + k\,\phi(n)) / e = (1 + 480k) / 7$$

$$= -959 / 7 = -137 \quad (\text{for } k = -2)$$

$$d = -137 \pmod{480} = 343$$

$$\text{Encryption } (C) = M^e \pmod{n} = 2^7 \pmod{527} = 128$$

$$\text{Decryption } M = C^d \pmod{n} = 128^{343} \pmod{527} = 2$$

- The intended receiver, in possession of the matching private key is able to invert the transformation.

$$X = D_{KR_b}(Y)$$

- An opponent, observing Y and having access to public key (KU_b), but not having access to private key (KR_b), must attempt to recover X. It is assumed that the opponent does have knowledge of the encryption (E) and decryption algorithms (D).
- Public key cryptography requires each user to have two keys : A public key used by anyone for encrypting messages to be sent to that user and a private key, which the user needs for decrypting messages.

Requirements for public key cryptography

1. It is computationally easy for a party B to generate a pair.
2. It is computationally easy for a sender A, to generate the corresponding ciphertext :

$$C = E(PU_b, M)$$

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message :

$$M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$$

4. It is computationally infeasible for an adversary, knowing the public key (PU_b) to determine the private key PR_b.
5. It is computationally infeasible for an adversary, knowing the public key (PU_b) and a ciphertext (C) to recover the original message (M).

3.1.1 Advantages and Disadvantages

- **Advantages of public key algorithm**

1. Only the private key must be kept secret.
2. The administration of keys on a network requires the presence of only a functional trusted TTP as opposed to an unconditionally trusted TTP.
3. A private/public key pair remains unchanged for considerable long periods of time.
4. There are many relatively efficient digital signature mechanisms as a result of asymmetric-key schemes.
5. In a large network the number of keys necessary may be considerably smaller than in the symmetric-key scenario.

- **Disadvantages of public key algorithm**

1. Slower throughput rates than the best known symmetric-key schemes.
2. Large key size.
3. No asymmetric-key scheme has been proven to be secure.
4. Lack of extensive history.

3.1.2 Comparison between Public Key and Private Key Algorithm

Sr. No.	Symmetric key cryptography	Asymmetric key cryptography
1.	Same key is used for encryption and decryption.	One key for encryption and other key for decryption.
2.	Very fast.	Slower.
3.	Key exchange is big problem.	Key exchange is not a problem.
4.	Also called **secret key** encryption.	Also called **public key** encryption.
5.	The key must be kept secret.	One of the two keys must be kept secret.
6.	The sender and receiver must share the algorithm and the key.	The sender and receiver must each have one of the matched pair of keys.
7.	Size of the resulting encrypted text is usually same as or less than the original clear text size.	Size of the resulting encrypted text is more than the original clear text size.
8.	Cannot be used for digital signatures.	Can be used for digital signature.

Ex. 3.1.1 *Perform encryption and decryption using RSA algorithm for $p = 17$, $q = 11$, $e = 7$ and $M = 2$.*

Sol. : P = 17 q = 31 and e = 7

$$n = p \times q = 17 \times 31 = 527$$

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

$$= (17 - 1)(31 - 1) = 480$$

$$d = (1 + k\,\phi(n)) / e = (1 + 480k) / 7$$

$$= -959 / 7 = -137 \quad \text{(for } k = -2\text{)}$$

$$d = -137 \pmod{480} = 343$$

$$\text{Encryption } (C) = M^e \pmod{n} = 2^7 \pmod{527} = 128$$

$$\text{Decryption } M = C^d \pmod{n} = 128^{343} \pmod{527} = 2$$

- The intended receiver, in possession of the matching private key is able to invert the transformation.

$$X = D_{KR_b}(Y)$$

- An opponent, observing Y and having access to public key (KU_b), but not having access to private key (KR_b), must attempt to recover X. It is assumed that the opponent does have knowledge of the encryption (E) and decryption algorithms (D)
- Public key cryptography requires each user to have two keys : A public key used by anyone for encrypting messages to be sent to that user and a private key, which the user needs for decrypting messages.

Requirements for public key cryptography

1. It is computationally easy for a party B to generate a pair.
2. It is computationally easy for a sender A, to generate the corresponding ciphertext :

$$C = E(PU_b, M)$$

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message :

$$M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$$

4. It is computationally infeasible for an adversary, knowing the public key (PU_b) to determine the private key PR_b.
5. It is computationally infeasible for an adversary, knowing the public key (PU_b) and a ciphertext (C) to recover the original message (M).

3.1.1 Advantages and Disadvantages

- **Advantages of public key algorithm**
  1. Only the private key must be kept secret.
  2. The administration of keys on a network requires the presence of only a functional trusted TTP as opposed to an unconditionally trusted TTP.
  3. A private/public key pair remains unchanged for considerable long periods of time.
  4. There are many relatively efficient digital signature mechanisms as a result of asymmetric-key schemes.
  5. In a large network the number of keys necessary may be considerably smaller than in the symmetric-key scenario.
- **Disadvantages of public key algorithm**
  1. Slower throughput rates than the best known symmetric-key schemes.
  2. Large key size.
  3. No asymmetric-key scheme has been proven to be secure.
  4. Lack of extensive history.

3.1.2 Comparison between Public Key and Private Key Algorithm

Sr. No.	Symmetric key cryptography	Asymmetric key cryptography
1.	Same key is used for encryption and decryption.	One key for encryption and other key for decryption.
2.	Very fast.	Slower.
3.	Key exchange is big problem.	Key exchange is not a problem.
4.	Also called secret key encryption.	Also called public key encryption.
5.	The key must be kept secret.	One of the two keys must be kept secret.
6.	The sender and receiver must share the algorithm and the key.	The sender and receiver must each have one of the matched pair of keys.
7.	Size of the resulting encrypted text is usually same as or less than the original clear text size.	Size of the resulting encrypted text is more than the original clear text size.
8.	Cannot be used for digital signatures.	Can be used for digital signature.

Ex. 3.1.1 *Perform encryption and decryption using RSA algorithm for p = 17, q = 11, e = 7 and M = 2.*

Sol. : P = 17 q = 31 and e = 7

$$n = p \times q = 17 \times 31 = 527$$

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

$$= (17 - 1)(31 - 1) = 480$$

$$d = (1 + k\,\phi(n)) / e = (1 + 480k) / 7$$

$$= -959 / 7 = -137 \quad \text{(for } k = -2\text{)}$$

$$d = -137 \pmod{480} = 343$$

$$\text{Encryption (C)} = M^e \pmod{n} = 2^7 \pmod{527} = 128$$

$$\text{Decryption M} = C^d \pmod{n} = 128^{343} \pmod{527} = 2$$

Review Questions

1. *Explain various public key distribution approaches.*
2. *What are different approaches of public key distribution ? Explain any one.*
3. *Compare between symmetric key encryption and asymmetric key encryption.*

3.2 RSA Algorithm

- RSA is a block cipher in which the plaintext and ciphertext are integers between 0 and n – 1 for some n.
- A typical size for n is 1024 bits.
- The RSA algorithm developed in 1977 by Rivest, Shamir, Adleman (RSA) at MIT. RSA algorithm is public key encryption type algorithm. In this algorithm, one user uses a public key and other user uses a secret (private key) key.
- In the RSA algorithm each station independently and randomly chooses two large primes p and q number, and multiplies them to produce n = pq which is the modulus used in the arithmetic calculations of the algorithm.
- The details of the RSA algorithm are described as follows :
- **Key generation :**
  1) Pick two large prime numbers p and q, $p \neq q$;
  2) Calculate $n = p \times q$;
  3) Calculate $\phi(n) = (p - 1)(q - 1)$;
  4) Pick e, so that gcd $(e, \phi(n)) = 1$, $1 < e < \phi(n)$;
  5) Calculate d, so that $d \cdot e \bmod \phi(n) = 1$, i.e. d is the multiplicative inverse of e in mod $\phi(n)$;
  6) Get public key as $K_U = \{e, n\}$;
  7) Get private key as $K_R = \{d, n\}$.
- **Encryption :**

For plaintext block $P < n$, its ciphertext $C = P^e \bmod n$.

- **Decryption :**

For ciphertext block C, its plaintext is $P = C^d \bmod n$.

Why RSA works :

- As we have seen from the RSA design, RSA algorithm uses modular exponentiation operation. For $n = p \cdot q$, e which is relatively prime to $\phi(n)$, has exponential inverse in mod n.
- Its exponential inverse d can be calculated as the multiplicative inverse of e in mod $\phi(n)$. The reason is illustrated as follows :

Based on Euler's theorem, for y which satisfies $y \bmod \phi(n) = 1$, the following equation holds :

$$x^y \bmod n = x \bmod n$$

AS $d \cdot e \bmod \phi(n) = 1$, we have that $p^{ed} \equiv P \bmod n$. So the correctness of RSA cryptosystem is shown as follows :

- **Encryption :** $C = P^e \bmod n$;
- **Decryption :** $P = C^d \bmod n = (P^e)^d \bmod n = P^{ed} \bmod n = P \bmod n = P$.

Why RSA is secure :

- The premise behind RSA's security is the assumption that factoring a big number (n into p and q) is hard. And thus it is difficult to determine $\phi(n)$. Without the knowledge of $\phi(n)$, it would be hard to derive d based on the knowledge of e.

Advantages

1. RSA can be used both for encryption as well as for digital signatures.
2. Trapdoor in RSA is in knowing value of n but not knowing the primes that are factors of n.

Disadvantages

1. If any one of p, q, m, d is known, then the other values can be calculated. So secrecy is important.
2. To protect the encryption, the minimum number of bits in n should be 2048.

3.2.1 Attacks on RSA

Attacks on RSA algorithm are as follows :

1. **Brute force :** This involves trying all possible private keys.
2. **Mathematical attacks :** This involves the factoring the product of two primes.
3. **Timing attacks :** These depends on the running time of the description algorithm.
4. **Chosen ciphertext attacks :** This type of attack exploits properties of the RSA algorithm.

3.2.1.1 Computing $\phi(n)$

- Computing $\phi(n)$ is no easier that factoring n. For, if n and $\phi(n)$ are known, and n is the product of two primes p, q, then n can be easily factored, by solving the two equations.

$$n = pq \quad \ldots (3.2.1)$$

$$\phi(n) = (p - 1)(q - 1) \quad \ldots (3.2.2)$$

for the two unknowns p and q.

- If we substitute $q = n/p$ into the equation (3.2.2), we obtain a quadratic equation in the unknown value p :

$$p^2 - (n - \phi(n) + 1)\, p + n = 0 \quad \ldots (3.2.3)$$

- The two roots of equation (3.2.3) will be p and q, the factors of n. If a cryptanalyst can learn the value of $\phi(n)$, then he can factor 'n' and break the system.

3.2.1.2 Timing Attacks

- Kocher described a new attack on RSA in 1995.
- If the attacker Eve knows Alice's hardware in sufficient detail and is able to measure the decryption times for several known cipher-texts, she can deduce the decryption key (d) quickly. This attack can also be applied against the RSA signature scheme.
- In 2003, Boneh and Brumley demonstrated a more practical attack capable of recovering RSA factorizations over a network connection. This attack takes advantage of information leaked by the Chinese remainder theorem optimization used by many RSA implementations.
- One way to thwart these attacks is to ensure that the decryption operation takes a constant amount of time for every cipher-text. However, this approach can significantly reduce performance.
- There is simple counter-measures against timing attacks :

1. **Constant exponentiation time :** Ensure that all exponentiations take the same time, but this will degrade performance.
2. **Random delay :** Better performance could be achieved by adding a random delay to the exponentiation algorithm to confuse the timing attack.
3. **Blinding :** Multiply the cipher-text by a random number before performing exponentiation. This process prevents the attacker from knowing what cipher-text bits are being processed inside the computer and therefore prevents the bit-by-bit analysis essential to the timing attack. RSA data security reports a 2 % to 10 % performance penalty for blinding.

3.2.1.3 Mathematical Attacks

- We can identify three approaches to attacking RSA mathematically :

1. Factor n into two prime factors, this enables calculation of $\phi(n) = (p - 1)(q - 1)$, which in turn, enables determination of $d = e^{-1} \bmod \phi(n)$.
2. Determine $\phi(n)$ directly, without first determining p and q.
3. Determine d directly, without first determining $\phi(n)$.

- Most discussions of cryptanalysis of RSA have focused on the task of factoring n into its two prime numbers. Determining $\phi(n)$ given n is equivalent to factoring n.
- With presently known algorithms, determining d given e and n appears to at least as time consuming as the factoring problem.

3.2.1.4 Adaptive Chosen Cipher-text Attacks

- In 1998, Daniel Bleichenbacher described the first practical adaptive chosen cipher-text attack, against RSA-encrypted messages using the PKCS#1 v1 padding scheme.
- Due to flaws with the PKCS#1 scheme, Bleichenbacher was able to mount a practical attack against RSA implementations of the Secure Socket Layer protocol and to recover session keys.
- As a result of this work, cryptographers now recommend the use of provably secure padding schemes such as Optimal Asymmetric Encryption padding and RSA laboratories has released new versions of PKCS#1 that are not vulnerable to these attacks.

Ex. 3.2.1 *For the given values $p = 19$, $q = 23$ and $e = 3$ find n, $\phi(n)$ and d using RSA algorithm.*

Sol. :

$$n = p * q$$

$$n = 19 \times 23$$

$$n = 437$$

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

$$\phi(n) = 18 \times 22$$

$$\phi(n) = 396$$

$$e.d. = 1 \bmod \phi(n)$$

$$3d = 1 \bmod 396$$

$$n = pq \quad \ldots (3.2.1)$$

$$\phi(n) = (p - 1)(q - 1) \quad \ldots (3.2.2)$$

for the two unknowns p and q.

- If we substitute $q = n/p$ into the equation (3.2.2), we obtain a quadratic equation in the unknown value p :

$$p^2 - (n - \phi(n) + 1)p + n = 0 \quad \ldots (3.2.3)$$

- The two roots of equation (3.2.3) will be p and q, the factors of n. If a cryptanalyst can learn the value of $\phi(n)$, then he can factor 'n' and break the system.

3.2.1.2 Timing Attacks

- Kocher described a new attack on RSA in 1995.
- If the attacker Eve knows Alice's hardware in sufficient detail and is able to measure the decryption times for several known cipher-texts, she can deduce the decryption key (d) quickly. This attack can also be applied against the RSA signature scheme.
- In 2003, Boneh and Brumley demonstrated a more practical attack capable of recovering RSA factorizations over a network connection. This attack takes advantage of information leaked by the Chinese remainder theorem optimization used by many RSA implementations.
- One way to thwart these attacks is to ensure that the decryption operation takes a constant amount of time for every cipher-text. However, this approach can significantly reduce performance.
- There is simple counter-measures against timing attacks :
  1. **Constant exponentiation time :** Ensure that all exponentiations take the same time, but this will degrade performance.
  2. **Random delay :** Better performance could be achieved by adding a random delay to the exponentiation algorithm to confuse the timing attack.
  3. **Blinding :** Multiply the cipher-text by a random number before performing exponentiation. This process prevents the attacker from knowing what cipher-text bits are being processed inside the computer and therefore prevents the bit-by-bit analysis essential to the timing attack. RSA data security reports a 2 % to 10 % performance penalty for blinding.

3.2.1.3 Mathematical Attacks

- We can identify three approaches to attacking RSA mathematically :
  1. Factor n into two prime factors, this enables calculation of $\phi(n) = (p - 1)(q - 1)$, which in turn, enables determination of $d = e^{-1} \bmod \phi(n)$.
  2. Determine $\phi(n)$ directly, without first determining p and q.
  3. Determine d directly, without first determining $\phi(n)$.
- Most discussions of cryptanalysis of RSA have focused on the task of factoring n into its two prime numbers. Determining $\phi(n)$ given n is equivalent to factoring n.
- With presently known algorithms, determining d given e and n appears to at least as time consuming as the factoring problem.

3.2.1.4 Adaptive Chosen Cipher-text Attacks

- In 1998, Daniel Bleichenbacher described the first practical adaptive chosen cipher-text attack, against RSA-encrypted messages using the PKCS#1 v1 padding scheme.
- Due to flaws with the PKCS#1 scheme, Bleichenbacher was able to mount a practical attack against RSA implementations of the Secure Socket Layer protocol and to recover session keys.
- As a result of this work, cryptographers now recommend the use of provably secure padding schemes such as Optimal Asymmetric Encryption padding and RSA laboratories has released new versions of PKCS#1 that are not vulnerable to these attacks.

Ex. 3.2.1 *For the given values p = 19, q = 23 and e = 3 find n, $\phi(n)$ and d using RSA algorithm.*

Sol. :

$$n = p * q$$

$$n = 19 \times 23$$

$$n = 437$$

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

$$\phi(n) = 18 \times 22$$

$$\phi(n) = 396$$

$$e.d. = 1 \bmod \phi(n)$$

$$3d = 1 \bmod 396$$

$$d = \frac{1}{3}$$

Ex. 3.2.2 *Using the RSA algorithm, encrypt the following :*
i) p = 3, q = 11, e = 7, M = 12
ii) p = 7, q = 11, e = 17, M = 25
iii) Find the corresponding ds for i) and ii) and decrypt the ciphertext.

Sol. : i)

$$n = p * q$$

$$n = 3 * 11 = 33$$

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

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

$$e \cdot d = 1 \bmod \phi(n)$$

$$7 \cdot d = 1 \bmod 20$$

$$d = 3$$

Ciphertext (C) $= M^e \bmod n$

$$= 12^7 \bmod 33$$

$$C = 12$$

ii)

$$n = p * q = 7 * 11 = 77$$

$$\phi(n) = (p - 1) * (q - 1) = 6 \times 10 = 60$$

$$e \cdot d = 1 \bmod \phi(n) \Rightarrow 17\ d = 1 \bmod 77$$

$$d = 3$$

Ciphertext (C) $= M^e \bmod n$

$$= 25^{17} \bmod 77 \Rightarrow 77 \Rightarrow c = 9$$

$$C = 12$$

iii) Decryption :

$$M = c^d \bmod n$$

In case (i) $M = 12^3 \bmod 33 = 12$

In case (ii) $M = 9^{57} \bmod 77 = 25$

Ex. 3.2.3 *In RSA system the public key of a given user is e = 7 and n = 187*
i) What is the private key of this user ?
ii) If the intercepted ciphertext is c = 11 and sent to a user whose public key is e = 7 and n = 187. What is the plaintext ?
iii) What are the possible approaches to defeating the RSA algorithm ?

Sol. : i) $n = p * q$

$$n = 11 \times 17 \Rightarrow 187$$

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

$$= (17 - 1)(11 - 1) = 16 \times 10 = 160$$

$$e \cdot d = 1 \bmod \phi(n)$$

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

$$7 \times 23 = 1 \bmod 160$$

Public key PU

$$(e, n) = 7, 187$$

Private key PR

$$(d, n) = 23, 187$$

ii) $c = 11,\ e = 7,\ n = 187$

Plaintext $p = c^d \bmod n$

$$= 11^{23} \bmod 187$$

$$= 79720245 \bmod 187$$

$\therefore$ Plaintext = 88

Ex. 3.2.4 *Explain about the RSA algorithm with example as : p = 11, q = 5, e = 3 and PT = 9*

Sol. : $p = 11,\ q = 5$

$$n = p*q = 11\times5 = 55$$

$$\phi(n) = (p-1)*(q-1) = 10*4$$

$$= 40$$

$$e = 3 \text{ and } m = 9$$

$$\gcd(\phi(n),(e) = \gcd(40, 3) = 1$$

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

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

$$3d \bmod 40 = 1$$

$$d = 27$$

public key $pu = \{e, n\} = \{3, 55\}$

private key $pr = \{d, n\} = \{27, 55\}$

Encryption : $C = M^e \bmod n$

$$= 9^3 \bmod 55 = 14$$

decryption : $M = c^d \bmod n$

$$M = 14^{27} \bmod 55 = 9$$

Ex. 3.2.5 *Perform encryption and decryption using RSA algorithm. p = 7, q = 11, e = 17 and M = 8.*

Sol. : RSA algorithm :

$$N = p \times q$$
$$= 7 \times 11$$
$$= 77$$

Calculate $\phi(n) = (p - 1)(q - 1)$
$$= (7 - 1)(11 - 1)$$
$$= 6 \times 10$$
$$= 60$$

So, $e = 17$

Determine d such that

$$ed = 1 \bmod \phi(n)$$
$$17d = 1 \bmod 60$$

According to GCD :

$$60 = 17 * 3 + 9$$
$$17 = 9 * 1 + 8$$
$$9 = 8 * 1 + 1$$
$$8 = 1 * 8 + 0$$

Therefore, we have :

$$1 = 9 - 8$$
$$= 9 - (17 - 9)$$
$$= 9 - (17 - (60 - 17 * 3))$$
$$= 60 - 17 * 3 - (17 - 60 + 17 * 3)$$
$$= 60 - 17 * 3 + 60 - 17 * 4$$
$$= 60 * 2 - 17 * 7$$

Hence, we get,

$$d = e^{-1} \bmod f(n)$$
$$= e^{-1} \bmod 60$$
$$= -7 \bmod 60$$
$$= (53 - 60) \bmod 60$$
$$= 53$$

So, the public key is {17, 77} and the private key is {53, 77}

Encryption :

Ciphertext (C) $= M^e \bmod N$
$$= (8)^{17} \bmod 77$$
$$C = 57$$

Ex. 3.2.6 *In a public key cryptosystem using RSA, given N = 187 and the encryption key (E) as 17, find out the corresponding private key (D).*

Sol. : $N = 187$

$N = p \times q = 17 \times 11$

$N = 187$

So $p = 17, \quad q = 11$

$\phi(n) = (p - 1) \times (q - 1)$
$= (17 - 1) \times (11 - 1) = 160$

$ED = 1 \bmod \phi(n)$

$17\ d = 1 \bmod 160$

$d = 113$

Ex. 3.2.7 *Let the given data be - Prime numbers p = 11, q = 19 and the plain text to be sent is 4. Assume public key e as 23. Using RSA algorithm determine the cipher text for the given plain text. Also perform the reverse process of finding the plain text. Also perform the reverse process of finding the plain text from the cipher text.*

Sol. : Given p = 11, q = 19, plain text (m) = 40,

Public key e = 23

$n = p \times q = 11 \times 19 = 209$

$\phi(n) = (p - 1) \times (q - 1)$
$= (11 - 1) \times (19 - 1) = 180$

Encryption :

$C = M^e \pmod n$
$= (40)^{23} \bmod 180$
$C = 160$

pretty good privacy (PGP)

Ex. 3.2.8 : *For the given parameters 'P' = 3 and 'Q' = 19 find the value of 'e' and 'd' using RSA algorithm and encrypt message 'M' = 6.*

Sol. : P = 3 Q = 19

$N = PQ$

$= 3 \times 19$

$N = 57$

Calculate $\phi(n) = (P - 1)(Q - 1)$

$= (3 - 1)(19 - 1)$

$= 36$

Public key 'e' is calculated by using Euclid algorithm. Using 36, GCD is calculated and 5 and 7 gives GCD = 1

So you can select e = 5 or 7. Here we selected e = 7

So public key (7, 57)

Private key generation (d) :

Determine d such that $ed = 1 \bmod \phi(n)$

$7d = 1 \pmod{36}$

$7 \times 31 = 1 \pmod{36}$

So d = 31

Encryption of message :

Ciphertext (C) $= M^e \bmod n$

$= 6^7 \bmod 57$

$C = 9$

Ex. 3.2.9 : *Use RSA algorithm to encrypt the plaintext "3" use following parameters p = 11, q = 3, e = 13.*

Sol. : p = 11, q = 3, e = 13

Plaintext = 3

$N = p \times q = 11 \times 3 = 33$

$\phi(n) = (p - 1)(q - 1) = (11 - 1)(3 - 1) = 20$

Given e = 13;

Determine d such that

$ed = 1 \bmod \phi(n)$

$13d = 1 \bmod 20$

$13 \times 17 = 1 \bmod 20$

$221 = 1 \bmod 20$

So $d = 17$

Ciphertext $(C) = M^e \bmod (n)$

$C = 3^{13} \bmod 33$

$C = 27$

Review Questions

1. *For the given parameters 'P' = 3 and 'Q' = 19 find the value of 'e' and 'd' using RSA algorithm and encrypt message 'M' = 6.*
2. *What is public key cryptography ? Explain RSA algorithm used for public key cryptography.*
3. *Use RSA algorithm to encrypt the plaintext "3" use following parameters p = 11, q = 3, e = 13.*
4. *Explain RSA algorithm with suitable example.*
5. *Explain operation of RSA public key encryption algorithm.*

3.3 Key Distribution

- The purpose of public key cryptography is
  1. The distribution of public keys.
  2. The use of public key encryption to distribute secret keys.

3.3.1 Distribution of Public Keys

- Different methods have been proposed for the distribution of public keys. These are
  1. Public announcement.
  2. Publicly available directory.
  3. Public key authority.
  4. Public key certificates.

1. Public announcement

- In public key algorithm, any participant can **send** his or her public key to any other participant or **broadcast** the key to the community at large.
- Fig. 3.3.1 shows the public key distribution.
- Because of the growing popularity of PGP, which makes use of RSA, many PGP users have adopted the practice of appending their public key to messages that they send to public forums, such as USENET newgroups and Internet mailing lists.

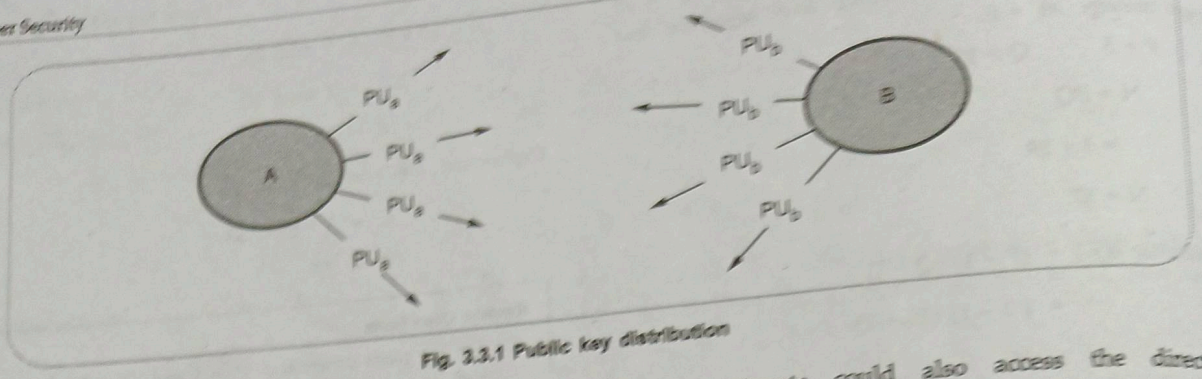


Fig. 3.3.1 Public key distribution

- The disadvantage is that, anyone can forge such a public announcement. That is, some user could pretend to be user A and send a public key to another participant or broadcast such a public key.

2. Public available directory

- Greater degree of security can be achieved by maintaining a publicly available dynamic directory of public keys. Maintenance and distribution of the public directory would have to be the responsibility of some trusted entity or organization.
- Fig. 3.3.2 shows public key publication.
- Such a scheme would include the following elements :

1. The authority maintains a directory with a {name, public key} entry for each participant.
2. Each participant registers a public key with the directory authority. Registration would have to be in person or by some form of secure authenticated communication.
3. A participant may replace the existing key with a new one at any time.
4. Participants could also access the directory electronically.

3. Public key authority

- Fig. 3.3.3 shows public key distribution scenario. (See Fig. 3.3.3 on next page)
- Following steps occur in public key distribution.

1. A sends a timestamped message to the public key authority containing a request for the current public key of B.
2. The authority responds with a message that is encrypted using the authority's private key, PR_{auth}. The message also contains B's public key (PU_b), original request and timestamp.
3. A stores B's public key and also uses it to encrypt a message to B containing an identifier of A (ID_A) and a nonce (N_1) which is used to identify this transaction uniquely.
4. B retrieves A's public key from the authority in the same manner as A retrieved B's public key.
5. Public keys have been securely delivered to A and B and they may begin their protected exchange.

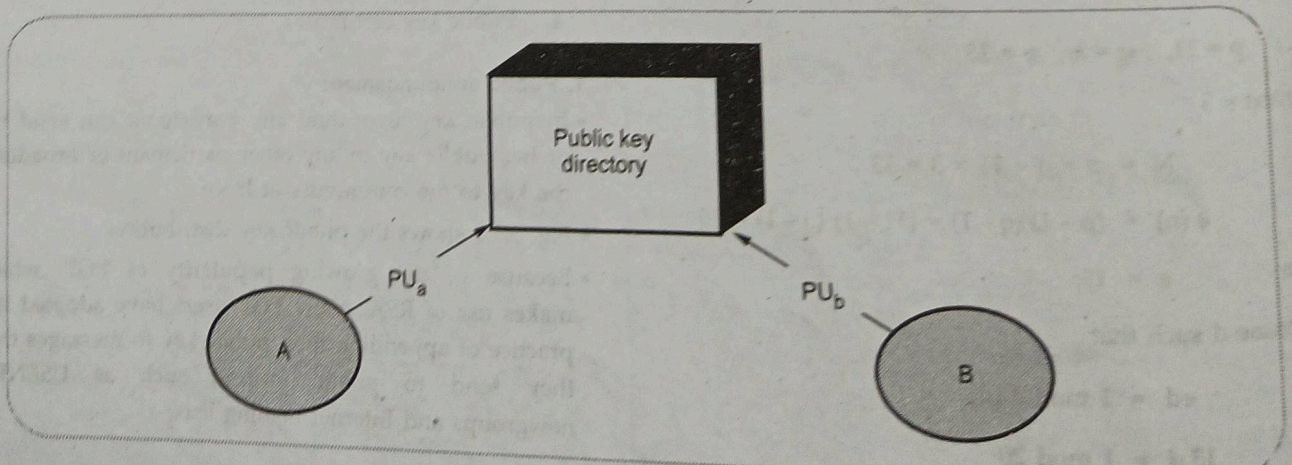


Fig. 3.3.2 Public key publication

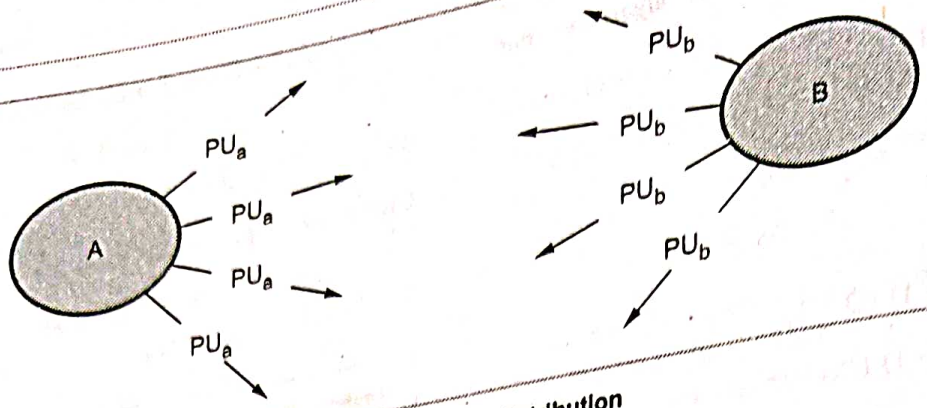


Fig. 3.3.1 Public key distribution

- The disadvantage is that, anyone can forge such a public announcement. That is, some user could pretend to be user A and send a public key to another participant or broadcast such a public key.

2. Public available directory

- Greater degree of security can be achieved by maintaining a publicly available dynamic directory of public keys. Maintenance and distribution of the public directory would have to be the responsibility of some trusted entity or organization.
- Fig. 3.3.2 shows public key publication.
- Such a scheme would include the following elements :

1. The authority maintains a directory with a {name, public key} entry for each participant.
2. Each participant registers a public key with the directory authority. Registration would have to be in person or by some form of secure authenticated communication.
3. A participant may replace the existing key with a new one at any time.
4. Participants could also access the directory electronically.

3. Public key authority

- Fig. 3.3.3 shows public key distribution scenario. (See Fig. 3.3.3 on next page)
- Following steps occur in public key distribution.

1. A sends a timestamped message to the public key authority containing a request for the current public key of B.
2. The authority responds with a message that is encrypted using the authority's private key, PR_{auth}. The message also contains B's public key (PU_b), original request and timestamp.
3. A stores B's public key and also uses it to encrypt a message to B containing an identifier of A (ID_A) and a nonce (N_1) which is used to identify this transaction uniquely.
4. B retrieves A's public key from the authority in the same manner as A retrieved B's public key.
5. Public keys have been securely delivered to A and B and they may begin their protected exchange.

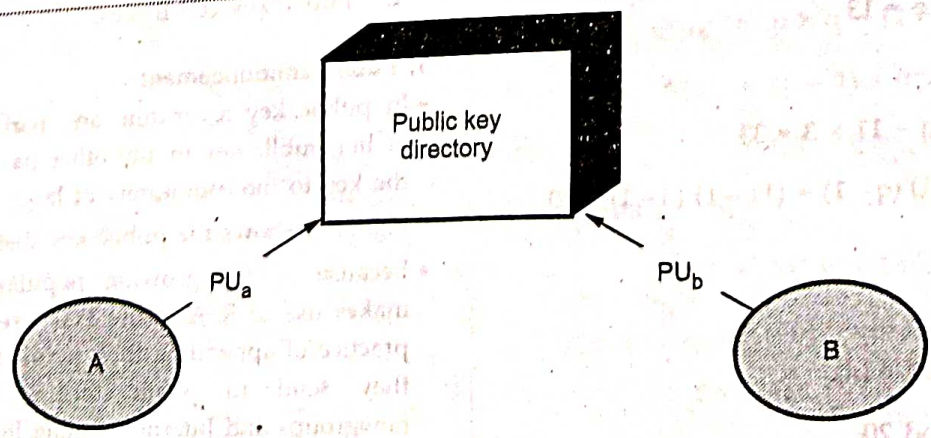


Fig. 3.3.2 Public key publication

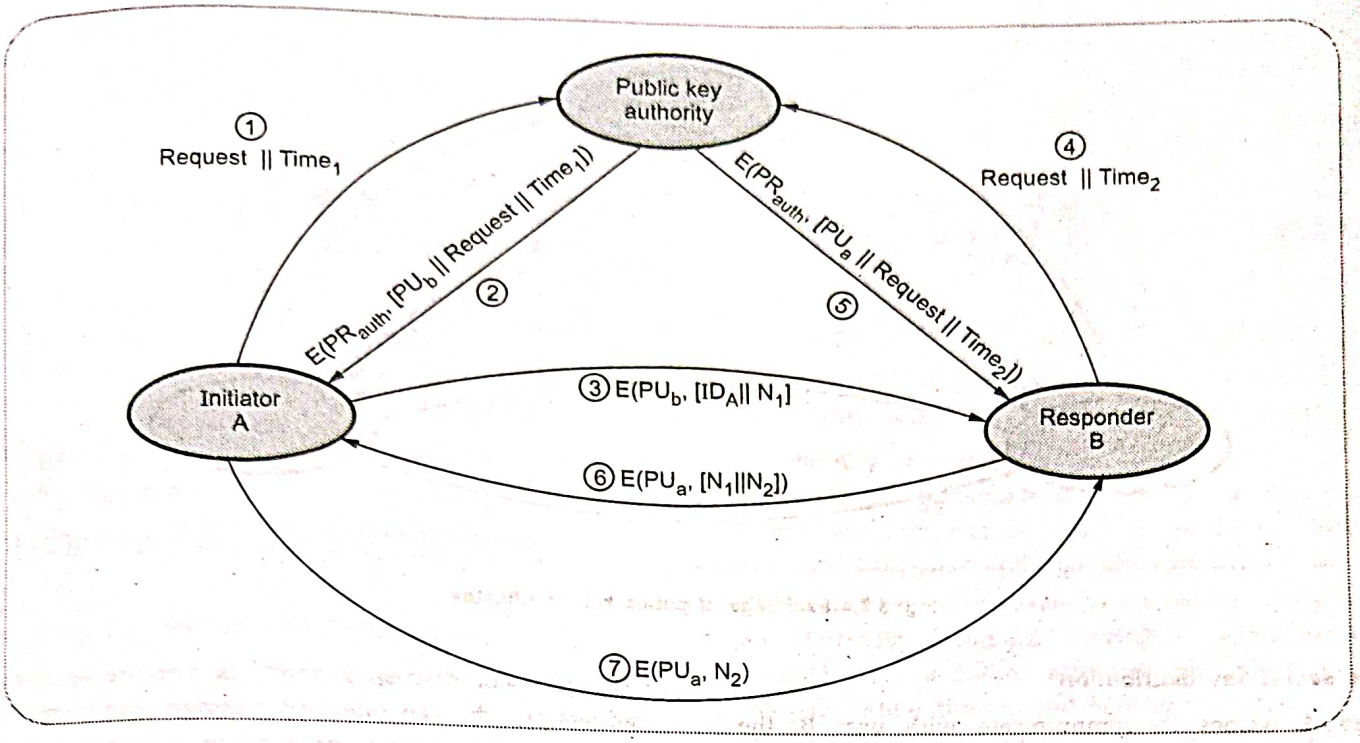


Fig. 3.3.3 Public key distribution scenario

6. B sends a message to A encrypted with PU_a and containing A's nonce (N_1) as well as a new nonce generated by B(N_2).
7. A returns N_2, encrypted using B's public key, to assure B that its correspondent is A.

Drawback

Public key authority could be somewhat of a bottleneck in the system. The directory of name and public keys maintained by the authority is vulnerable to tampering.

4. Public key certificates

- Certificates can be used by participants to exchange keys without contacting a public key authority. Certificate consists of a public key plus an identifier of the key owner, with the whole block signed by a trusted third party.
- The third party is a certificate authority, such as government agency or a financial institution, that is trusted by the user community.
- A user can present his or her public key to the authority in a secure manner, and obtain a certificate. The user can then publish the certificate.
- Requirements on this scheme :

1. Any participant can read a certificate to determine the name and public key of the certificate's owner.
2. Any participant can verify that the certificate originated from the certificate authority and is not counterfeit.
3. Only the certificate authority can create and update certificates.
4. Any participant can verify the currency of the certificate.

- A certificate scheme is illustrated in Fig. 3.3.4. Each participant applies to the certificate authority, supplying a public key and requesting a certificate.
- For participant A, the authority provides a certificate of the form

$$C_A = E(PR_{auth}, [T \| ID_A \| PU_a])$$

where PR_{auth} is the private key used by the authority and T is a timestamp.

3.3.2 Distribution of Secret Keys using Public Key Cryptography

- Public key encryption provides for the distribution of secret key to be used for conventional encryption.

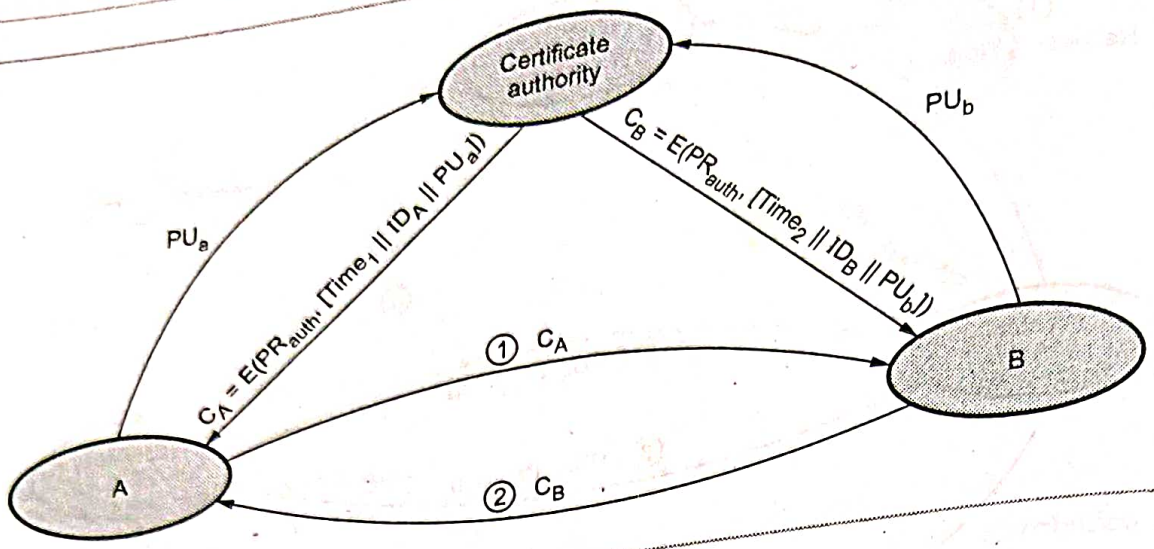


Fig. 3.3.4 Exchange of public key certificates

Simple secret key distribution

If user A wishes to communicate with user B, the following procedure is employed :

1. User A generates a public/private key pair {PU_a, PR_a} and transmits a message to user B consisting of PU_a and an identifier of A, ID_A.
2. User B generates a secret key (K_s) and transmits it to user A, encrypted with A's public key.
3. User A computes $D(PR_a, E(PU_a, K_s))$ to recover the secret key. Because only A can decrypt the message, only user A and user B know the identity of K_s.
4. User A discards PU_a and PR_a and user B discards PU_a.
5. Fig. 3.3.5 shows use of public key encryption.

- User A and B can now securely communicate using conventional encryption and the session key K_s. At the completion of the exchange, both user A and B discard K_s.
- The protocol discussed above is insecure against a adversary who can intercept messages and then eith relay the intercepted message or substitute anoth message. Such an attack is known as a **man in midd attack.**

Secret key distribution with confidentiality an authentication

- Fig. 3.3.6 shows the public key distribution of secr keys. (See Fig. 3.3.6 on next page.)
- It provides protection against both passive and activ attacks.

1. A uses B's public key to encrypt a message to B containing an identifier of A (ID_A) and a nonce (N_1), which is used to identify this transaction uniquely.
2. B sends a message to A encrypted with PU_a and containing A's nonce (N_1) as well as a new nonce generated by B(N_2).
3. A returns N_2, encrypted using B's public key, to assure B that its correspondent is A.

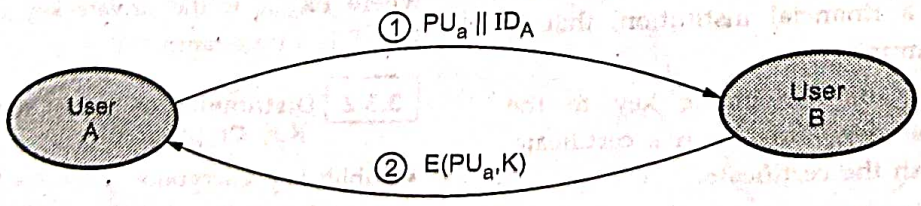


Fig. 3.3.5 Use of public key encryption

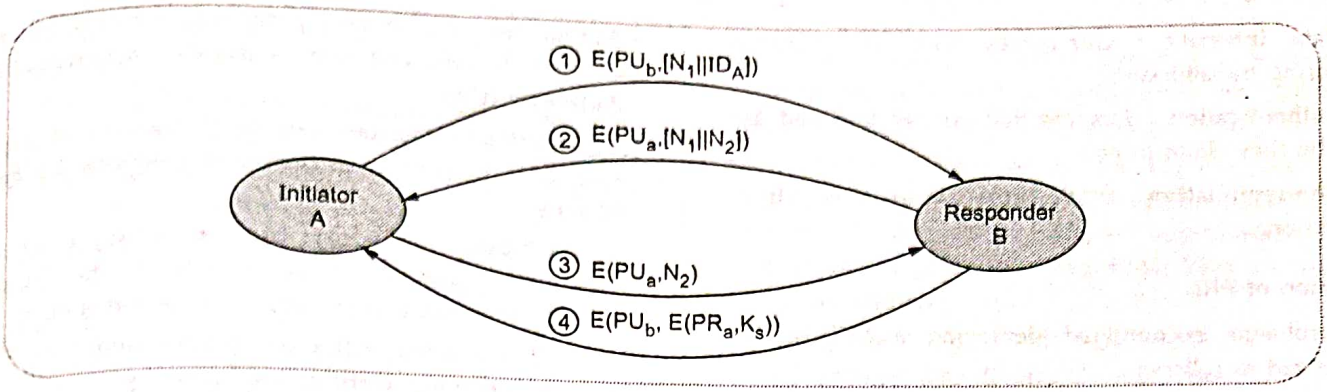


Fig. 3.3.6 Public key distribution of secret keys

4. A selects a secret key K_s and sends $M = E(PU_b, E(PR_a, K_s))$ to B.
5. B computes $D(PU_a, D(PR_b, M))$ to recover the secret key.

3.3.3 Key Distribution and Certification

- Management and handling of the pieces of secret information is generally referred to as **key management.**
- Activities of key management includes selection, exchange, storage, certification, revocation, changing, expiration and transmission of the key.
- Key management is the set of processes and mechanisms which support key establishment and maintenance of ongoing keying relationship between parties, including replacing older key with new keys.
- Two major issues in key management are :

1. Key life time 2. Key exposure

Key life time - limit of use which can be measured as a duration of time.

Issue related to key :

1. Users must be able to obtain securely a key pair suited to their efficiency and security needs.
2. Keys need to be valid only until a specified expiration date.
3. The expiration date must be chosen properly and publicized securely.
4. User must be able to store their private keys securely.
5. Certificates must be unforgettable, obtainable in a secure manner.

1. Public Key Infrastructure

- Public Key Infrastructure (PKI) is a well-known technology that can be used to establish identities, encrypt information and digitally sign documents.
- PKI identifies and manages relationships of parties in an electronic exchange, serving a wide array of security needs including access control, confidentiality, integrity, authentication and non-repudiation.
- PKI also uses unique Digital Certificates (DC) to secure eCommerce, email, data exchange and Virtual Private Networks (VPN) and intranets and is also used to verify the identity and privileges of each user.
- The Certificate Authority (CA) provides a full life-cycle management of public keys and certificates, including issuance, authentication, storage, retrieval, backup, recovery, updating and revocation to the PKI.
- All users of PKI must have a registered identity, which is stored in a digital certificate issued by a CA.
- Remote users and sites using public private keys and public key certificates can authenticate each other with a high degree of confidence.
- Authentication is dependent on three conditions :
  1. It must be established that each party have a private key that has not been stolen or copied from the owner.
  2. The certificate must be issued to the owner in accord with the stated policy of the certificate issuer.
  3. The policies of the certificate issuer must be satisfactory to the parties so as to verify identity.

Benefits of PKI

1. **Confidential communication :** Only intended recipients can read files.

2. **Data integrity** : Guarantees files are unaltered during transmission.
3. **Authentication** : Ensures that parties involved are who they claim to be.
4. **Non-repudiation** : Prevents individuals from denying.

Limitation of PKI

The problems encountered deploying a PKI can be categorized as follows :

1. Public key infrastructure is new
2. Lack of standards
3. Shortage of trained personnel
4. Public key infrastructure is mostly about policies.

2. Certificate

- **Certificates** are digital documents that are used for secure authentication of communicating parties.
- A certificate binds identity information about an entity to the entity's public key for a certain validity period.
- A certificate is digitally signed by a Trusted Third Party (TTP) who has verified that the key pair actually belongs to the entity.
- Certificates can be thought of as analogous to passports that guarantee the identity of their bearers.
- **Authorities** : The trusted party who issues certifica to the identified end entities is called a **Certificati Authority (CA).**
- Certification authorities can be thought of as bei analogous to governments issuing passports for th citizens.
- A certification authority can be managed by external certification service provider or the CA c belong to the same organization as the end entities.
- CAs can also issue certificates to other (sub) CAs. Th leads to a tree-like **certification hierarchy.**
- The highest trusted CA in the tree is called a root CA
- In large organizations, it may be appropriate delegate the responsibility for issuing certificates several different certificate authorities.
- For example, the number of certificates required ma be too large for a single CA to maintain; differe organizational units may have different polic requirements; or it may be important for a CA to b physically located in the same geographic area as th people to whom it is issuing certificates.
- The X.509 standard includes a model for setting up hierarchy of the certification authority.
- Fig. 3.3.7 shows the hierarchy of certificate authorities.
- In the Fig. 3.3.7, the root CA is at the top of th hierarchy. The root CA's certificate is a self-signe

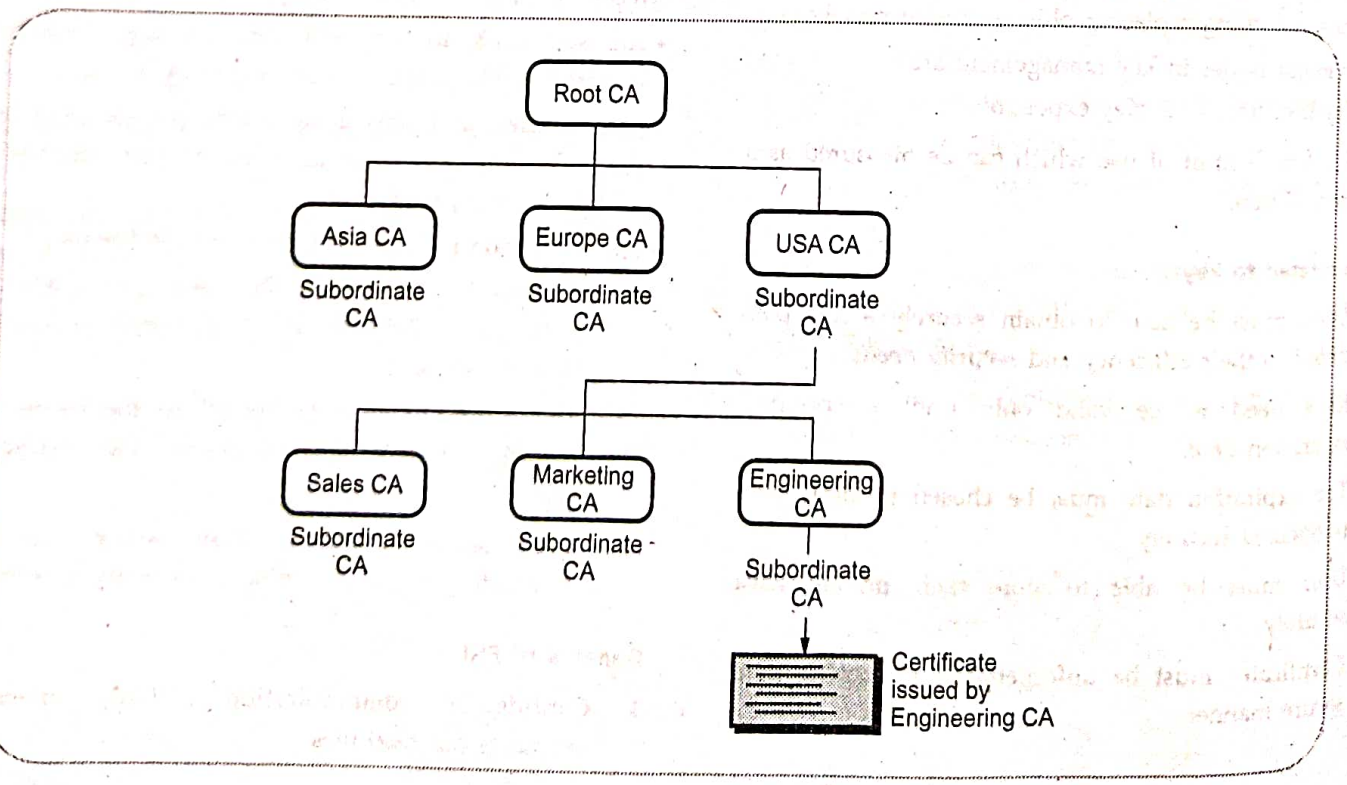


Fig. 3.3.7 Hierarchy of CA

certificate : That is, the certificate is digitally signed by the same entity.

- The CAs, that are directly subordinate to the root CA, have CA certificates signed by the root CA. CAs under the subordinate CAs in the hierarchy have their CA certificates signed by the higher-level subordinate CAs.
- Organizations have a great deal of flexibility in terms of the way they set up their CA hierarchies.
- **Certificate chains** : Certificate chain is series of certificates issued by successive CAs.
- In some cases, a CA can delegate the actual identification of end entities as well as some other administrative tasks to a separate entity, the **Registration Authority (RA).**

Verifying certificates

- When authentication is required, the entity presents a signatures it has generated from authentication data using its private key, and a certificate corresponding to that key.
- The receiving entity can verify the signature with the public key of the sender contained in the certificate.
- Next the receiving entity must verify the certificate itself by checking the validity time of the certificate and the signature of the CA in the certificate.
- If the CA is a sub CA, the receiving entity must also verify the signatures of all higher-level CAs up to the root CA.
- The list of certificates needed for verification is called a **certification path.**
- If all signatures are valid and the receiving entity trusts the root CA, the first entity will be authenticated successfully.
- If a private key of an end entity is compromised or the right to authenticate with a certificate is lost before its natural expiration date, the CA must revoke the certificate and inform all PKI users about this.
- The CA will periodically publish a **Certificate Revocation List (CRL).**
- The CRL is a list identifying the revoked certificates and it is signed by the CA.
- The end entities should check the latest CRL whenever they are verifying a validity of a certificate.

3. Key length and encryption strength

- The strength of encryption depends on both the cipher used and the length of the key.
- Encryption strength is often described in terms of the size of the keys used to perform the encryption : In general, longer keys provide stronger encryption.
- Key length is measured in bits. For example, 128-bit keys for use with the RC4 symmetric-key cipher supported by SSL provide significantly better cryptographic protection than 40-bit keys for use with the same cipher.
- Roughly speaking, 128-bit RC4 encryption is 3×10^{26} times stronger than 40-bit RC4 encryption.
- Different ciphers may require different key lengths to achieve the same level of encryption strength.
- The RSA cipher used for public-key encryption, for example, can use only a subset of all possible values for a key of a given length, due to the nature of the mathematical problem on which it is based.
- Other ciphers, such as those used for symmetric key encryption, can use all possible values for a key of a given length, rather than a subset of those values.
- Thus a 128-bit key for use with a symmetric key encryption cipher would provide stronger encryption than a 128-bit key for use with the RSA public-key encryption cipher.

3.3.4 Key Distribution

- For symmetric encryption to work, the two parties to an exchange must share the same key, and that key must be protected from access by others. **Key distribution** refers to the means of delivering a key to two parties who wish to exchange data, without allowing others to see the key.
- For two parties A and B, key distribution can be achieved in a number of ways, as follows.
  1. User A can select a key and physically deliver it to user B.
  2. A third party can select the key and physically deliver it to user A and user B.
  3. If user A and user B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
  4. If user A and user B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to user A and user B.
- For manual delivery of key, **options 1 and 2** are used. These options are suitable for **link encryption.**

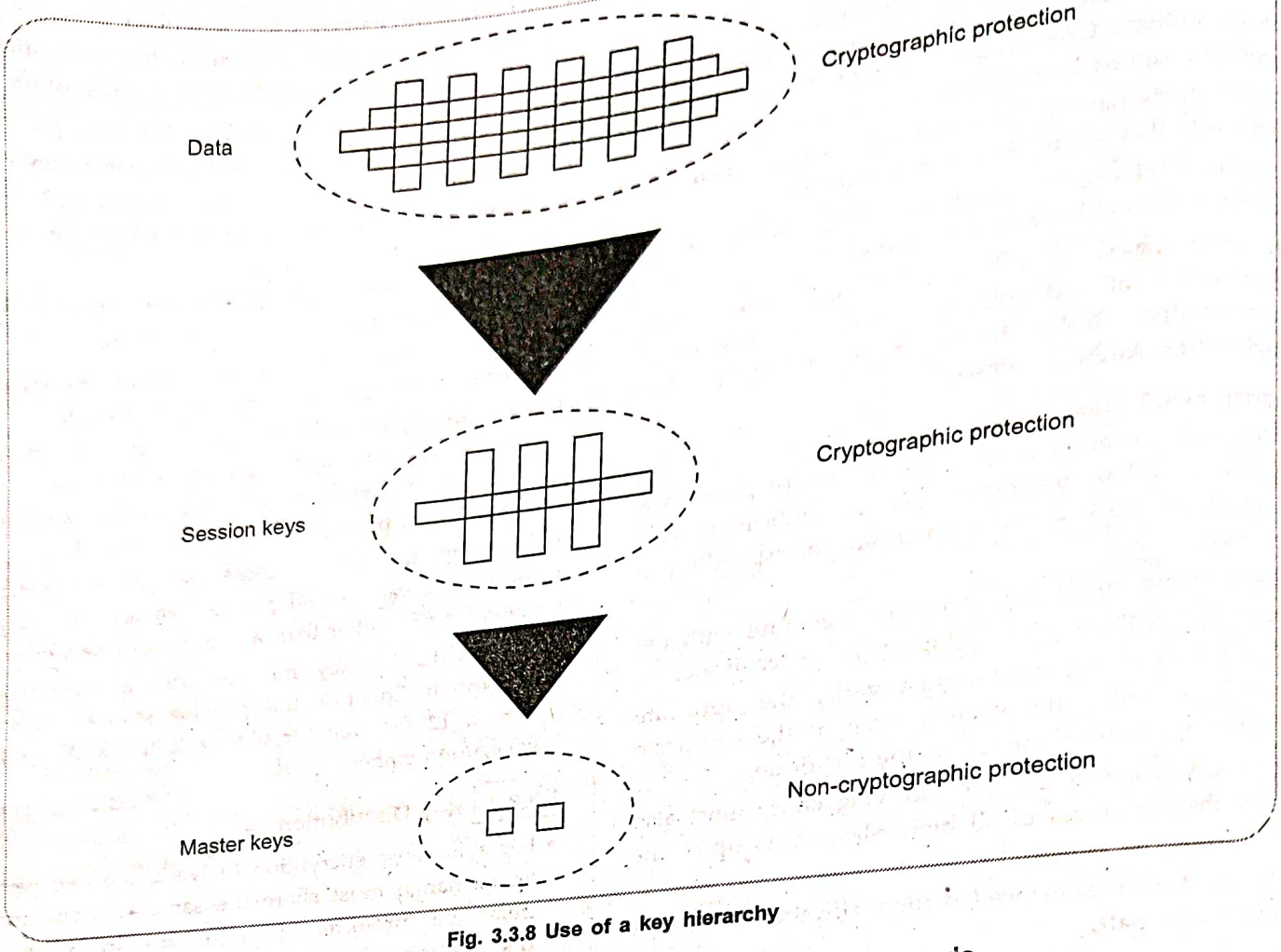


Fig. 3.3.8 Use of a key hierarchy

- Option 3 is suitable for link encryption or end-to-end encryption.
- For end-to-end encryption, some variation on option 4 has been widely adopted.
- The use of a key distribution center is based on the use of a hierarchy of keys. Minimum two levels of keys are used. Fig. 3.3.8 shows the use of a key hierarchy.
- Communication between end systems is encrypted using a temporary key, often referred to as a **session key**. The **session key** is used for the duration of a logical connection, such as a frame relay connection, or transport connection and then discarded.
- Session keys are transmitted in encrypted form; using a **master key** that is shared by the key distribution center and an end system or user. For each end user, there is a unique master key that it shares with the key distribution center.

A key distribution scenario

- User A wishes to establish a logical connection wit user B and requires a one time session key to prote the data transmitted over the connection. User A has master key (K_a), known only to itself and the KD User B shares the master key K_b with the KDC. Th following steps occur :

1. A issues a request to the KDC for a session ke to protect a logical connection to B. The messag includes the identity of A and B and a unique identifier (N_1) for this transaction.
2. KDC responds with a message encrypted using K_a.
3. A stores the session key for use in the upcoming session and forward to B the information that originated at the KDC for B :
4. User B sends a nonce N_2 to A.

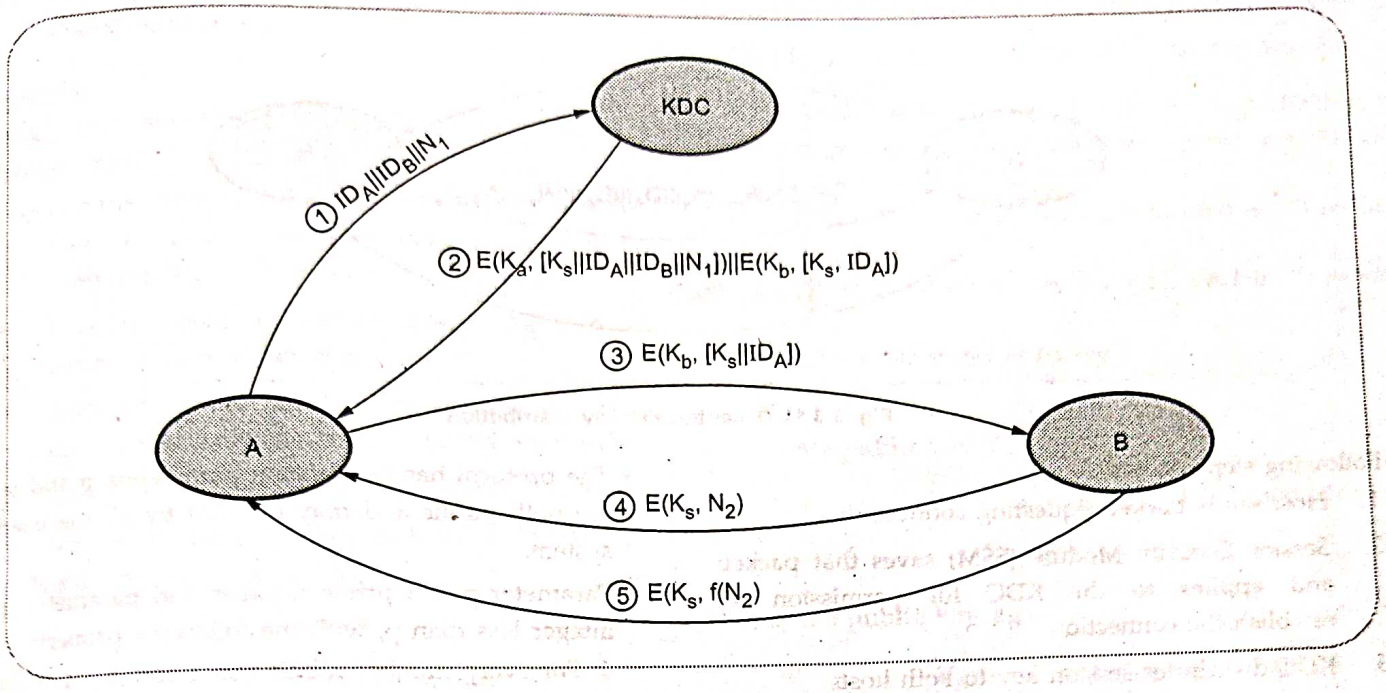


Fig. 3.3.9 Key distribution scenario

- Fig. 3.3.9 shows the key distribution scenario.
- Steps 1, 2 are used for key distribution and steps 3, 4, 5 for authentication.

Session key lifetime

1. **For connection-oriented protocol**
   - Use the same session key for the length of time that the connection is open. Use new session key for each new session.
   - For long lifetime, change the session key periodically.
2. **For connectionless protocol**
   - The most secure approach is to use a new session key for each exchange. For connectionless protocol, such as a transaction-oriented protocol, there is no explicit connection initiation or termination.

Transparent key control scheme

- Fig. 3.3.10 shows automatic key distribution for connection - oriented protocol.
- Assume that communication make use of a connection-oriented end-to-end protocol, such as TCP.

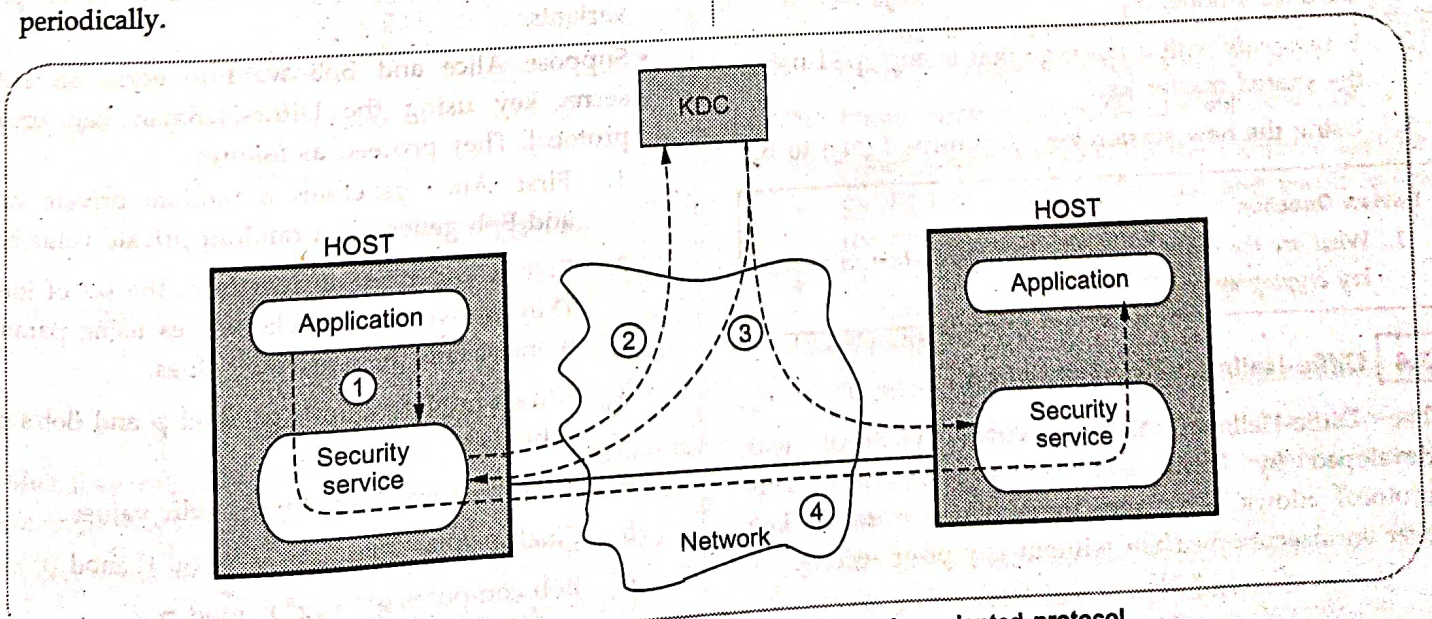


Fig. 3.3.10 Automatic key distribution for connection-oriented protocol

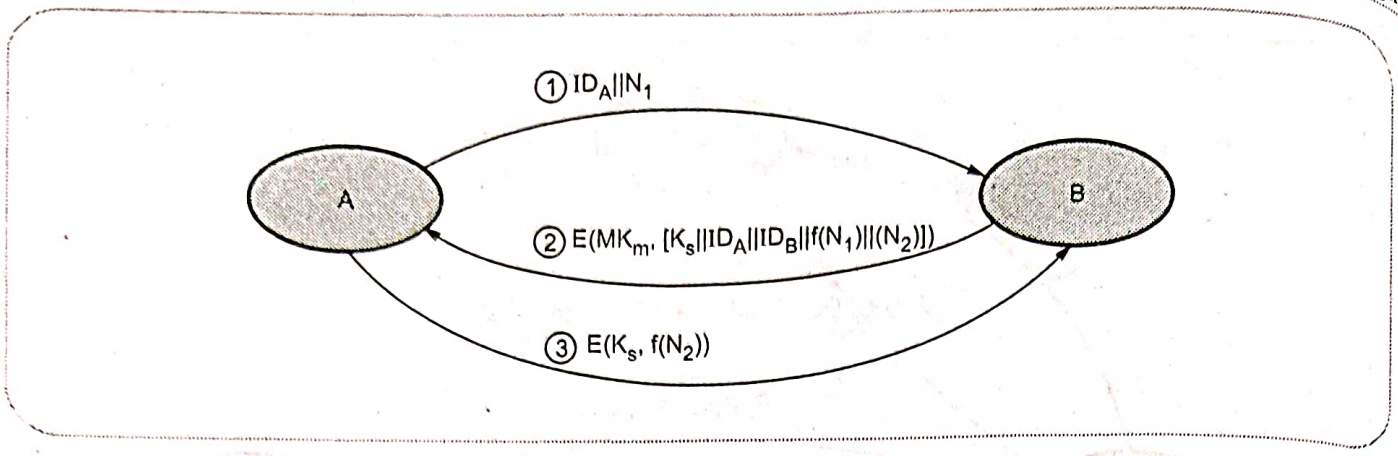


Fig. 3.3.11 Decentralized key distribution

- Following steps occurs :
  1. Host sends packet requesting connection.
  2. Session Security Module (SSM) saves that packet and applies to the KDC for permission to establish the connection.
  3. KDC distributes session key to both hosts.
  4. The requesting SSM can now release the connection request packet, and a connection is set up between the two end systems.

Decentralized key control

- Decentralized approach requires that each end system be able to communicate in a secure manner with all potential parter end systems for purposes of session key distribution.
- A session key may be established with the following sequence of steps.
  1. A issues a request to B for a session key and includes a none, N_1.
  2. B responds with a message that is encryped using the shared master key.
  3. Using the new session key, A returns f (N_2) to B.

Review Question

1. *What are the methods used in key distribution in public key cryptography.*

3.4 Diffie-Hellman Key Exchange

- The Diffie-Hellman key agreement protocol was developed by Diffie and Hellman in 1976. This protocol allows two users to exchange a secret key over an insecure medium without any prior secrets.
- The protocol has two system parameters p and g. The are both public and may be used by all the users in system.
- Parameter p is a prime number and parameter g is a integer less than p, with the following property :
  1. For every number n between 1 and p – 1 inclusive
  2. There is a power k of g such that $n = g^k \bmod p$.
- The protocol depends on the discrete logarithm problem for its security. It assumes that it computationally infeasible to calculate the share secret key $k = g^{ab} \bmod p$ given the two public value $g^a \bmod p$ and $g^b \bmod p$ when the prime p sufficiently large.
- The Diffie-Hellman key exchange is vulnerable to man-in-the-middle attack. This vulnerability is presen because Diffie-Hellman key exchange does no authenticate the participants. Possible solutions includ the use of digital signatures and other protoco variants.
- Suppose Alice and Bob want to agree on a shared secret key using the Diffie-Hellman key agreement protocol. They proceed as follows :
  1. First, Alice generates a random private value a and Bob generates a random private value b.
  2. Both a and b are drawn from the set of integers. They derive their public values using parameters p and g and their private values.
  3. Alice's public value is $g^a \bmod p$ and Bob's public value is $g^b \bmod p$.
  4. They then exchange their public values.
  5. Finally, Alice computes $g^{ab} = (g^b)^a \bmod p$.
  6. Bob computes $g^{ba} = (g^a)^b \bmod p$.

7. Since $g^{ab} = g^{ba} = k$, Alice and Bob now have a shared secret key k.

Algorithm :

- Select two numbers (1) prime number q (2) α an integer that is a primitive root of q.
- Suppose the users A and B wish to exchange a key.
  1. User A select a random integer $X_A < q$ and computes $Y_A = \alpha^{X_A} \bmod q$.
  2. User B selects a random integer $X_B < q$ and compute $Y_B = \alpha^{X_B} \bmod q$.
  3. Both side keeps the X value private and makes the Y value available publicly to the other side.
  4. User A computes the key as $K = (Y_B)^{X_B} \bmod q$.
  5. User B computes the key as $K = (Y_A)^{X_B} \bmod q$.
- Both side gets same results :

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

$$= (\alpha^{X_B} \bmod q)^{X_A} \bmod q$$

$$= (\alpha^{X_B})^{X_A} \bmod q = \alpha^{X_B X_A} \bmod q$$

$$= (\alpha^{X_A} \bmod q)^{X_B} \bmod q$$

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

Example

- Key exchange is based on the use of the prime number and a primitive root of prime number.
- Prime number $q = 353$

  Primitive root $\alpha = 3$
- A and B select secret keys.

  $X_A = 97$ $X_B = 233$
- Calculates the public keys

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

$= (3)^{97} \bmod 353$

$= (1.9080 \times 10^{97}) \bmod 353 = 40$

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

$= (3)^{233} \bmod 353$

$= (1.4765 \times 10^{111}) \bmod 353 = 248$

- After they exchange public keys, each can compute the common *secret key*.

A computes $K = (Y_B)^{X_A} \bmod q = (248)^{97} \bmod 353$

$= (1.8273 \times 10^{232}) \bmod 353 = 160$

B computes $K = (Y_A)^{X_B} \bmod q = (40)^{233} \bmod 353$

$= (1.9053 \times 10^{373}) \bmod 353 = 160$

Ex. 3.4.1 *User A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root $\alpha = 7$.*

a) If user A has private key $X_A = 5$, what is A's public key Y_A ?

b) If user B has private key $X_B = 12$, what is B's public key Y_B ?

c) What is the shared secret key ?

Sol. :

a) A's public key Y_A

$$Y_A = \alpha^{X_A} \bmod q = (7)^5 \bmod 71$$

$$= 16807 \bmod 71 = 51$$

b) B's public key Y_B

$$Y_B = \alpha^{X_B} \bmod q = (7)^{12} \bmod 71$$

$$= 13841287201 \bmod 71 = 4$$

c) Shared secret key

i) At user A $K = (Y_B)^{X_A} \bmod q$

$= (4)^5 \bmod 71 = 1024 \bmod 71$

$K = 30$

The man in middle attack can work against the Diffie-Hellman key exchange algorithm, causing it to fail.

Advantages

1. Any user can choose a random x and publish g^x in a public database such as a phone book.
2. Phone book must be maintained by a TTP.
3. Other users can look up the database and get the public key for the individual and use it to encrypt the message.
4. Ideal for use with emails.

Disadvantages

1. Does not protect against man-in-the-middle attacks.
2. Even can intercept all traffic between Alice and Bob and generate separate keys for communication with them.
3. If Allice sends an encrypted message for Bob with his public key, Eve simply forwards it.

4. For large prime p, (p – 1) is an even number and so Z_p^* will have an subgroup of order 2.

Ex. 3.4.2 *If generator g = 2 and n or P = 11, using Diffie-Hellman algorithm solve the following :*
i) Show that 2 is a primitive root of 11.
ii) If A has a public key '9' what is A's private key ?
iii) If B has a public key '3' what is B's private key ?
iv) Calculate the shared secret key.

Sol. : i)

$2^1 \bmod 11 = 2$

$2^2 \bmod 11 = 4$

$2^3 \bmod 11 = 8$

$2^4 \bmod 11 = 5$

$2^5 \bmod 11 = 10$

$2^6 \bmod 11 = 9$

$2^7 \bmod 11 = 7$

$2^8 \bmod 11 = 3$

$2^9 \bmod 11 = 6$

Using 2 as integer, we get all the integer values between 1 to 11. So 2 is a primitive root of 11.

ii) Public key = 9

$2^6 \bmod 11 = 9$

$X_A = 6$

iii) $Y_B = (11)^6 \bmod 9$

$Y_B = 1$

iv) Shared secret key :

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

$K = 3^6 \bmod 11$

$K = 3$

Ex. 3.4.3 : *Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root α = 2.*
i) If user A has the public key Y_A = 9; what is A's private key X_A ?
ii) If user A has a public key Y_A = 3 ; what is the shared secret key X_A ?

Sol. : i) q = 11, α = 2, Y_A = 9, X_A = ?

$2 \bmod 11 = 2$

$2^2 \bmod 11 = 4$

$2^3 \bmod 11 = 8$

$2^4 \bmod 11 = 5$

$2^5 \bmod 11 = 10$

$2^6 \bmod 11 = 9$

$2^7 \bmod 11 = 7$

$2^8 \bmod 11 = 3$

Since $2^e \bmod 11$ for $0 < i < 11$ contains all numbers from 1 to 11 – 1, the size of this set is equal to $\phi(q)$, the order of q.

From the above values $2^6 \bmod 11 = 9$ therefore $X_A = 6$

ii) From the above values

$\alpha^{X_A} \bmod 11 = Y_A$

$2^{X_A} \bmod 11 = 3$

$2^{X_8} \bmod 11 = 3$

$\therefore \quad X_A = 8$

Review Question

1. *Explain "Diffie-Hellman" key exchange algorithm with suitable example.*

3.5 Elliptic Curve

- An elliptic curve is a set of points on the cooridnate plane satisfying an equation of the form $y^2 + axy + by = x^3 + cx^2 + dx + e$. In order to use elliptic curves for say, Diffie-Hellman, there needs to be some mathematical operation on two points in the set that will always produce a point also in the set.
- ECC can be done with at least two types of arithmetic, each of which gives different definitions of multiplication. The two types of arithmetic are
  1. Zp arithmetic
  2. GF (2^n) arithmetic, which can be done with shifts and ⊕ s.
- To form a cryptographic system using elliptic curves, we need to find a hard problem corresponding to factoring the product of two primes or taking the discrete logarithm.

- Consider the equation $Q = KP$ where $Q, P \in E_P(a, b)$ and $K < P$. It is relatively easy to calculate Q given K and P, but it is relatively hard to determine K given Q and P. This is called the **discrete logarithm problem for elliptic curves.**

Ex. 3.5.1 *Consider the group $E_{23}(9, 17)$. This is the group defined by the equation $y^2 \bmod 23 = (x^3 + 9x + 17) \bmod 23$. What is the discrete logarithm K of $Q = (4, 5)$ to the base $P = (16, 5)$?*

Sol. : The brute-force method is to compute multiples of P until Q is found.

Thus,

$P = (16, 5)$

$2P = (20, 20)$

$3P = (14, 14)$

$4P = (19, 20)$

$5P = (13, 10)$

$6P = (7, 3)$

$7P = (8, 7)$

$8P = (12, 17)$

$9P = (4, 5)$

Because $9P = (4, 5) = Q$, the discrete logarithm $Q = (4, 5)$ to the base $P = (16, 5)$ is $K = 9$.

Analog of Diffie-Hellman key exchange

A key exchange between users A and B can be accomplished as follows

1. A selects an integer n_A less than n. This is A's private key. A then generates a public key $P_A = n_A \times G$; the public key is a point in $E_q(a, b)$.
2. B similarly selects a private key n_B and computes a public key P_B.
3. A generates the secret key $K = n_A \times P_B$.
   B generates the secret key $K = n_B \times P_A$.

The two calculations in step 3 produce the same result because

$$n_A \times P_B = n_A \times (n_B \times G)$$
$$= n_B \times (n_A \times G)$$
$$= n_B \times P_A$$

Elliptic curve encryption and decryption

- For an encryption/decryption, system requires a point G and an elliptic group $E_q(a, b)$ as parameters. Each user A selects a private key n_A and generates a public key $P_A = n_A \times G$.
- To encrypt and send message P_m to user B, A chooses a random positive integer K and produces the ciphertext C_m consisting of the pair of points

$$C_m = \{KG, P_m + KP_B\}$$

- To decrypt the ciphertext, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point

$$= P_m + KP_B - n_B(KG)$$
$$= P_m + K(n_B G) - n_B(KG)$$
$$= P_m$$

Review Question

1. *Describe elliptic curve cryptography.*

3.6 Authentication Methods

- Authentication is a service used to provide the identity of an entity.
- Identification and authentication is the process that can be used to identify and verify the users on their secure systems. In secure system, the user must identify himself/herself, then the system will authenticate the identity before using the system.
- However, authentication verifies the user who is requesting access process of determining the identity of a user that is attempting to access a system

3.6.1 Password Based Authentication Methods

- Password is a front line protection against the unauthorized access (intruder) to the system. A password authenticate the identifier (ID) and provides security to the system. Therefore almost all systems are password protected.

1] Password vulnerability

- Passwords are extremely common. Passwords can often be guessed. Use of mechanisms to keep passwords secret does not guarantee that the system security can not be broken. It only says that it is difficult to obtain passwords. The intruder can always use a trial and error method. A test of only a limited

set of potential strings tends to reveal most passwords because there is a strong tendency for people to choose relatively short and simple passwords that they can remember. Some techniques that may be used to make the task of guessing a password difficult are as follows

1. Longer passwords.
2. Salting the password table.
3. System assistance in password selection.

- The length of a password determines the ease with which a password can be found by exhaustion. For example, 3-digit password provides 1000 variations whereas a four digit passwords provides 10,000 variations. Second method is the system assistance. A password can be either system generated or user selected. User selected passwords are often easy to guess. A system can be designed to assist users in using passwords that are difficult to guess.

2] Encrypted passwords

- Instead of storing the names and passwords in plain text form, they are encrypted and stored in cipher text form in the table. In this case, instead of directly using a user specified name and password for table lookup, they are first encrypted and then the results are used for table lookup. If the stored encoded password is seen, it can not be loaded, so the password cannot be determined. The password file does not need to be kept secret.

3] One time passwords

- Set of paired passwords solve the problem of password sniffing. When a session begins, the system randomly selects and presents one part of a password pair; user must supply the other part. In this, user is challenged and must respond with the correct answer to that challenge. In this method, the password is different in each instance. One time passwords are among the only ways to prevent improper authentication due to password exposure. Commercial implementations of one time password system such as secur ID, use hardware calculators.

Password selection strategies

- Too short password is too easy to guess. If the passward is 8 random character, it is impossible to crack the password. In order to eliminate gaussable passwords four basic techniques are suggested.

1. User education
2. Computer generated password
3. Reactive password checking
4. Proactive password checking

3.6.2 Extensible Authentication Protocol

- Extensible Authentication Protocol is a universal authentication framework frequently used in wireless networks and Point-to-Point connections.
- The Extensible Authentication Protocol is a protocol commonly used in 802.1x to authenticate users.
- WPA and WPA2 standard has officially adopted five EAP types as its official authentication mechanisms.
- EAP is a way for a supplicant to authenticate, usually against a back-end RADIUS server. EAP comes from the dial access world and PPP.
- EAP sits inside PPP's authentication protocol. It provides a generalized framework for all sorts of authentication methods.
- EAP is supposed **to head off** proprietary authentication systems and let everything from **passwords to challenge-response tokens** and PKI **certificates** work smoothly.
- With a **standardized EAP**, interoperability and compatibility across authentication methods becomes simpler.
- Only the client and the authentication server have to be coordinated.
- By supporting **EAP authentication**, a RAS server (in **wireless this is the AP) gets out of** the business of actively participating in the authentication dialog.
- EAP supports multiple authentication methods, such as token card, Kerberos, one-time password, certificate, public key authentication, and smart card.

3.6.3 Biometric Authentication

Biometric identification systems can be grouped based on the main physical characteristic that lends itself to biometric identification.

- **Fingerprint identification :** Fingerprint ridges are formed in the womb; you have fingerprints by the fourth month of fetal development. Once formed, fingerprint ridges are like a picture on the surface of a

balloon. As the person ages, the fingers do get larger. However, the relationship between the ridges stays the same, just like the picture on a balloon is still recognizable as the balloon is inflated.

- **Hand geometry :** Hand geometry is the measurement and comparison of the different physical characteristics of the hand. Although hand geometry does not have the same degree of permanence or individuality as some other characteristics, it is still a popular means of biometric authentication.
- **Palm vein authentication :** This system uses an infrared beam to penetrate the users hand as it is waved over the system; the veins within the plam of the user are returned as black lines. Palm vein authentication has a high level of authentication accuracy due to the complexity of vein patterns of the palm. Because the palm vein patterns are internal to the body, this would be a difficult system to counterfeit. Also, the system is contactless and therefore hygienic for use in public areas.
- **Retina scan :** A retina scan provides an analysis of the capillary blood vessels located in the back of the eye; the pattern remains the same throughout life. A scan uses a low intensity light to take an image of the pattern formed by the blood vessels. Retina scans were first suggested in the 1930's.
- **Iris scan :** An iris scan provides an analysis of the rings, furrows and freckles in the colored ring that surrounds the pupil of the eye. More than 200 points are used for comparison.
- **Face recognition :** Facial characteristics are depends on the size and shape of facial characteristics, and their relationship to each other. Although this method is the one that human beings have always used with each other, it is not easy to automate it. Typically, this method uses relative distances between common landmarks on the face to generate a unique "faceprint".
- **Signature :** Although the way you sign your name does change over time, and can be consciously changed to some extent, it provides a basic means of identification.
- **Voice analysis :** The analysis of the pitch, tone, cadence and frequency of a person's voice.

Advantages

There are a number of advantages to this technology

- Biometric identification can provide extremely accurate, secured access to information; fingerprints, retinal and iris scan produce absolutely unique data sets when do properly.
- Current methods like password verification have many problems (people write them down, they forget them, they make up easy-to-hack passwords).
- Automated biometric identification can be done very rapidly and uniformly, with a minimum of training.
- Your identity can be verified without resort to documents that may be stolen, lost or altered.

Review Question

1. *What is authentication ? Explain various methods for authentication.*

3.7 Message Digest

- A message-digest algorithm is also called **a hash function** or a cryptographic hash function.
- It accepts a message as input and generates a fixed-length output, which is generally less than the length of the input message. The output is called a **hash value**, a fingerprint or a message digest.
- Message Digest 5 (MD5) processes the input text in 512-bit blocks. These blocks are further divided into 16 32-bit sub blocks.
- MD5 is a 128-bit hash.
- The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private key under a public-key cryptosystem such as RSA.

3.7.1 MD5 Description

- Suppose if we have b-bit message as input, and that we wish to find its message digest. Here b is an arbitrary non-negative integer; b may be zero, it need not be a multiple of eight and it may be arbitrarily

large. The bits of the message written down as follows:

m_0 m_1 ... m_{b-1}

- The following five steps are performed to compute the message digest of the message.

Step 1 : Append Padding Bits

- The message is "padded" so that its length is congruent to 448, modulo 512. Padding is always performed, even if the length of the message is already congruent to 448, modulo 512.
- Padding is performed as follows : A single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448, modulo 512. In all, at least one bit and at most 512 bits are appended.

Step 2 : Append Length

- A 64-bit representation of b is appended to the result of the previous step. In the unlikely event that b is greater than 2^{64}, and then only the low-order 64 bits of b are used.
- At this point the resulting message (after padding with bits and with b) has a length that is an exact multiple of 512 bits. Equivalently, this message has a length that is an exact multiple of 16 (32-bit) words.
- Let M[0 ... N-1] denote the words of the resulting message, where N is a multiple of 16.

Step 3 : Initialize MD Buffer

- A four-word buffer (A, B, C, and D) is used to compute the message digest. Here each of A, B, C, D is a 32-bit register. These registers are initialized to the following values in hexadecimal :

Word A : 01 23 45 67

Word B : 89 ab cd ef

Word C : fe dc ba 98

Word D : 76 54 32 10

Step 4 : Process Message in 16-Word Blocks

- We first define four auxiliary functions that each take as input three 32-bit words and produce as output one 32-bit word.

F(X,Y,Z) = XY v not(X) Z

G(X,Y,Z) = XZ v Y not(Z)

H(X,Y,Z) = X xor Y xor Z

I(X,Y,Z) = Y xor (X v not(Z))

- In each bit position F acts as a conditional: if X then Y else Z. The function F could have been defined using + instead of v since XY and not(X)Z will never have 1's in the same bit position.
- It is interesting to note that if the bits of X, Y, and Z are independent and unbiased, the each bit of F(X, Y, Z) will be independent and unbiased.
- The functions G, H and I are similar to the function F, in that they act in "bitwise parallel" to produce their output from the bits of X, Y, and Z, in such a manner that if the corresponding bits of X, Y, and Z are independent and unbiased, then each bit of G(X,Y,Z), H(X,Y,Z), and I(X,Y,Z) will be independent and unbiased.
- This step uses a 64-element table T[1 ... 64] constructed from the sine function. Let T[i] denote the i-th element of the table, which is equal to the integer part of 4294967296 times abs(sin(i)), where i is in radians.

Step 5 : Output

- The message digest produced as output is A, B, C, and D. That is, we begin with the low-order byte of A, and end with the high-order byte of D.

3.7.2 Differences between MD4 and MD5

The following are the differences between MD4 and MD5 :

1. A fourth round has been added.
2. Each step now has a unique additive constant.
3. The function g in round 2 was changed from (XY v XZ v YZ) to (XZ v Y not(Z)) to make g less symmetric.
4. Each step now adds in the result of the previous step. This promotes a faster "avalanche effect".
5. The order in which input words are accessed in rounds 2 and 3 is changed, to make these patterns less like each other.
6. The shift amounts in each round have been approximately optimized, to yield a faster "avalanche effect." The shifts in different rounds are distinct.

3.7.3 Comparison between MD5 and SHA

Sr. No.	MD5	SHA
1.	MD length is 128-bits	Length is 160-bits
2.	Speed is faster than SHA	Slower than MD5
3.	Number of iteration is 64	Number of iteration is 80
4.	Buffer space is 128-bits	Buffer space is 160-bits
5.	MD5 is vulnerable to cryptanalytic attacks	SHA-1 appears not to be vulnerable to cryptanalytic attack
6.	MD5 uses a little endian scheme	SHA-1 uses a big endian scheme
7.	Simple to implement and do not need any large programs or complex table	Simple to implement and do not need any large programs or complex table.
8.	No limit on maximum message size.	Maximum message size is $2^{64} - 1$ bits.

Review Questions

1. *Explain operation of MD5 message digest algorithm.*
2. *What is message digest ? Compare MD5 with SHA - 1.*

3.8 Kerberos

- Kerberos is an **authentication protocol**. It provides a way to authenticate clients to services to each other through a trusted third party.
- Kerberos makes the assumption that the connection between a client and service is insecure. Passwords are encrypted to prevent others from reading them. Clients only have to authenticate once during a pre-defined lifetime.
- Kerberos was designed and developed at MIT by Project Athena. Currently, Kerberos is upto Version 5. Version 4 being the first version to be released outside of MIT.
- Kerberos has been adopted by several private companies as well as added to several operating systems.
- Its creation was inspired by client-server model replacing time-sharing model. Kerberos is a network authentication protocol designed to allow users, clients and servers, authenticate themselves to each other.
- This **mutual authentication** is done using **secret-key cryptography** with parties proving to each other their identity across an insecure network connection.
- Communication between the client and the server can be secure after the client and server have used Kerberos to prove their identity.
- From this point on, subsequent communication between the two can be encrypted to assure privacy and data integrity.

Requirement of Kerberos

- Kerberos client/server authentication requirements are :
  1. **Security :** That Kerberos is strong enough to stop potential eavesdroppers from finding it to be a weak link.
  2. **Reliability :** That Kerberos is highly reliable employing a distributed server architecture where one server is able to back up another. This means that Kerberos systems are fail safe, meaning graceful degradation, if it happens.
  3. **Transparency :** That user is not aware that authentication is taking place beyond providing passwords.
  4. **Scalability :** Kerberos systems accept and support new clients and servers.

  To meet these requirements, Kerberos designers proposed a third-party trusted authentication service to arbitrate between the client and server in their mutual authentication.

3.8.1 Kerberos Terminology

- Kerberos has its own terminology to define various aspects of the service.
  1. **Authentication Server (AS) :** A server that issues tickets for a desired service which are in turn given to users for access to the service.
  2. **Client :** An entity on the network that can receive a ticket from Kerberos.
  3. **Credentials :** A temporary set of electronic credentials that verify the identity of a client for a particular service. It also called a ticket.
  4. **Credential cache or ticket file :** A file which contains the keys for encrypting communications between a user and various network services.
  5. **Crypt hash :** A one-way hash used to authenticate users.

6. **Key :** Data used when encrypting or decrypting other data.
7. **Key Distribution Center (KDC) :** A service that issue Kerberos tickets and which usually run on the same host as the Ticket-Granting Server (TGS).
8. **Realm :** A network that uses Kerberos composed of one or more servers called KDCs and a potentially large number of clients.
9. **Ticket-Granting Server (TGS) :** A server that issues tickets for a desired service which are in turn given to users for access to the service. The TGS usually runs on the same host as the KDC.
10. **Ticket-Granting Ticket (TGT) :** A special ticket that allows the client to obtain additional tickets without applying for them from the KDC.

3.8.2 Kerberos Version 4

- Kerberos version 4 uses DES for providing authentication service. Some aspect of version 4 are
  A) Simple Authentication Dialogue.
  B) More Secure Authentication Dialogue.

3.8.2.1 Simple Authentication Dialogue

- For a secure transaction, server should confirm the client and its request. In unprotected network it creates burden on server, therefore an Authentication Server (AS) is used. The Authentication Server (AS) maintains passward of all users in centralized database. Also the authentication server shares a unique secret key with each server.

- Let
  Client is represented as C
  Authentication server is represented as AS
  Server is represented as V
  Identifier of user on C is represented as ID_C
  Identifier of V is represented as ID_V
  Password of user on C is P_C
  Network address of C is represented as AD_C
  Secret encryption key shared by AS and V is K_V
  Then consider a hypothetical dialogue.

	Sender and receiver		Contents of message
1.	$C \rightarrow AS$	:	$IDc \parallel Pc \parallel IDv$
2.	$AS \rightarrow C$	:	Ticket
3.	$C \rightarrow V$	:	$IDc \parallel Ticket$
4.	Ticket	=	$E [Kv, (IDc \parallel ADc \parallel IDv)]$

Explanation

1. **Client Clogs on to workstation requesting to access to server V :** The workstation requests user's passward and sends message to AS including user ID + Server ID + User passward. The AS checks this message with database and verifies it.
2. **AS issues ticket :** On verifying the tests. AS issues ticket containing user ID + Server ID + Network address.

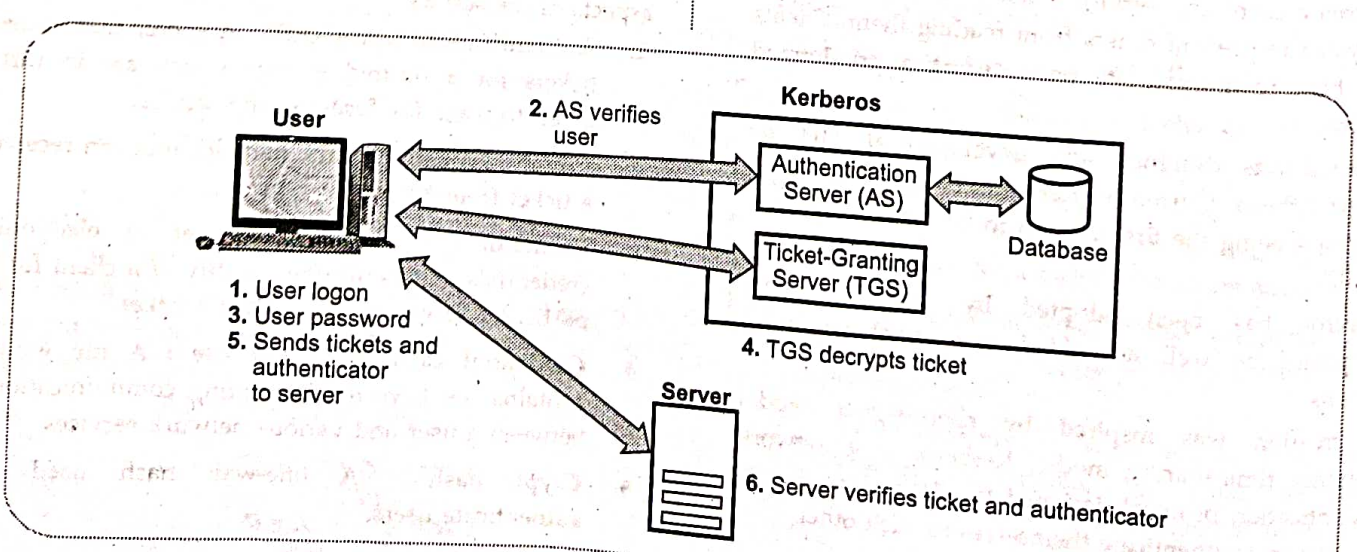


Fig. 3.8.1 Overview of kerberos

3. **Client C applies server V :** With this ticket, client C asks server V for access. Server V decrypts the ticket and verify the aunthenticity of data then grants the requested service. In above hypothetical dialogue, symbol || represents concatenation.

3.8.2.2 Secure Authentication Dialogue

- Kerberos version 4 protocol ensures secure authentication dialogue involving three sessions.
  - i] **Authentication Service :** Exchange to obtain ticket-granting ticket.
  - ii] **Ticket-granting Service :** Exchange to obtain service granting ticket.
  - iii] **Client/server authentication :** Exchange to obtain service.
- Each of the above session has two steps, as shown in table below

Session	Step	Sender-Receiver
i]	1.	C → AS
	2.	AS → C
ii]	3.	C → TGS (Ticket-granting server)
	4.	TGS → C
iii]	5.	C → V
		V → C

- Fig. 3.8.1 shows how the steps are executed in Kerberos version 4.

3.8.2.3 Kerberos Realms

- The constituents of a full-service Kerberos environment are
  a) A Kerberos server
  b) Clients
  c) Number of application server.
- **Requirements of Kerberos sever :**
  a) Kerberos server should have user ID.
  b) Hashed password for all users.
  c) All users should be registered with Kerberos server.
  d) Kerberos server should have secret key with each server.
  e) All servers should be registered with Kerberos server.
- A **Kerberos realm** is referred as is the environment where
  - All nodes share same secured database.
  - Changing and accessing the Kerberos database requires Kerberos master password.
  - A read only copy of Kerberos database resides in computer system.
- Networks have different realms under different administrative organizations. The users of one realm may access the servers in other realm provided the users are authenticated. The interoperating Kerberos shares a secret key with the server in other realm.

3.8.3 Kerberos Version 5

- Version 4 of Kerberos have some environmental shortcoming and technical deficiencies.

Environmental shortcomings of version 4

1. Encryption system dependence
2. Internet protocol dependence
3. Message byte ordering
4. Ticket lifetime
5. Authentication forwarding
6. Inter realm authentication.

Technical deficiencies of version 4

1. Double encryption
2. PCBC (Propagating Cipher Block Chaining) encryption
3. Session keys
4. Password attacks

3.8.3.1 Version 5 Authentication Dialogue

The Kerberos version 5 message exchange involves three session, these are

1. Authentication service exchange
2. Ticket - granting exchnage
3. Client/server authentication exchange

- Each session has two steps. Table 3.8.1 summarizes session, steps and their functions.

	Session	Step	Function
i]	Application service exchange	C → AS AS → C	To obtain ticket-granting ticket.
ii]	Ticket-granting service exchange	C → TGS TGS → C	To obtain service-granting ticket.
iii]	Client/Server authentication exchange	C → V V → C	To obtain service.

Table 3.8.1

- The flags field is expanded in ticket in version 5 of Kerberos. Various flags that may be included in a ticket, are

i) INITIAL
ii) PRE-AUTHENT
iii) HW-AUTHENT
iv) RENEWABLE
v) MAY-POSTDATE
vi) POSTDATED
vii) INVALID
viii) PROXIABLE
ix) PROXY
x) FORWARDABLE
xi) FORWARDED

3.8.4 Comparison between Kerberos Versions 4 and 5

Parameters	Kerberos Versions 4	Kerberos Versions 5
Encryption algorithms used	DES only	DES and other encryptions
Ticket lifetime	5 min units, Maximum = 1280 minutes	Start and end time is arbitrary
Message byte ordering	Tagged message with ordering	Abstract syntax notation on basis encoding rules.
Password attack	Initial request in clear and use it for offline attack.	Need to send pre-authentication data
Two times encryption	Supported	Not supported
Session keys	Replay risk using repeated ticket	Sub session key once only
Hierarchy of realms	Limits to pairs	Transition allowed

3.8.5 Strengths of Kerberos

1. Passwords are never sent across the network unencrypted. This prevents those unscrupulous people from being able to read the most important data sent over the network.
2. Clients and applications services mutually authenticate. Mutual authentication allows for both ends to know that they truly know whom they are communicating with.
3. Tickets have a limited lifetime, so if they are stolen, unauthorized use is limited to the time frame that the ticket is valid.
4. Authentication through the AS only has to happen once. This makes the security of Kerberos more convenient.
5. Shared secret keys between clients and services are more efficient than public-keys.
6. Many implementations of Kerberos have a large support base and have been put through serious testing.
7. Authenticators, created by clients, can only be used once. This feature prevents the use of stolen authenticators.

3.8.6 Weakness of Kerberos

1. Kerberos only provides authentication for clients and services.
2. Kerberos 4 uses DES, which has been shown to be vulnerable to brute-force-attacks with little computing power.
3. The principal-key database on the KDC has to be hardened or else bad things can happen.
4. Like any security tool, it is also vulnerable to users making poor password choices.
5. Kerberos doesn't work well in a time-sharing environment.
6. Kerberos requires a continuously available Kerberos Server. If the Kerberos Server goes down, the Kerberos network is unusable.
7. Kerberos does not protect against modifications to system software like Trojan horses.

3.8.7 Difference between Kerberos and SSL

Sr. No.	Kerberos	SSL
1.	Uses private key encryption.	Uses public key encryption.
2.	Based on the trusted third party.	Based on certificate.
3.	Ideal for network environment.	Ideal for the WWW.
4.	Key revocation can be accomplished by disabling a user at the authentication server.	Key revocation requires revocation server to keep track of bad certificate.
5.	Password resides in user's minds where they are usually not subject to secret attack.	Certificates sit on a user hard drive where they are subject to being cracked.
6.	Kerberos open source and free available.	Uses patented material, so the service is not free.

Review Questions

1. *Explain the operation of Kerberos.*
2. *What is kerberos ? Explain its operation.*

3.9 X.509 Authentication Service

- X.509 is part of X.500 recommendations for directory service i.e. set of servers which maintains a database of information about users and other attributes.
- X.509 defines authentication services e.g. certificate structure and authentication protocols. Also X.509 also defines alternative authentication protocols base on use of public-key certificates. The X.509 certificate format is emplied in S/MIME, IP security, SET and SSL/TLS.
- X.509 standard uses RSA algorithm and hash function for digital signature. Fig. 3.9.1 shows generation of public key certificate.

3.9.1 X.509 Format of Certificate

- The current version of the standard is version 3, called as X.509V3. The general format of digital certificate X.509V3 is shown in Fig. 3.9.2.

1	Version
2	Certificate Serial Number
3	Signature Algorithm Identifier
4	Issuer Name
5	Period of Validity
6	Subject Name
7	Subject's Public Key Info.
8	Issuer Unique Identifier
9	Subject Unique Identifier
10	Extensions
11	Signature

Fig. 3.9.2 X.509 Digital certificate format version 3

1. **Version** : Identifies successive versions of certificate format the default is version.
2. **Certificate Serial Number** : It contains an unique integer number, which is generated by Certification Authority (CA).
3. **Signature Algorithm Identifier** : Identifies the algorithm used by the CA to sign the certificate.
4. **Issuer Name** : Identifies the distinguished name of the CA that created and signed this certificate.
5. **Period of Validity** : Consists of two date-time values (not before and not after) within which the certificate is valid.
6. **Subject Name** : It specifies the name of the user to whom this certificate is issued.

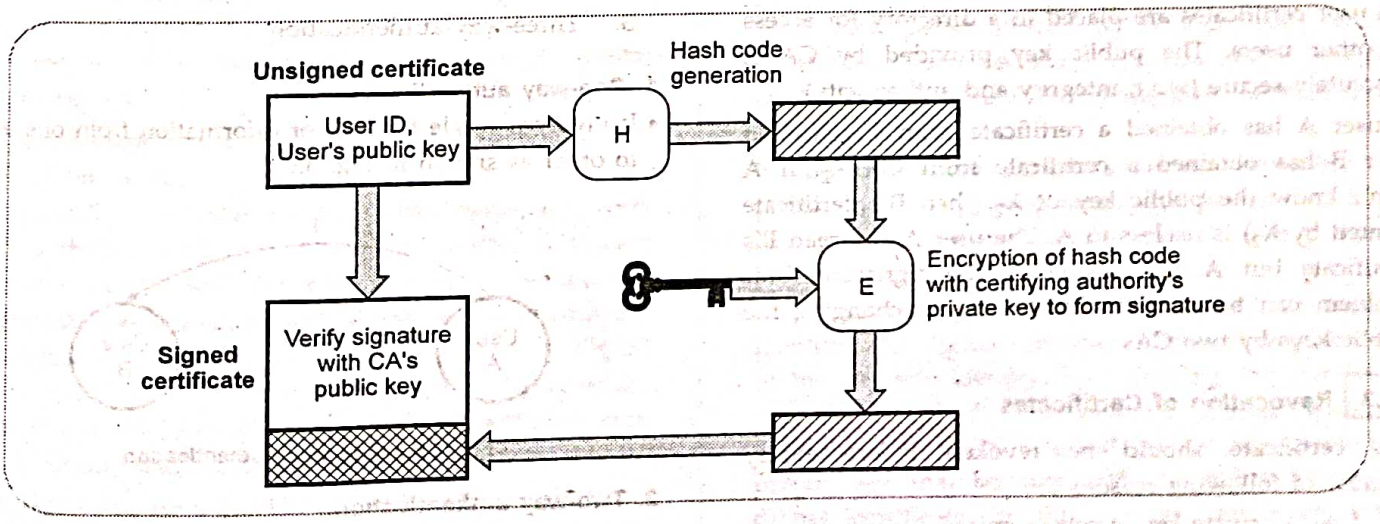


Fig. 3.9.1 Public key certificate

7. **Subject's Public Key Information** : It contains public key of the subject and algorithms related to that key.
8. **Issuer Unique Identifier** : It is an optional field which helps to identify a CA uniquely if two or more CAs have used the same Issuer Name.
9. **Subject Unique Identifier** : It is an optional field which helps to identify a subject uniquely if two or more subjects have used the same Subject Name.
10. **Extensions** : One or more fields used in version 3. These extensions convey additional information about the subject and issuer keys.
11. **Signature** : It contains hash code of the fields, encrypted with the CA's private key. It includes the signature algorithm identifier.

Standard notations for defining a certificate

$$CA\langle\langle A\rangle\rangle = CA\{V, SN, AI, CA, T_A A, A_P\}$$

where,

$CA\langle\langle A\rangle\rangle$ indicates the certificate of user A issued by certification authority CA.

$CA\{V \ldots\ldots A_P\}$ indicates signing of $V \ldots\ldots A_P$ by CA.

3.9.2 Obtaining User's Certificate

- The characteristics of user certificate are -
  1. Any user who can access public key of CA can verify user public key.
  2. Only certification Authority (CA) can modify the certificate.
- All user certificates are placed in a directory for access of other users. The public key provided by CA is absolutely secure (w.r.t. integrity and authenticity).
- If user A has obtained a certificate from CA X_1 and user B has obtained a certificate from CA X_2. If A don't know the public key of X_2, then B's certificate (issued by X_2) is useless to A. The user A can read B's certificate but A can not verify the signature. This problem can be resolved by securely exchanging the public keys by two CAs.

3.9.3 Revocation of Certificates

- The certificate should be revoked before expiry because of following reasons :
  1. User's private key is compromised.
  2. User is not certified by CA.
  3. CA's certificate is compromised.
- Each CA has a list of all revoked but not expired certificates. The Certificate Revocation List (CRL) is posted in directory signed by issuer and includes issuer's name, date of creation, date of next CRL. Fig. 3.9.3 Certificate revocation list. Each certificate has unique serial number of identify the certificate.

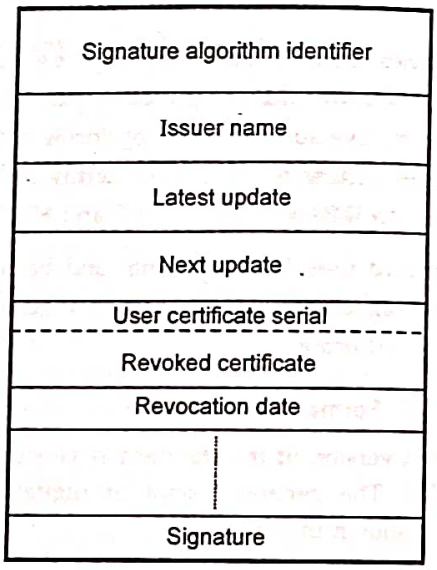


Fig. 3.9.3 Certificate revocation list

3.9.4 Authentication Procedures

- X.509 supports three types of authenticating using public key signatures. The types of authentication are
  1. One-way authentication
  2. Two-way authentication
  3. Three-way authentication

1. One-way authentication

- It involves single transfer of information from one user to other as shown in Fig. 3.9.4.

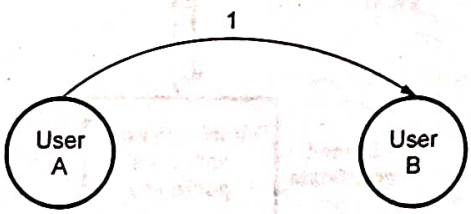


Fig. 3.9.4 One way authentication

2. Two-way authentication

- Two-way authentication allows both parties to communicate and verify the identity of the user.

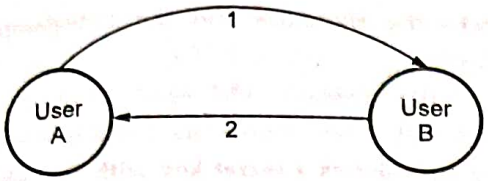


Fig. 3.9.5 Two-way authentication

3. Three-way authentication

- Three-way authentication is used where synchronized clockes are not available Fig. 3.9.6 shows three-way authentication.

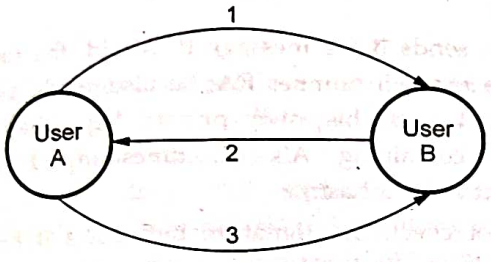


Fig. 3.9.6 Three-way authentication

3.9.5 Digital Certificate

- A data structure that securely binds an individual or entity to a public key used in cryptographic operations such as digital signatures or asymmetric encryption.
- To obtain digital certificate an organization must apply to a certification authority which is responsible for validating and ensuring the authenticity of requesting organization. The certificate will identify the name of the organization, a serial number, the validity date and the organization's public key where encryption to / from that organization is required.
- In addition, the digital certificate will also contain the digital signature of the certification authority to allow any recipient to confirm the authenticity of the digital certificate.
- A digital certificate is an ID that is carried with a file. To validate a signature, a certifying authority validates information about the software developers and then issues them digital certificates. The digital certificate contains information about the person to whom the certificate was issued, as well as information about the certifying authority that issued it. When a digital certificate is used to sign programs, ActiveX controls, and documents, this ID is stored with the signed item in a secure and verifiable form so that it can be displayed to a user to establish a trust relationship.
- A digital certificate allows unique identification of an entity; it is essentially an electronic ID card, issued by a trusted third party. Digital certificates form part of the ISO authentication framework, also known as the X.509 protocol. This framework provides for authentication across networks.
- A digital certificate serves two purposes: it establishes the owner's identity, and it makes the owner's public key available. A digital certificate is issued by a Certification Authority (CA). It is issued for only a limited time, and when its expiry date has passed, it must be replaced.
- A digital certificate consists of :
  1. The public key of the person being certified
  2. The name and address of the person being certified, also known as the Distinguished Name (DN)
  3. The digital signature of the CA
  4. The issue date
  5. The expiry date
- The Distinguished Name is the name and address of a person or organization. You enter your Distinguished Name as part of requesting a certificate. The digitally-signed certificate includes not only your own Distinguished Name, but the Distinguished Name of the CA, which allows verification of the CA.
- To communicate securely, the receiver in a transmission must trust the CA that issued the certificate that the sender is using. This means that when a sender signs a message, the receiver must have the corresponding CA's signer certificate and public key designated as a trusted root key. For example, your web browser has a default list of signer certificates for trusted CAs. If you want to trust certificates from another CA, you must receive a certificate from that CA and designate it as a trusted root key.
- If you send your digital certificate containing your public key to someone else, what keeps that person from misusing your digital certificate and posing as you ? The answer is : your private key.
- A digital certificate alone is not proof of anyone's identity. The digital certificate allows verification only of the owner's identity, by providing the public key needed to check the owner's digital signature. Therefore, the digital certificate owner must protect the private key that belongs with the public key in the digital certificate. If the private key were stolen, anyone could pose as the legitimate owner of the digital certificate.

3.10 Digital Signatures

- A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator's private key.

Requirements

- Message authentication protects two parties who exchange messages from any third party. However, it does not protect the two parties against each other.
- In situations where there is not complete trust between sender and receiver, something more than authentication is needed. The most attractive solution to this problem is the digital signature. The digital signature is analogous to the handwritten signature.
- It must have the following properties
  1. It must verify the author and the date and time of the signature.
  2. It must to authenticate the contents at the time of the signature.
  3. It must be verifiable by third parties, to resolve disputes.
- The digital signature function includes the authentication function. On the basis of these properties, we can formulate the following requirements for a digital signature.
- Must be a bit pattern depending on the message being signed.
- Signature must use some information unique to the sender to prevent forgery and denial.
- Computationally easy to produce a signature.
- Computationally easy to recognize and verify the signature.
- Computationally infeasible to forge a digital signature.
  a) either by constructing a new message for an existing digital signature.
  b) or by constructing a fraudulent digital signature for given message.
- Practical to retain a copy of the digital signature in storage.

Two general schemes for digital signatures

1) Direct 2) Arbitrated

3.10.1 Arbitrated Digital Signatures

Every signed message from A to B goes to an arbiter BB (Big Brother) that everybody trusts.

- BB checks the signature and the timestamp, origin, content, etc.
- BB dates the message and sends it to B with an indication that it has been verified and it is legitimate.

e.g. Every user shares a secret key with the arbiter

- A sends to BB in an encrypted form the plaintext P together with B's id, a timestamp and a random number RA.
- BB decrypts the message and thus makes sure it comes from A; it also checks the timestamp to protect against replays.
- BB then sends B the message P, A's id, the timestamp and the random number RA; he also sends a message encrypted with his own private key (that nobody knows) containing A's id, timestamp t and the plaintext P (or a hash).
- B cannot check the signature but trusts it because it comes from BB-he knows that because the entire communication was encrypted with KB.
- B will not accept the messages or messages containing the same RA to protect against replay.
- In case of dispute, B will show the signature he got from BB (only B may have produced it) and BB will decrypt it.

3.10.2 Direct Digital Signature

- This involves only the communicating parties and it is based on public keys.
- The sender knows the public key of the receiver.
- Digital signature : Encrypt the entire message (or just a hash code of the message) with the sender's private key.
- If confidentiality is required : Apply the receiver's public key or encrypt using a shared secret key.
- In case of a dispute the receiver B will produce the plaintext P and the signature E(KRA, P) - the judge will apply KUA and decrypt P and check the match : B does not know KRA and cannot have produced the signature himself.

Weaknesses

- The scheme only works as long as KRA remains secret : If it is disclosed (or A discloses it herself), then the argument of the judge does not hold : Anybody can produce the signature.
- **Attack** : To deny the signature right after signing simply claim that the private key has been lost-similar to claims of credit card misuse.

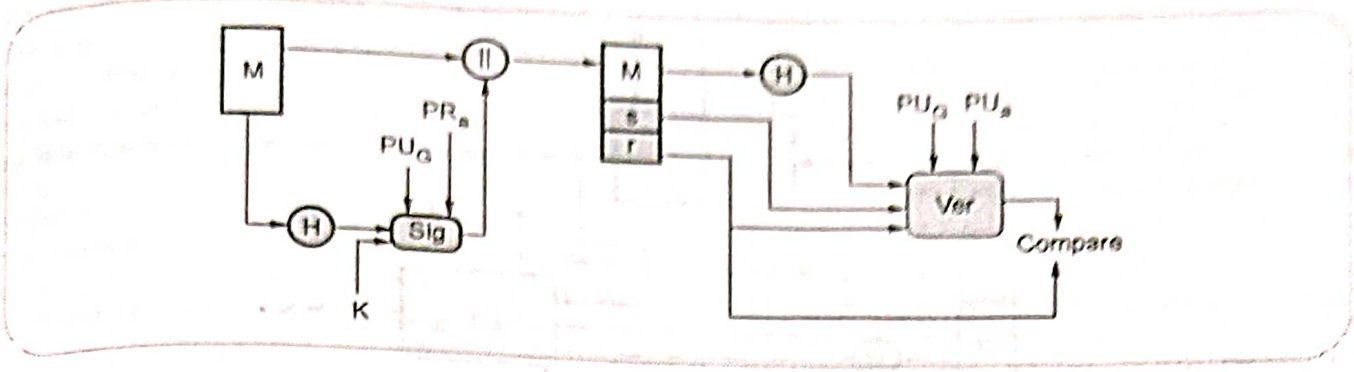


Fig. 3.10.1 DSS approach

i.e. If A changes her public-private keys (she can do that often) the judge will apply the wrong public key to check the signature.

- **Attack** : To deny the signature change your public-private key pair-this should not work if a PKI is used because they may keep trace of old public keys.
  i.e. A should protect her private key even after she changes the key.
- **Attack** : Eve could get hold of an old private key and sign a document with an old timestamp.

3.10.3 Digital Signature Standard

- The Digital Signature Standard (DSS) makes use of the Secure Hash Algorithm (SHA) and presents a new digital signature technique, the Digital Signature Algorithm (DSA). DSS cannot be used for encryption or key exchange. Fig. 3.10.1 shows the DSS approach.
- It uses a hash function. The hash code is provided as input to a signature function along with a random number K generated for this particular signature.
- The signature function also depends on the sender's private key (PR_a) and a set of parameters known to a group of communicating principles.
- The result is a signature consisting of two components, labeled s and r.
- At the receiving end, the hash code of the incoming message is generated. This plus the signature is input to a verification function.
- Fig. 3.10.2 shows the RSA approach. In the RSA approach, the message to be signed is input to a hash function that produces a secure hash code of fixed length. This hash code is then encrypted using the sender's private key to form the signature. Both the message and the signature are then transmitted.
- The recipient takes the message and produces a hash code. The recipient also decrypts the signature using the sender's public key. If the calculated hash code matches the decrypted signature, the signature is accepted as valid.

3.10.4 Digital Signature Algorithm

- There are three parameters that are public and can be common to a group of users. **Prime number q is chosen and it is 160-bit. A prime number p is selected with a length between 512 and 1024 bits such that q** divides (P – 1).

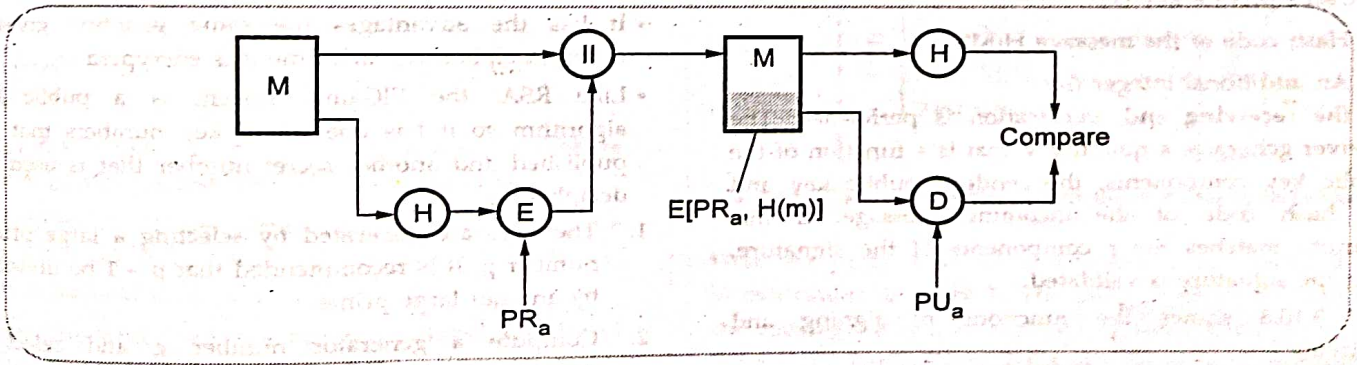


Fig. 3.10.2 RSA approach

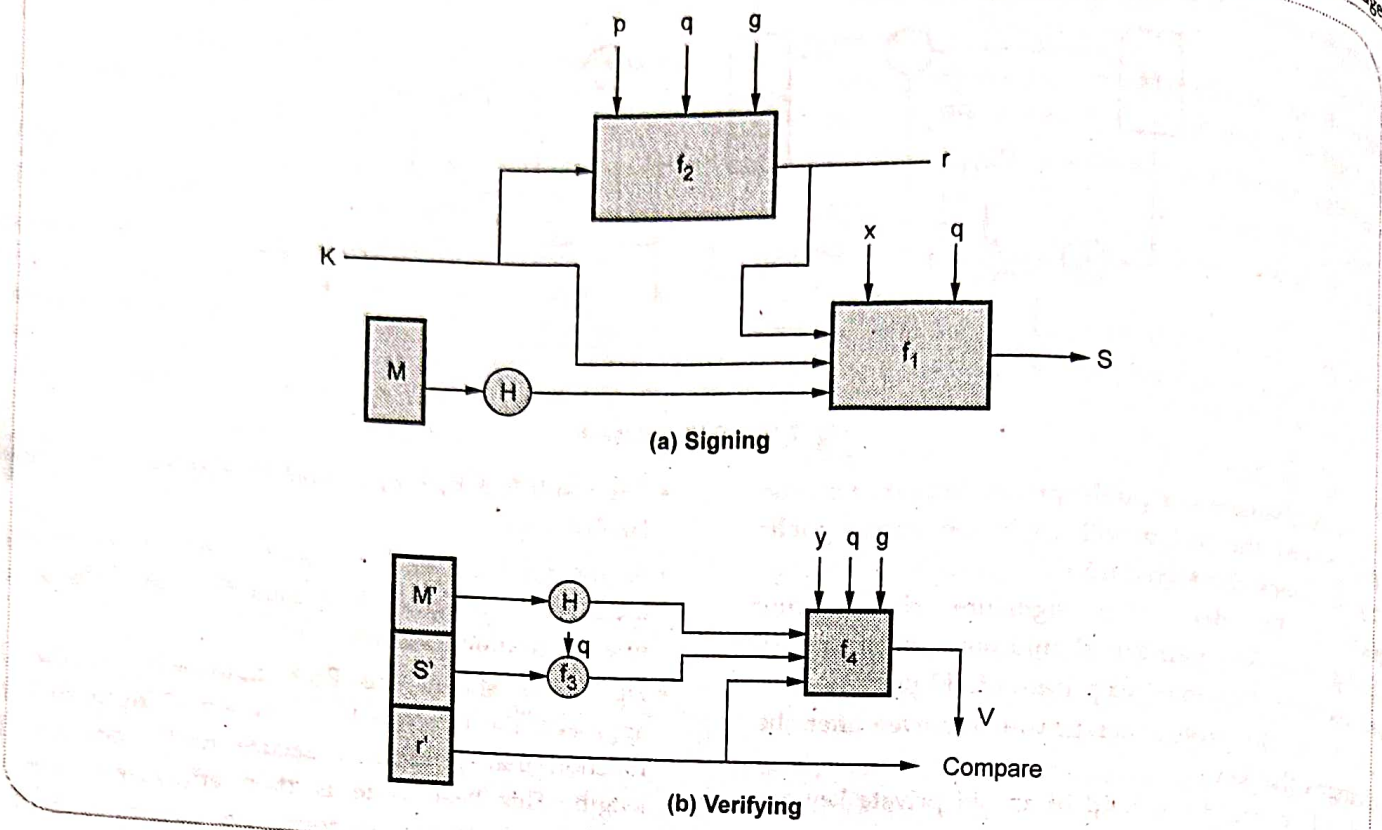


Fig. 3.10.3 Signing and verifying

- g is chosen to be of the form $h^{(p-1)/q}$ mod p where h is an integer between 1 and (p – 1).
- With these number, user selects a private key and generate a public key. The private key x must be a number from 1 to (q – 1) and should be chosen randomly or pseudorandomly.
- The public key is calculated from the private key as $y = g^x \bmod p$.
- To create a signature, a user calculates two quantities, **rands**, that are functions of
  - i) Public key components (p, q, g)
  - ii) User's private key (x)
  - iii) Hash code of the message H(M)
  - iv) An additional integer (K)
- **At the receiving end**, verification is performed. The receiver generates a quantity V that is a function of the public key components, the sender's public key and the hash code of the incoming message. If this quantity matches the r components of the signature, then the signature is validated.
- Fig. 3.10.3 shows the functions of signing and verifying.

3.10.5 ELGamal Digital Signatures

- The ElGamal algorithm provides an alternative to the RSA for public key encryption.
1. Security of the RSA depends on the difficult of factoring large integers.
2. Security of the ElGamal algorithm depends on the difficulty of computing discrete logs in a large prime modulus.
- ElGamal has the disadvantage that the ciphertext is twice as long as the plaintext.
- It has the advantages the same plaintext gives a different ciphertext each time it is encrypted.
- Like RSA, the ElGamal system is a public key algorithm so it has one set of key numbers that are published and another secret number that is used for deciphering.
1. The keys are generated by selecting a large prime number p. It is recommended that p – 1 be divisible by another large prime.
2. Compute a generator number g and select a random integer "a" less than p – 1.

3. With these numbers compute $b = g^a \pmod p$.
4. The public key consists of the three number (p, g, b) and the secret key is the number a.
5. To find "a" given the public key, an attacker must be able to solve the discrete logarithm problem.

Encryption :

- If Bob wants to send a message to Alice he begins by looking up her public key (p, g, b) and representing the message as an integer m in the range 0 to p – 1.
- He then selects a random key, k that is less than p – 1.
- Using these numbers, Bob computes two numbers :

$$c_1 = g^k \quad \text{and} \quad c_2 = mb^k$$

- He sends (c_1, c_2) to Alice.

Decryption :

- When Alice receives the cipher-text, she will recover the plaintext using her secret key, "a" to compute :

$$m = c_2 c_1^{-a} \bmod p$$

- This works because :

$$c_2 c_1^{-a} = mb^k (g^k)^{-a} \, mb^k \, (g^a)^k \, (g^k)^{-a}$$
$$= mg^{ak} \, g^{-ak} = m \pmod p$$

- Bob should choose a different random integer k for each message he sends to Alice. If M is a longer message, so it is divided into blocks, he should choose a different k for each block.
- Say he encrypts two messagers (or blocks) M_1 and M_2, using the same k, producing cipher-texts.
- Eve intercepts both cipher-text messages and discovers one plaintext message M_1, she can compute the other plaintext message M_2.

Example : Alice selected her initial prime number p = 11, found the primitive element g = 7 and selected her random secret key a = 2, then her public key is :

$$b = 7^2 \bmod 11 = 5$$

- She would publish her public key : (11, 7, 5)
- Bob wants to send the letter "a" to Alice

1. He first breaks it up into a set of numbers where each number is less than 11 (the value of p).
2. Since the ASCII representation of "a" is 01100001, he might break it up into four messages (01 10 00 01) or in decimal (1, 2, 0, 1).
3. Next, he would select a random number k = 3 and then compute and send to Alice :

m	c_1	c_2
1	$7^3 \bmod 11 = 2$	$1 \times 5^3 \bmod 11 = 4$
2	$7^3 \bmod 11 = 2$	$2 \times 5^3 \bmod 11 = 8$
0	$7^3 \bmod 11 = 2$	$0 \times 5^3 \bmod 11 = 0$
1	$7^3 \bmod 11 = 2$	$1 \times 5^3 \bmod 11 = 4$

- The cipher-text is ((2, 4), (2, 8), (2, 0), (2, 4)).

Deciphering a Message

- When Alice receives this message from Bob, she uses her secrete key a = 2 as follows :

(2, 4) : $m = 4(2) - 2 = 4(4) - 1 = 12 \bmod 11 = 1$ (4 and 3 are inverse mod 11)

(2, 8) : $m = 8(2) - 2 = 8(4) - 1 = 24 \bmod 11 = 2$

(2, 0) : $m = 0(2) - 2 = 0(4) - 1 = 0 \bmod 11 = 0$

(2, 4) : m = 1

Alice reassembles the message into the letter "a".

Review Question

1. *Explain digital signature algorithm.*

3.11 Authentication Protocol

3.11.1 Mutual Authentication

It is often necessary for both communicating themselves to each other.

3.11.1.1 Based on a Shared Secret Key

In this protocol, a secret key is shared with both party. i.e. source and destination. One party sends random number to the other, other side transforms it in a special way and then returns a result. This type of protocols are called challenge-response protocols. The working of this protocol is as follows.

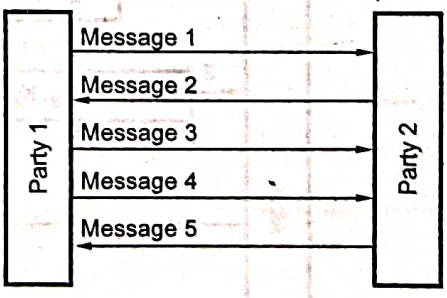


Fig. 3.11.1 Two way authentication using a challenge-response protocol

First the party 1 sends a message 1 to party 2 i.e. identification of party 1. The party 2 needs to find out the message which it received is from party 1 or any other third party. Party 2 sends a large random number

to party 1 in plaintext. The party 1 then encrypts the message with the key which shares with party 2 and sends the ciphertext back in message 3. When party 2 receives this message, they know that message is from party 1 because of the shared secret key. Uptill now party 2 is sure only about communication, but party 1 is not sure about the communication between him and party 2. The party 1 sends a random number to party 2 as plaintext in message 4. When party 2 responds with secret key, party 1 knows they are communicating with party 2. This protocol has some disadvantages. It is slower and contains extra messages. These can be eliminated by combining information.

3.11.1.2 Using Public Key Cryptography

In this method, A sends a random number R_A and identity by encrypting. A uses B's public-key E_B for sending message. When B receives this messages, B sends A back a message containing A's random number R_A and his own random number R_B and a proposed session key, K_s. When A gets message 2, A decrypts it using private key. After examining the message 2, A finds out the random number R_A. A knows that message 2 is from B only. Then A agrees to the session by sending back message 3 to B. When B reads R_B encrypted with the session key which is generated by B, B knows that A got message 2 and verified R_A.

This protocol does has some disadvantage. It assumes that both user (A and B) already know each others public keys.

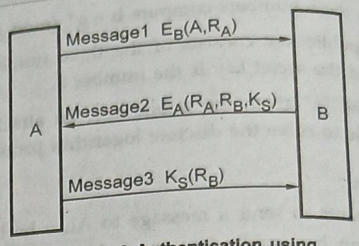


Fig. 3.11.2 Authentication using public key cryptography

3.11.2 Needham Schroeder Protocol

- The Needham Schroeder protocol refers to two methods of communication protocols through an insecure network.

1. Needham Schroeder symmetric key protocol, which is based on symmetric encryption algorithm to establish a session key between two parties in a network.
2. Needham Schroeder public-key protocol, based on the public key cryptography to provide mutual authentication between two communication parties over a network.

Needham Schroeder public key authentication protocol

- The Needham Schroeder public key authentication protocol aims to provide a mutual authentication between two parties Alice (A) and Bob (B).
- Both parties want to insure each other identity before starting to communicate. The protocol is as follows :

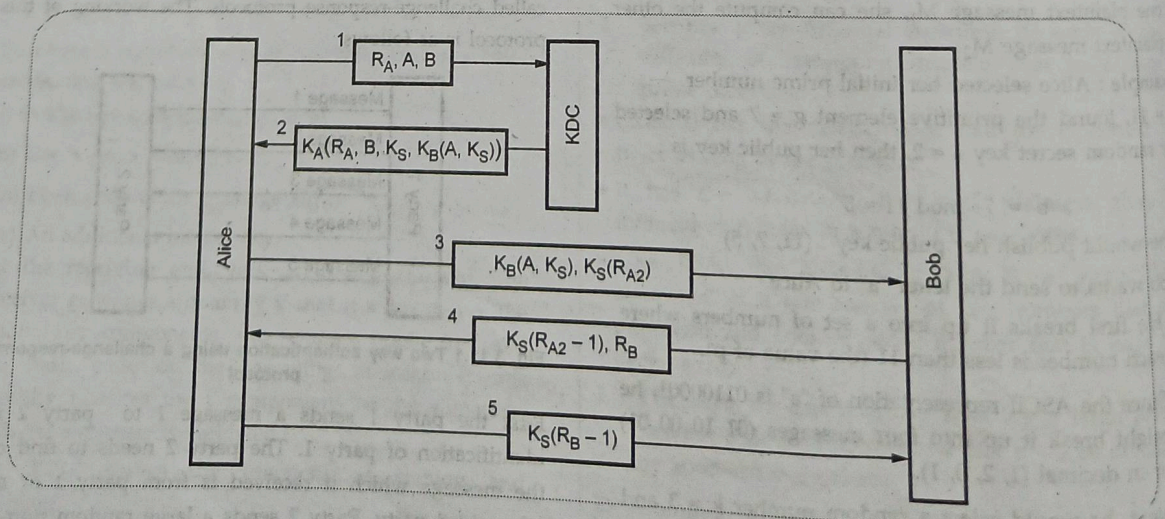


Fig. 3.11.3 Needham Schroeder authentication protocol

to party 1 in plaintext. The party 1 then encrypts the message with the key which shares with party 2 and sends the ciphertext back in message 3. When party 2 receives this message, they know that message is from party 1 because of the shared secret key. Uptill now party 2 is sure only about communication, but party 1 is not sure about the communication between him and party 2. The party 1 sends a random number to party 2 as plaintext in message 4. When party 2 responds with secret key, party 1 knows they are communicating with party 2. This protocol has some disadvantages. It is slower and contains extra messages. These can be eliminated by combining information.

3.11.1.2 Using Public Key Cryptography

In this method, A sends a random number R_A and identity by encrypting. A uses B's public-key E_B for sending message. When B receives this messages, B sends A back a message containing A's random number R_A and his own random number R_B and a proposed session key, K_s. When A gets message 2, A decrypts it using private key. After examining the message 2, A finds out the random number R_A. A knows that message 2 is from B only. Then A agrees to the session by sending back message 3 to B. When B reads R_B encrypted with the session key which is generated by B, B knows that A got message 2 and verified R_A.

This protocol does has some disadvantage. It assumes that both user (A and B) already know each others public keys.

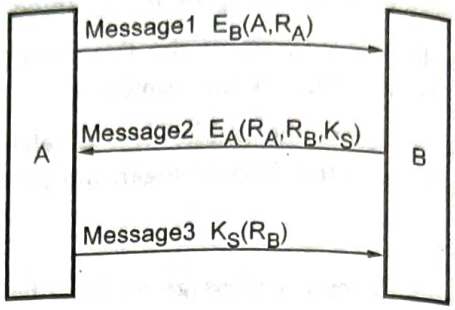


Fig. 3.11.2 Authentication using public key cryptography

3.11.2 Needham Schroeder Protocol

- The Needham Schroeder protocol refers to two methods of communication protocols through an insecure network.

1. Needham Schroeder symmetric key protocol, which is based on symmetric encryption algorithm to establish a session key between two parties in a network.
2. Needham Schroeder public-key protocol, based on the public key cryptography to provide mutual authentication between two communication parties over a network.

Needham Schroeder public key authentication protocol

- The Needham Schroeder public key authentication protocol aims to provide a mutual authentication between two parties Alice (A) and Bob (B).
- Both parties want to insure each other identity before starting to communicate. The protocol is as follows :

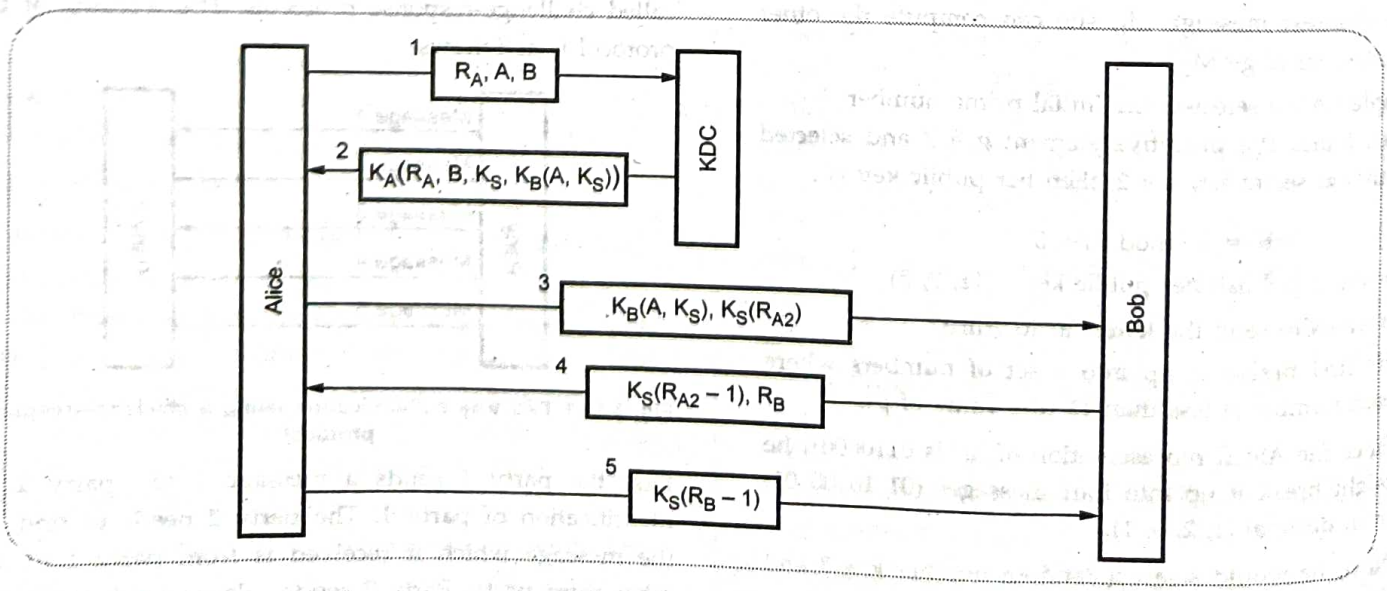


Fig. 3.11.3 Needham Schroeder authentication protocol

Unit IV

4

Security Requirements

Syllabus

IP Security : Introduction, Architecture, IPV6, IPv4, IPSec protocols, and Operations, AH Protocol, ESP Protocol, ISAKMP Protocol, VPN. WEB Security: Introduction, Secure Socket Layer (SSL), SSL Session and Connection, SSL Record Protocol, Change Cipher Spec Protocol, Alert Protocol, Handshake Protocol. Electronic Mail Security: Introduction, Pretty Good Privacy, MIME, S/MIME, Comparison. Secure Electronic Transaction (SET).

Contents

4.1 IPv4

- IP corresponds to the network layer in the OSI reference model and provides a connectionless best effort delivery service to the transport layer. An Internet Protocol (IP) address has a fixed length of 32 bits.
- IPv4 addresses are unique. Two devices on the internet can never have the same address at the same time.
- The address structure was originally defined to have a two level hierarchy : Network ID and host ID.
- The network ID identifies the network the host is connected to. The host ID identifies the network connection to the host rather than the actual host.
- IP addresses are usually written in dotted decimal notation so that they can be communicated conveniently by people.
- The IP address structure is divided into five address classes : Class A, Class B, Class C, Class D and Class E, identified by the most significant bits of the addresses.

4.1.1 IPv4 Header Format

- Packets in the IPv4 layer are called datagrams. A datagram is a variable length packet consisting of two parts : Header and data.
- Fig. 4.1.1 shows IPv4 header format

1. **VER** is the field that contains the IP protocol version. The current version is 4.5 is an experimental version. 6 is the version for IPv6.
2. **HLEN** is the length of the IP header in multiples of 32 bits without the data field.The minimum value for a correct header is 5 (i.e. 20 bytes), the maximum value is 15 (i.e., 60 bytes).
3. **Service type** : The service type is an indication of the quality of service requested for this IP datagram. It contains the following information.

Precedence	Types of service	R

Precedence specifies the nature / priority :

000	Routine
001	Priority
010	Immediate
011	Flash
100	Flash override
101	Critical
110	Internetwork control
111	Internetwork control

TOS specifies the type of service value :

TOS bits	Description
1000	Minimize delay
0100	Maximum throughout
0010	Maximize reliability
0001	Minimize monetary cose
0000	Normal service

The last bit is reserved for future use.

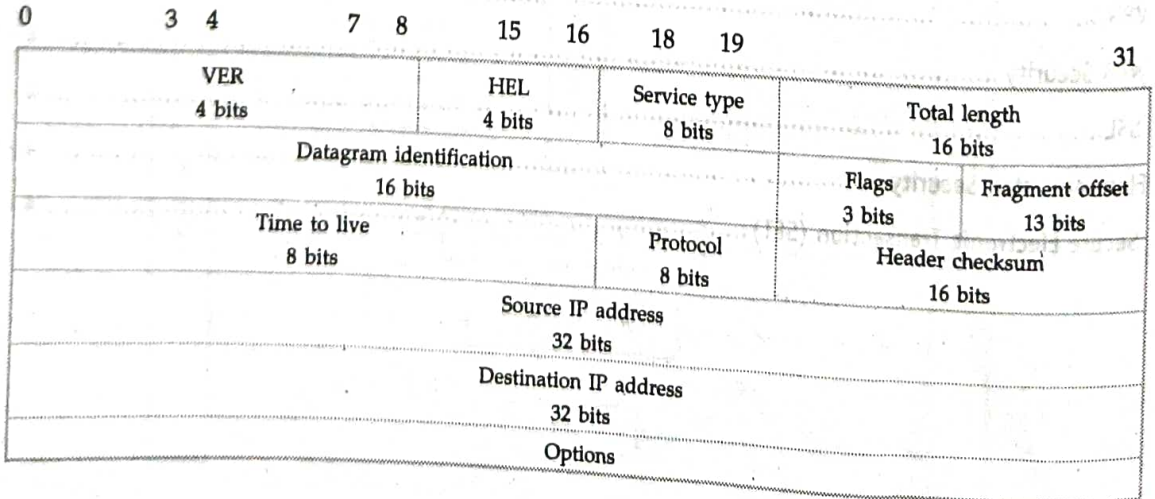


Fig. 4.1.1 IPv4 header format

4. **Total length** specifies the total length of the datagram, header and data, in octets.
5. **Identification** is a unique number assigned by the sender used with fragmentation.
6. **Flags** contain control flags :
   a. The first bit is reserved and must be zero;
   b. The 2nd bit is DF (Do not Fragment), 0 means allow fragmentation;
   c. The third is MF (More Fragments), 0 means that this is the last fragment.
7. **Fragment offset** is used to reassemble the full datagram. The value in this field contains the number of 64-bit segments (header bytes are not counted) contained in earlier fragments. If this is the first (or only) fragment, this field contains a value of zero.
8. **TTL** (Time To Live) specifies the time (in seconds) the datagram is allowed to travel. In practice, this is used as a hop counter to detect routing loops.
9. **Protocol number** indicates the higher level protocol to which IP should deliver the data in this datagram. E.g., ICMP = 1; TCP = 6; UDP = 17.
10. **Header checksum** is a checksum for the information contained in the header. If the header checksum does not match the contents, the datagram is discarded.
11. **Source/Destination IP addresses** are the 32-bit source/destination IP addresses.
12. **IP options** is a variable-length field (there may be zero or more options) used for control or debugging and measurement. For instance :
    a. The **loose source routing** option provide a means for the source of an IP datagram to supply explicit routing information;
    b. The **timestamp** option tell the routers along the route to put timestamps in the option data.
13. **Padding** is used to ensure that the IP header ends on a 32 bit boundary. The padding is zero.

4.2 IPv6

- IPv6 addresses are 128 bits in length. Addresses are assigned to individual interface on nodes, not to the node themselves.
- A single interface may have multiple unique unicast addresses. The first field of any IPv6 address is the variable length format prefix, which identifies various categories of addresses.
- A new notation has been devised for writing 16-byte addresses. They are written as eight groups of four hexadecimal digits with colons between the groups, like this 8000 : 0000 : 0000 : 0000 : 0123 : 4567 : 89AB : CDEF
- IPv6 allows three types of addresses: 1. Unicast 2. Anycast 3. Multicast

4.2.1 Packet Format

- The IPv6 packet is shown in Fig. 4.2.1. Each packet is composed of a mandatory base header followed by the payload. The payload consists of two parts : Optional and data.
- Fig. 4.2.2 shows the IPv6 datagram header format.

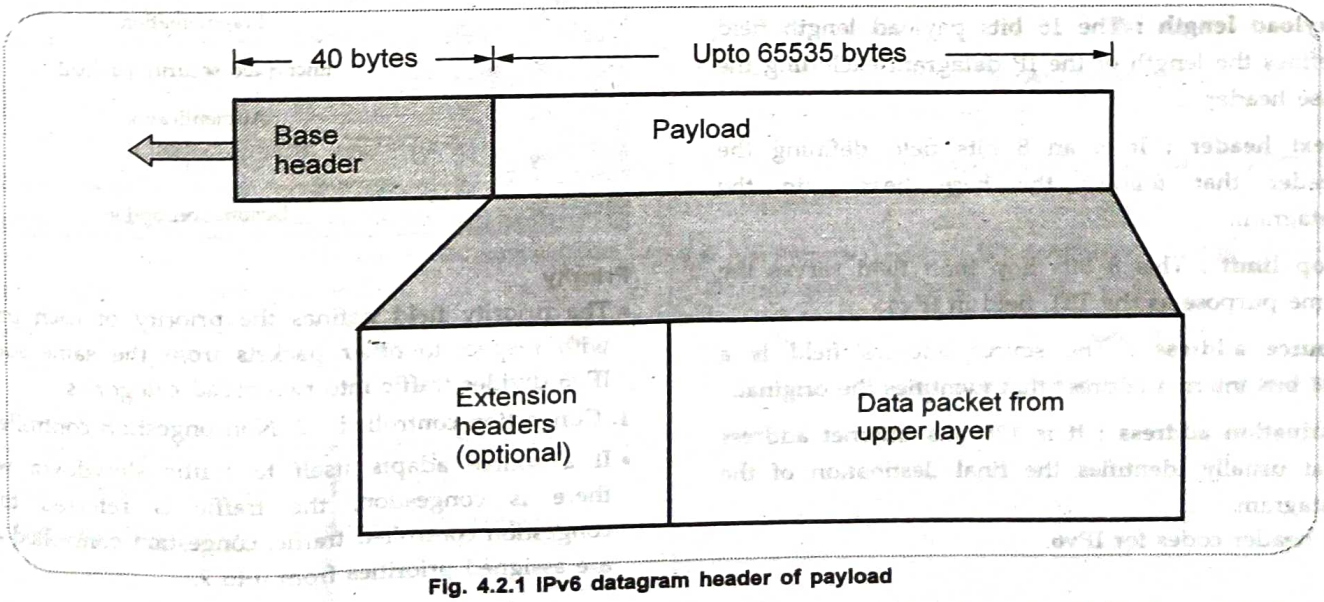


Fig. 4.2.1 IPv6 datagram header of payload

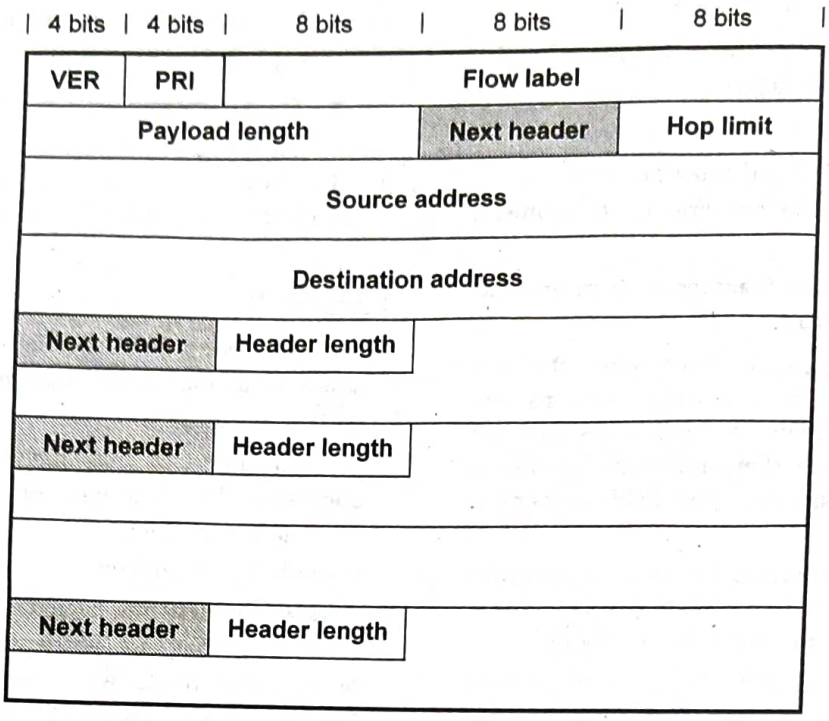


Fig. 4.2.2 IPv6 header

1. **Versions** : This 4 bits field defines the version number of the IP. The value is 6 for IPv6.
2. **Priority** : The 4 bits priority field defines the priority of the packet with respect to traffic congestion.
3. **Flow label** : It is 24 bits field that is designed to provide special handling for a particular flow of data.
4. **Payload length** : The 16 bits payload length field defines the length of the IP datagram excluding the base header.
5. **Next header** : It is an 8 bits field defining the header that follows the base header in the datagram.
6. **Hop limit** : This 8 bits hop limit field serves the same purpose as the TTL field in IPv4.
7. **Source address** : The source address field is a 128 bits internet address that identifies the original.
8. **Destination address** : It is 128 bits Internet address that usually identifies the final destination of the datagram.

Next header codes for IPv6.

Code	Next header
0	Hop by hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null
60	Destination option

Priority

- The priority field defines the priority of each packet with respect to other packets from the same source. IPv6 divides traffic into two broad categories

1. Congestion controlled 2. Noncongestion controlled

- If a source adapts itself to traffic slowdown when there is congestion, the traffic is referred to as congestion controlled traffic. congestion controlled data are assigned priorities from 0 to 7.

Priority	Meaning
0	No specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

- A priority of 0 is the lowest; a priority of 7 is the highest.
- Noncongestion controlled traffic refers to a type of traffic that excepts minimum delay. Discarding of packets is not desirable. Retransmission in most cases is impossible. Real time audio and video are examples of this type of traffic.
- Priority numbers from 8 to 15 are assigned to noncongestion controlled traffic.

4.3 IPSec Protocols

- Different application specific security mechanisms are developed such as electronic mail (PAG, S/MIME), client/server (Kerberos), web access (secure sockets layer). An IP level security can ensure secure networking not only for applications with security mechanisms but also for many security ignorant applications.
- IP Security (IPSec) is the capability that can be added to present versions of Internet Protocol (IPv4 and IPv6) by means of additional headers for secure communication across LAN, WAN and Internet.
- IPSec is a set of protocols and mechanism that provide confidentiality, authentication, message integrity and replay detection at IP layer. The device (firewall or gateway) on which the IPSec mechanism reside is called as **security gateway**.
- IPSec has two modes of operation.
  1. Transport mode
  2. Tunnel mode
- IPSec uses two protocols for message security.
  1. Authentication Header (AH) protocol.
  2. Encapsulating Security Payload (ESP) protocol.

4.3.1 Applications of IPSec

1. Secure connectivity over the Internet : A Virtual Private Network (VPN) can be established over the Internet. This reduces cost of private networks and network management overheads.

2. Secure remote access over the Internet : With IPSec, Secure access to a company network is possible.

3. Extranet and intranet connectivity : With IPSec, secure communication with other organizations, ensures authentication and confidentiality and provide a key exchange mechanism.

4. Enhanced electronic-commerce security : Use of IPSec enhances the security in electronic commerce applications.

4.3.2 IP Security Scenario

Fig. 4.3.1 shows an IP security scenario. (See Fig. 4.3.1 on next page)

- Many organizations have LAN at multiple places. The IPSec protocols are used which operates in networking devices e.g. router or firewall.
- The IPSec networking encrypt and compress the outgoing traffic while it decrypt and decompress all incoming traffic. These processes are transparent to workstations and servers on LAN.

4.3.3 Benefits of IPSec

1. IPSec provides strong security within and across the LANs.
2. IPSec in a firewall avoids bypass if all traffic from the outside must use IP.
3. No need to change software for implementing IPSec.
4. IPSec is below transport layer and hence is transparent to applications.
5. IPSec is transparent to end users also.
6. If required IPSec can provide security to individual users.

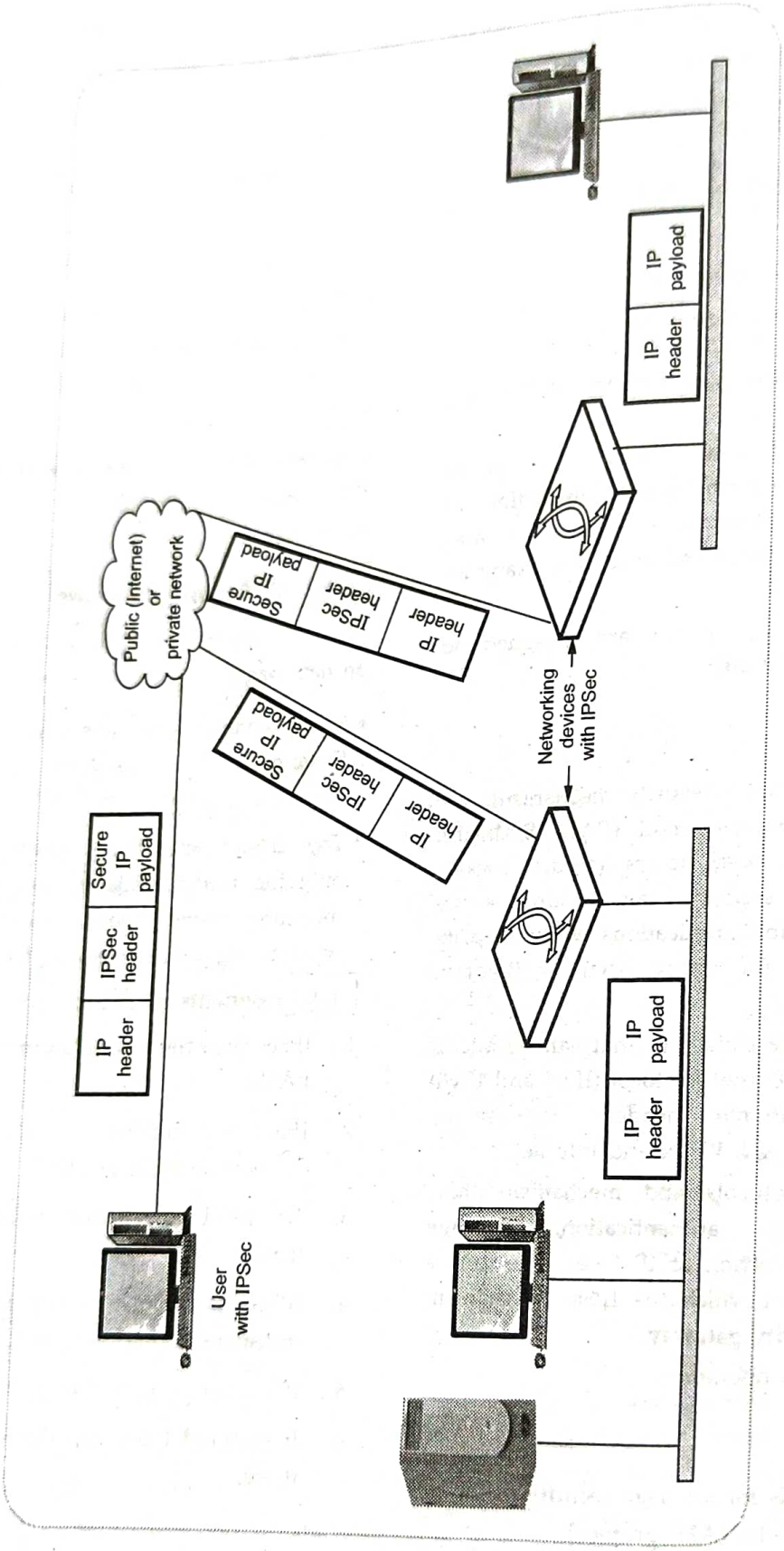


Fig. 4.3.1 IPSec scenario

Review Questions

1. *Describe IPsec protocol with its components and security services.*
2. *List and explain components of IPSec protocol.*

4.4 IP Security Architecture

- IPSec mechanism uses Security Policy Database (SPD) which determines how a messages are to handle also the security services needed and path the packet should take.
- Various documents are used to define complex IPSec specification. The overall architecture of IPSec is constituted by three major components.

1. IPSec documents
2. IPSec services
3. Security Associations (SA)

4.4.1 IPSec Documents

- IPSec specifications are described in various documents. Few important documents and specifications described are as under -

Sr. No.	Documents	Specifications
1.	RFC 2401	Overview of security architecture.
2.	RFC 2402	Packet authentication extension to IPv4 and IPv6.
3.	RFC 2406	Packet encryption extension to IPv4 and IPv6.
4.	RFC 2408	Key management capabilities

- All above specifications are essentially supported by IPv6 and are optional for IPv4. The security features are incorporated as extension header to the main IP header for both IPv4 and IPv6.
- The extension header for authentication is called as Authentication Header (AH) and the extension header for encryption is called as Encapsulating Security Payload (ESP) header.
- Besides RFC various other documents are published by Internet Engineering Task Force (IETF). These documents can be divided into seven groups.
- IPSec protocol consists of seven different groups of document as shown in Fig. 4.4.1.

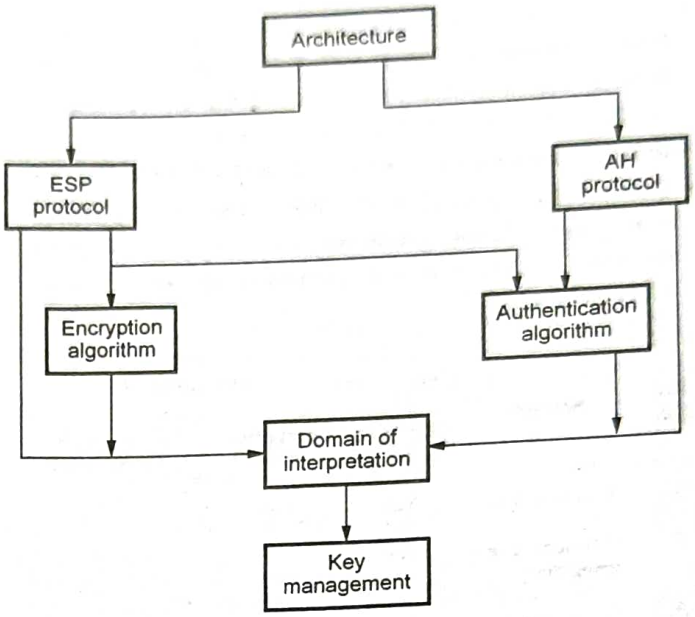


Fig. 4.4.1 IPSec document

1. **Architecture** : Covers security requirements, definitions, IPSec technology.
2. **Encapsulating Security Payload (ESP)** : Covers packet format, packet encryption authentication.
3. **Authentication Header (AH)** : Covers packet format, general issues.
4. **Authentication algorithm** : Encryption algorithms used for ESP.
5. **Key management** : Key management schemes.
6. **Domain of Interpretation (DoI)** : Values to relate documents with each other.

4.4.2 IPSec Services

- IPSec provides security serives at IP layer by selecting required security protocols, algorithms and cryptographic keys as per the services requested.
- Two protocols performs the function of providing security. These are authentication header protocol and protocol for encapsulating security payload. The services provide by these protocols are -

a. Access control
b. Connectionless integrity
c. Data origin authentication
d. Rejection of replayed packets
e. Confidentiality
f. Limited traffic flow confidentiality

IPSec protocol suit

- IP packet consists of two parts; IP header and data. IPSec features are incorporated into an additional IP header called extension header. Different extension headers are used for different services.
- IPSec defines two protocols : 1. AH 2. ESP
- The services provided by ESP protocol is possible with and without authentication option. Various services by AH and ESP protocols are summarized in Table 4.4.1.

Sr. No.	Service	AH protocol	ESP protocol	
			Encryption only	Encryption + Authentication
1.	Access control	Yes	Yes	–
2.	Connectionless integrity	Yes	–	Yes
3.	Data origin authentication	Yes	–	Yes
4.	Rejection of packets	Yes	Yes	Yes
5.	Confidentiality	Yes	Yes	Yes
6.	Limited traffic flow confidentiality	–	Yes	Yes

Table 4.4.1

4.4.3 Security Associations (SA)

- Security Association (SA) is the common between authentication and confidentiality mechanisms. An association is a one-way relationship between transmitter and receiver. For a two-way secure exchange two security associations are required.
- A security association is defined by parameters.
  1. Security Parameters Index (SPI)
  2. IP destination address
  3. Security protocol identifiers

1. Security Parameters Index (SPI) : SPI is a string of bit assigned to this SA and has local significance only. SPI is located in AH and ESP headers. SPI enables the receiving system under which the packet is to process.

2. IP destination address : It is the end point address of SA which can be end user system or a network system (firewall / router).

3. Security protocol identifiers : Security protocol identifier indicates whether the association is an AH or ESP security association.

4.4.4 SA Parameters

- A Security Association (SA) is normally defined by following parameters.

1. Sequence number counter : Sequence number counter is a 32-bit value that indicates the sequence number field in AH or ESP.

2. Sequence counter overflow : Sequence counter overflow is a flag used to indicate whether overflow of the sequence number counter should generate an auditable event and prevent further transmission of packets on SA.

3. Anti-replay window : Anti - replay window determines whether on inbound AH or ESP packet is a replay.

4. AH information : AH information includes authentication algorithm, keys, key life times and related parameters being used with AH.

5. ESP information : ESP information includes encryption and authentication algorithm, keys, initialization values required for ESP implementation.

6. IPSec protocol mode : IPSec protocol mode can be tunnel, transport or wildcard.

7. Path MTU : Path MTU means observed path maximum transmission unit which indicates maximum size of a packet that can be transmitted without fragmentation.

4.4.5 Transport Mode

- AH and ESP can support two modes of operation.
  1. Transport mode
  2. Tunnel mode
- Transport mode mainly provide protection for upper layer protocols. The protection extends to the payload of an IP packet. For example, TCP or UDP segment or ICMP packet.
- The transport mode is suitable for end-to-end communication between two workstations.
- In transport mode, ESP encrypts the IP payload excluding IP header. Authentication of IP payload is optional.
- AH authenticates the IP payload and specific portions of IP header.

4.4.6 Tunnel Mode

- Tunnel mode provides protection to entire IP packets. Security fields are added to IP packets and entire packet (AH or ESP packet + Security packet) is new IP packet with a new IP header.
- Entire new IP packet travels through a tunnel from one point to other over IP network. No router over the network are able to detect inner IP header. Since original packet is encapsulated by new larger packet having different source and destination address.
- Tunnel mode is preferred when one or both ends of an SA a security gateway such as a firewall or router that implements IPSec.
- In tunnel mode, number of hosts on network with firewalls may engage in secure transmission without IPSec. The unsecured packets generated are tunneled through external networks by tunnel mode SAs or IPSec in firewall or router.
- ESP encrypts and optionally authenticates the entire inner IP packet including IP header.
- AH authenticates the entire inner IP packet and selected portion of outer IP header.
- The tunnel mode and transport mode functionality is summarized in Table 4.4.2.

Protocol	Transport mode	Tunnel mode
AH	Authenticates IP paylaod and selected portion of IP header.	Authenticates entire IP packet and selected portion of outer IP header.
ESP	Encrypts IP payload and IPv6 extension headers.	Encrypts entire inner IP packet.
ESP with Authentication	Authenticates IP payload and not IP header. Encrypts IP payload and IPv6 header.	Authenticates inner IP packet. Encrypts entire inner IP packet.

Table 4.4.2

4.5 Authentication Header

- It provides support for data integrity and authentication of IP packets.
- Data integrity service insures that data inside IP packets is not altered during the transit.
- Authentication service enables and end user to authenticate the user at the other end and decides to accept or reject packets accordingly.
- Authentication also prevents the IP spoofing attack.
- AH is based on the MAC protocol, i.e. two communication parties must share a secret key.
- AH header format is shown in Fig. 4.5.1.

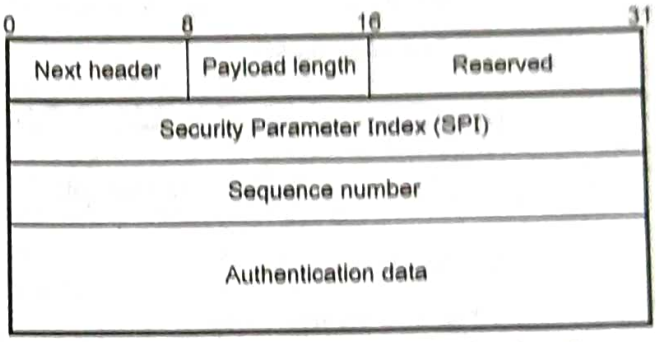


Fig. 4.5.1 IPSec authentication header format

1. **Next header** - This is 8-bits field and identifies the type of header that immediately follows the AH.
2. **Payload length** - Contains the length of the AH in 32-bit words minus 2. Suppose that the length of the authentication data field is 96-bits (or three 32-bit words) with a three word fixed header, then we have a total of 6-words in the header. Therefore this field will contain a value of 4.
3. **Reserved** - Reserved for future use (16-bit).
4. **SPI** - Used in combination with the SA and DA as well as the IPSec protocol used (AH or ESP) to uniquely identify the security association for the traffic to which a datagram belongs.
5. **Sequence number** - To prevent replay attack.

Replay attack

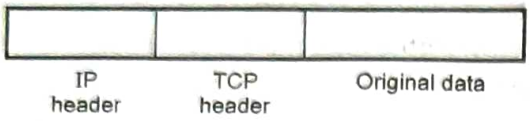
1. Suppose user A wants to transfer some amount to user C's bank account.
2. Both user A and C have the accounts with bank B.
3. User A might send an electronic message to bank B requesting for the funds transfer.
4. User C could capture this message and send a second copy of the message to bank B.
5. Band B have no idea that this is an unauthorized message.
6. User C would get the benefit of the funds transfer twice.

Authentication data

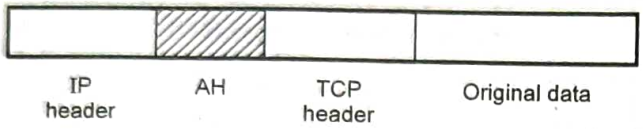
Also called Integrity check value for the datagram. This value is the MAC used for authentication and integrity purposes.

4.5.1 AH Transport Mode

- The position of the AH is between the original IP header and original TCP header of the IP packet.
- Fig. 4.5.2 shows the AH in transport mode.



(a) Before applying AH



(b) After applying AH

Fig. 4.5.2 Transport mode

4.5.2 AH Tunnel Mode

- The entire original IP packet is authenticated.
- AH is inserted between the original IP header and a new outer IP header.
- Fig. 4.5.3 shows AH tunnel mode.

4.6 ESP

- Encapsulating Security Payload (ESP) provides confidentiality services and limited traffic flow confidentiality. An authentication service is optional feature.

4.6.1 ESP Format

- Fig. 4.6.1 shows IPSec ESP format.

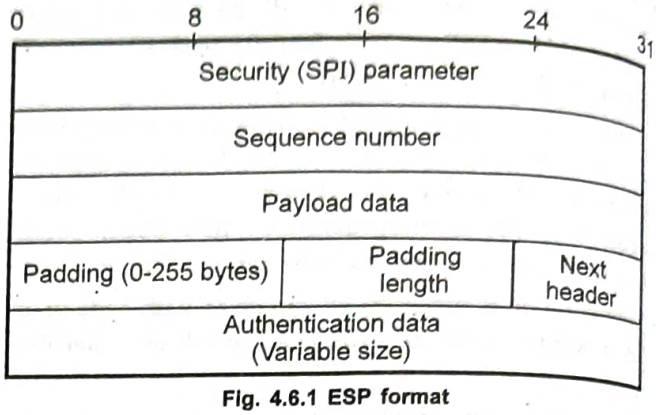
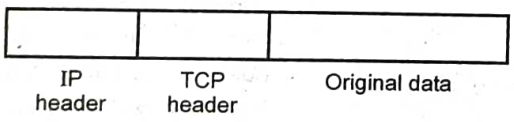
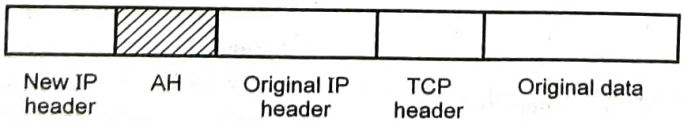


Fig. 4.6.1 ESP format

1. **SPI** - It is 32-bits field used in combination with the source and destination address. It identifies a security association.
2. **Sequence number** - This 32-bit field is used to prevent replay attacks.
3. **Payload data** - This is a transport level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
4. **Padding** - It contains the padding bits.
5. **Padding length** - Indicates the number of pad bytes immediately preceding this field.
6. **Next header** - It identifies the type of encapsulated data in the payload.
7. **Authentication data** - It is variable length field contains the authentication data called as the integrity check value for the datagram.



(a) Before applying AH



(b) After applying AH

Fig. 4.5.3 Tunnel mode

4.6.2 Encryption and Authentication Algorithms

- The payload data, padding, pad length and next header fields are encrypted by ESP.
- Various algorithms used for encryption are -

1. Three-key triple DES 2. RCS 3. IDEA
4. Three-key triple IDEA 5. CAST 6. Blowfish

4.6.3 Padding

- Padding field is used for various purposes such as

1. To expand the plain text if an encryption algorithm requires the plain text to be a multiple of number of bytes.
2. To assure the alignment of cipher text to make it integer multiple of 32-bits.
3. To provide partial traffic flow confidentiality by concealing the actual length of payload.

4.6.4 Comparison between AH and ESP

Sr. No.	AH	ESP
1.	Defined in RFC 2402	Defined in RFC 2406
2.	AH mandatory for IPv6 compliance.	Use of ESP with IPv6 is optional.
3.	Provides stronger authentication in transport mode.	Authentication provided is not as strong as AH.
4.	Requires less overhead since it only inserts a header into the IP packet.	Requires more overhead as it inserts a header and trailer.
5.	Provides connectionless integrity and data origin authentication for IPv4 and IPv6	Provides confidentiality, data origin authentication, connectionless integrity, an anti-reply service and limited traffic flow confidentiality.
6.	Protects as much of the IP header as possible as well as upper level protocol data.	It only protects those IP header fields that it encapsulates.
7.	It provides a packet authentication service.	It encrypts and /or authenticates data.

4.7 ISAKMP Protocol

- Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes.
- ISAKMP defines procedures and packet formats to establish, negotiate, modify and delete Security Associations.
- ISAKMP defines payloads for exchanging key generation and authentication data. These formats provide a consistent framework for transferring key and authentication data which is independent of the key generation technique, encryption algorithm and authentication mechanism.
- ISAKMP by itself does not dictate a specific key exchange algorithm; rather, ISAKMP consists of a set of message types that enable the use of a variety of key exchange algorithms.
- ISAKMP provides a "cookie" or an anti- clogging token (ACT) to make it easier to handle denial of service and prevents connection hijacking by linking the authentication, key exchange and Security Association exchanges.
- Fig. 4.7.1 shows ISAKMP header format.
- **Initiator cookie (8 bytes) :** The cookie of the entity that initiated SA establishment, SA notification, or SA deletion.
- **Responder cookie (8 bytes) :** The cookie of the entity that is responding to an SA establishment request, SA notification, or SA deletion.
- **Next payload (8 bits) :** Indicates the type of the first payload in the message.
- **Mj version (4 bits) :** The major version of the ISAKMP protocol in use.
- **Mn version (4 bits) :** The minor version of the ISAKMP protocol in use.
- **Exchange type (8 bits) :** Indicates the type of exchange being used. This dictates the message and payload orderings in the ISAKMP exchanges.
- **Flags (8 bits) :** Indicates the options that are set for the ISAKMP exchange
- **Message ID (4 bytes) :** A unique value used to identify the protocol state during Phase 2 negotiations. It is randomly generated by the initiator of the Phase 2 negotiation.
- **Length (4 bytes) :** The total length of the ISAKMP header and the encapsulated payloads in bytes. The

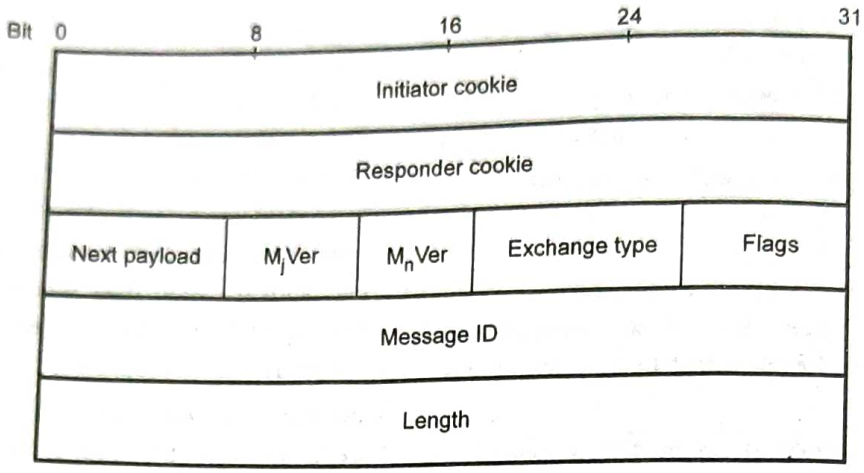


Fig. 4.7.1 ISAKMP header format

Length field of the ISAKMP header shows the total length of the message and the header together in octets.

4.7.1 OAKLEY Determination Protocol

- Key management is related to determination and distribution of secret keys. Four keys for communication between two applications : Transmitter and receiver pairs for both AH and ESP.
- Basically Oakley is a protocol to carry out the key exchange negotiation process for both peers, in which both ends after being authenticated can agree on secure and secret keying material.
- Oakley is based on the Diffie-Hellman key algorithm in which two gateways can agree on a key without the need to encrypt.
- Two users A and B agree on two global parameters : q, a large prime number and a primitive root of q.
- Secret keys created only when needed. Exchange requires no preexisting infrastructure. This algorithm is simple to use and did not require to much computational time.
- Authentication is used as part of the identity protection and since the oakley protocol uses the users public key we see a hash function used to retain the certification of these keys.
- Cookie generation criteria :
  1. must depend on the specific parties
  2. must not be possible for anyone other than the issuing entity to generate cookies that will be accepted by that entity
  3. cookie generation function must be fast to thwart attacks intended to sabotage CPU resources
  4. hash over the IP source & destination address, the UDP source and destination ports and a locally generated secret random value

Review Questions

1. *Explain OAKLEY key determination protocol.*
2. *Explain ISAKMP protocol for IP sec.*
3. *What is the role OAKLEY protocol in communication ?*

4.8 VPN

- Generalized architecture of VPN is shown in Fig. 4.8.1.
- Virtual Private Network (VPN) based on IPSec protocol are widely used for providing secure encrypted communication over insecure network, such as the internet. Asynchronous transfer mode (ATM)
- VPN can be implemented on the top of ATM.
- Authentication in IPSec is handled by the Internet Key Exchange (IKE) protocol.
- Virtual private network is a restricted to use logical computer network that is constructed from the system resources of a public and physical network such as the Internet, by using encryption.

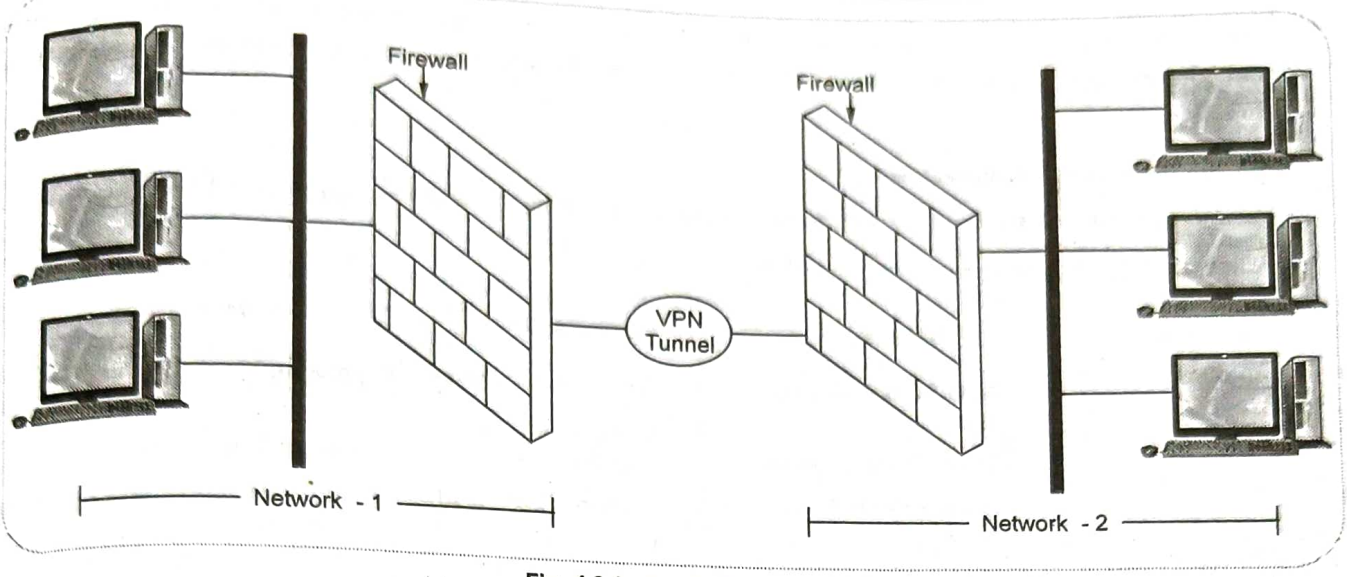


Fig. 4.8.1 VPN architecture

- VPN technology is based on a tunneling strategy. Tunneling involves encapsulating packets constructed in a base protocol format within some other protocol.
- In the case of VPNs running over the Internet, packets in one of several VPN protocol formats are encapsulated within IP packets.
- Following network protocols have become popular as a result of VPN developments : PPTP, L2F, L2TP, IPsec, SOCKS etc.
- Authentication allows VPN clients and servers to correctly establish the identity of people on the network.
- Encryption allows potentially sensitive data to be hidden from the general public.

4.8.1 Components of VPN

- A VPN connection includes the following components :

1. **VPN server** : A computer that accepts VPN connections from VPN clients.
2. **VPN client** : A computer that initiates a VPN connection to a VPN server. A VPN client can be an individual computer or a router.
3. **Tunnel** : The portion of the connection in which your data is encapsulated.
4. **VPN connection** : The portion of the connection in which your data is encrypted. For typical secure VPN connections, the data is encrypted and encapsulated along the same partion of the connection.
5. **Tunneling protocols** : Protocols that are used to manage tunnels and encapsulate private data. Data that is tunneled must also be encrypted to be a VPN connection.
6. **Tunneled data** : Data that is usually sent across a private point-to-point link.
7. **Transit internetwork** : The shared or public network crossed by the encapsulated data. The transit internetwork can be the Internet or a private IP-based intranet.

Review Questions

1. *State security measure applied by VPN for security.*
2. *What is VPN ? Explain types of VPN.*

4.9 WEB Security

- The Web is very visible. The WWW is widely used by businesses, government agencies, and many individuals. But the Internet and the Web are extremely vulnerable to compromises of various sorts, with a range of threats.
- Complex software hides many security flaws. Web servers are easy to configure and manage. Users are not aware of the risks.
- These can be described as passive attacks including eavesdropping on network traffic between browser and server and gaining access to information on a Web site that is supposed to be restricted.

- Active attacks including impersonating another user, altering messages in transit between client and server, and altering information on a Web site. The Web needs added security mechanisms to address these threats.

Web Traffic Security Approaches

- Various approaches are used for providing security to the Web. One of the examples is IP security.
- Following table shows the comparison of threats on the web.

Parameters	Threats	Consequences	Countermeasures
Integrity	1. Modification of user data 2. Trojan horse browser 3. Modification of memory 4. Modification of message traffic in transit	1. Loss of information 2. Compromise of machine 3. Vulnerability to all other threats	Cryptographic checksums
Confidentiality	1. Eavesdropping on the Net 2. Theft of information from server 3. Theft of data from client 4. Information about network configuration 5. Information about which client talks to server	1. Loss of information 2. Loss of privacy	Encryption, Web proxies
Denial of Service	1. Killing of user threads 2. Flooding machine with bogus requests 3. Filling up disk or memory 4. Isolating machine by DNS attacks	1. Disruptive 2. Annoying 3. Prevent user from getting work done	Difficult to prevent
Authentication	1. Impersonation of legitimate users 2. Data forgery	1. Misrepresentation of user 2. Belief that false information is valid	Cryptographic techniques

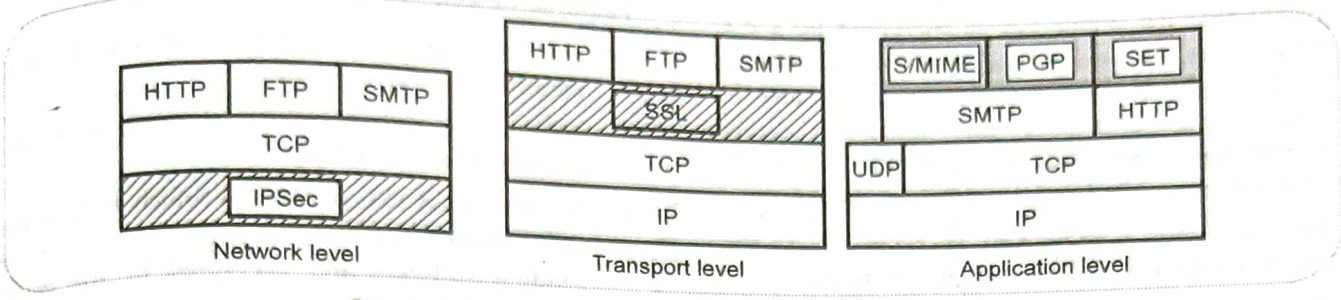


Fig. 4.9.1 Relative locations of security facilities in TCP/IP

- Fig 4.9.1 shows the relative location of security facilities in the TCP/IP protocol stack.

4.9.1 Transport Layer Security (TLS)

- Transport Layer Security (TLS) is a feature of mail servers designed to secure the transmission of electronic mail from one server to another using encryption technology. TLS can reduce the risk of eavesdropping tampering and message forgery mail communications.
- TLS is a security protocol from the Internet Engineering Task Force (IETF) that is based on the Secure Sockets Layer (SSL) 3.0 protocol developed by Netscape.
- TLS was designed to provide security at the transport layer. TLS is a non-proprietary version of SSL. For transactions on Internet, a browser needs :
  1. Make sure that server belongs to the actual vendor.
  2. Contents of message are not modified during transition.
  3. Make sure that the imposter does not interpret sensitive information such as credit card number.
- Fig. 4.9.2 shows the position of TLS in the protocol.

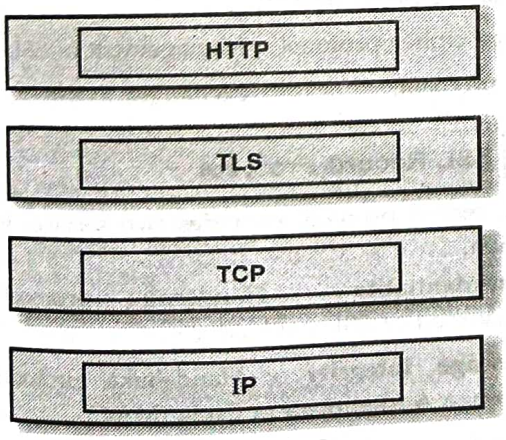


Fig. 4.9.2 TLS

- TLS has two protocols : Handshake and data exchange protocol
  1. **Handshake :** Responsible for negotiating security, authenticating the server to the browser and (optionally) defining other communication parameters. The TLS handshake protocol allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.
  2. **Data exchange (record) protocol :** Data exchange (record) protocol uses the secret key to encrypt the data for secrecy and to encrypt the message digest for integrity. The TLS record protocol is designed to protect confidentiality by using symmetric data encryption.

Handshake protocol

- Fig. 4.9.3 shows the TLS handshake protocol.

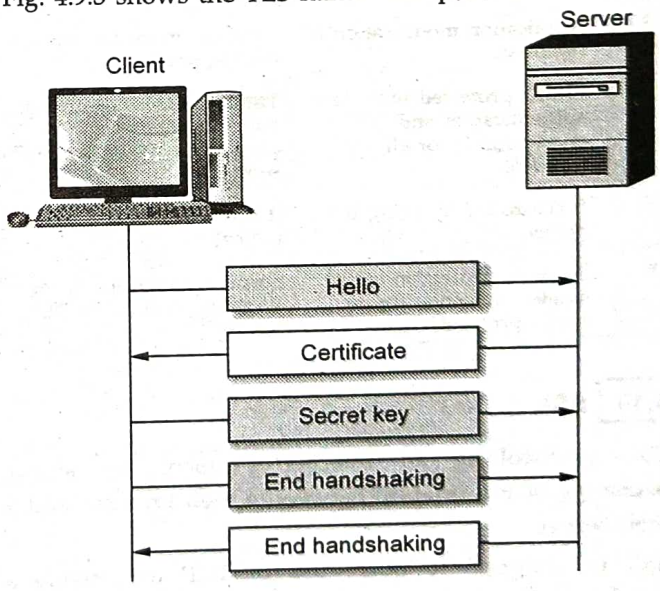


Fig. 4.9.3 TLS handshake protocol

1. Browser sends a hello message that includes TLS version and some preferences.
2. Server sends a certificate message that includes the public key of the server. The public key is certified by some certification authority, which

means that the public key is encrypted by a CA private key. Browser has a list of CAs and their public keys. It uses the corresponding key to decrypt the certification and finds the server public key. This also authenticates the server because the public key is certified by the CA.

3. Browser sends a secret key, encrypts it with the server public key and sends it to the server.
4. Browser sends a message, encrypted by the secret key to inform the server that handshaking is terminating from the browser key.
5. Server decrypts the secret key using it private key and decrypts the message using the secret key. It then sends a message, encrypted by the secret key, to inform the browser that handshaking is terminating from the server side.

4.9.2 Comparison between IPsec and TLS

Sr. No.	IPSec	TLS
1.	Type of security is device to device.	Type of security is application to application.
2.	It provides network segment protection.	It does not provides network segment protection.
3.	Application modification is required.	Application modification is not required.
4.	Traffic protected with data authentication and encryption is for all protocol.	Traffic protected with data authentication and encryption is only for TCP protocol.
5.	It controlled by using IPSec policy.	It controlled by using TLS policy.
6.	Scope of protection is for single connection for all traffic protocol.	Scope of protection is for single connection for TLS session.

4.10 SSL

- SSL protocol is an internet protocol for secure exchange of information between a web browser and a web server.
- SSL is designed to make use of TCP to provide a reliable end to end secure service.
- Secure Socket Layer (SSL) provides security services between TCP and applications that use TCP. The SSL protocol is an internet protocol for secure exchange of information between a web browser and a web server.

Features of SSL

1. SSL server authentication, allowing a user to confirm a server's identity.
2. SSL client authentication, allowing a server to confirm a user's identity.
3. An encrypted SSL session, in which all information sent between browser and server is encrypted by a sending software and decrypted by the receiving software.
4. SSL supports multiple cryptographic algorithms.

4.10.1 SSL Protocol Stack

SL uses TCP to provide reliable end-to-end secure service. SSL consists of two subprotocols, one for establishing a secure connection and other for using it. Fig. 4.10.1 shows SSL protocol stack.

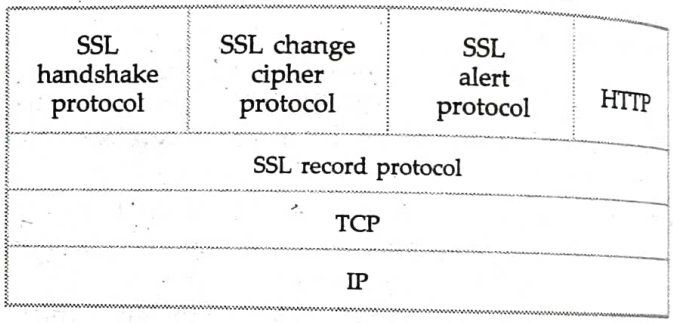


Fig. 4.10.1 SSL protocol stack

SSL record protocol : It provides basic security services to various higher layer protocols

HTTP : Provides the transfer service for web client/server interaction.

SSL handshake protocol,
SSL change cipher protocol, : Management of SSL
SSL alert protocol. exchanges.

4.10.2 SSL Record Protocol

- The SSL record protocol provides two services for SSL connection.
  1. **Confidentiality** - Handshake protocol for encryption of SSL payload.
  2. **Message integrity** - Handshake protocol for Message Authentication Code (MAC).
- SSL record protocol operation is shown in Fig. 4.10.2.

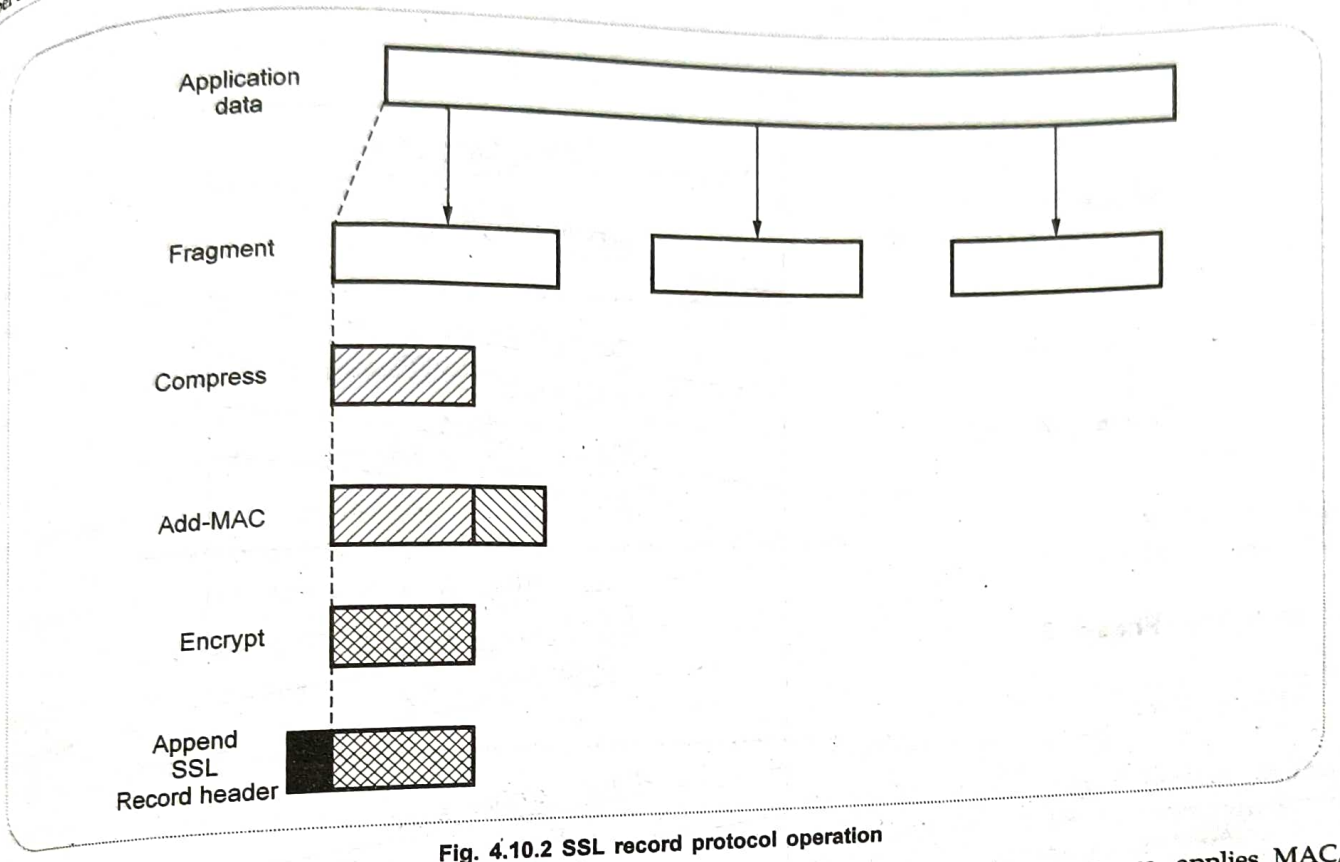


Fig. 4.10.2 SSL record protocol operation

- The record protocol takes application message to transmit, fragments the data, compress, applies MAC, encrypts, adds a header and transmits the TCP segment.

4.10.3 Handshake Protocol

- Handshake protocol allows the server and client to authenticate each other and to negotiate an encryption before transmitting application data various massages are used in protocol. Table 4.10.1 enlist these messages and there associated function.

Phase	Message type	Function
1.	Hello - request	Null
	Client - hello	Version, session id, cipher, compression
	Server - hellow	Version, session id, cipher, compression.
2.	Certificate	Chain of X.509 V3 certificates.
	Server - key - exchange	Parameters, signature.
	Certificate - request	Type, authorities.
	Server - done	Null
3.	Certificate - verify	Signature
4.	Client - key - exchange finished.	Parameters, signature hash value.

Table 4.10.1 SSL handshake protocol message types

Fig. 4.10.3 shows handshake protocol action.

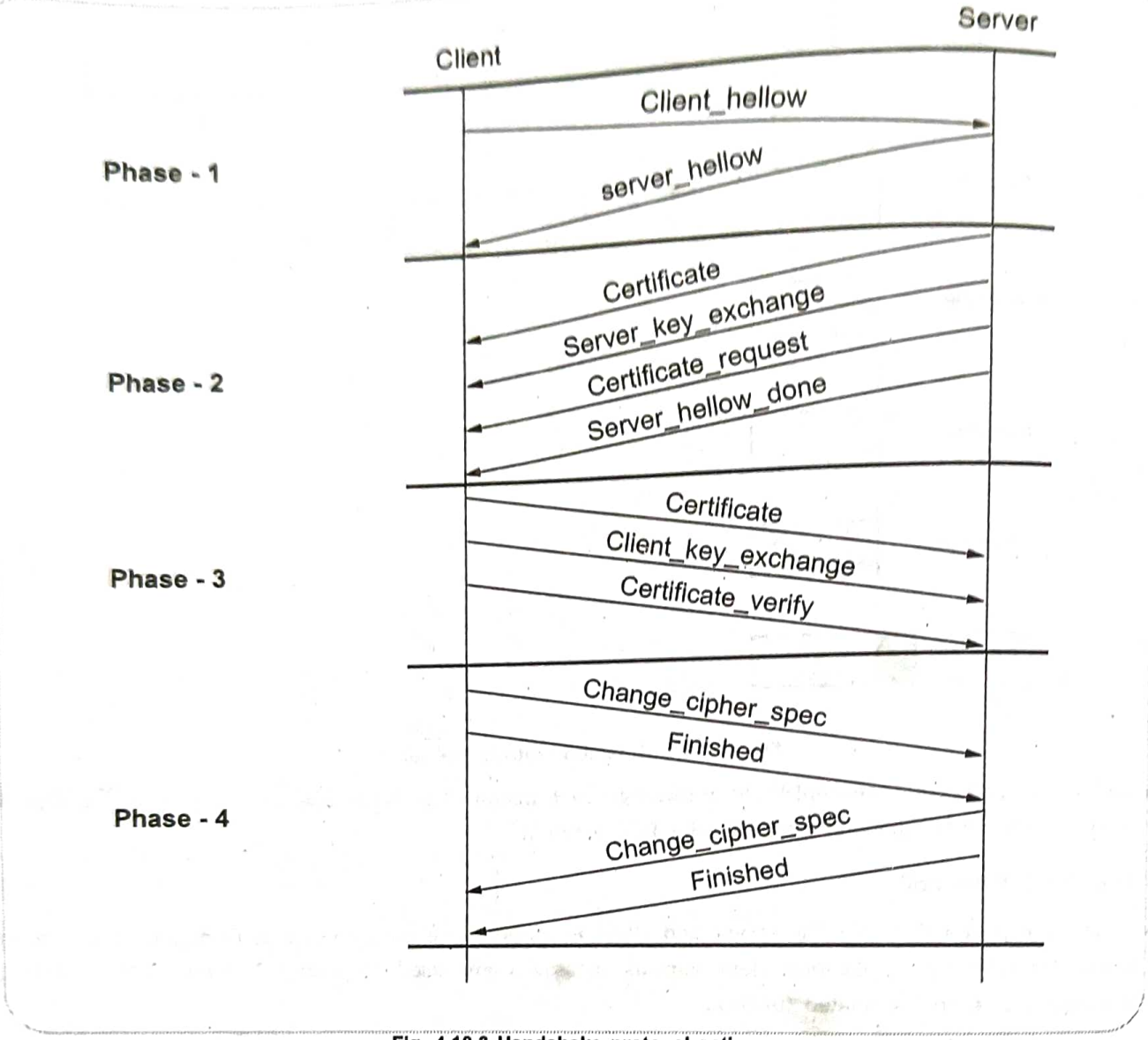


Fig. 4.10.3 Handshake protocol action

4.10.4 Change Cipher Spec Protocol

- The change cipher spec protocol is used to change the encryption being used by the client and server. It is normally used as part of the handshake process to switch to symmetric key encryption.
- This protocol consists of a single message which consists of a single byte with the value 1.
- The sole purpose of this message is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.
- The change cipher spec protocol exists to signal transitions in ciphering strategies. The protocol consists of a single message, which is encrypted and compressed under the current CipherSpec. The message consists of a single byte of value 1.
- The change cipher spec message is sent by both the client and server to notify the receiving party that subsequent records will be protected under the just-negotiated CipherSpec and keys.
- When the client or server receives a change cipher spec message, it copies the pending read state into the current read state.
- When the client or server writes a change cipher spec message, it copies the pending write state into the current write state.
- The client sends a change cipher spec message following handshake key exchange and certificate verify messages (if any), and the server sends one after successfully processing the key exchange message it received from the client.

4.10.5 Alert Protocol

- The Alert Protocol is used to convey SSL-related alerts to the peer entity.
- Alert messages are encrypted and compressed, as specified by the current connection state.
- Alert messages with a level of fatal, result in the immediate termination of the connection.
- In this case, other connections corresponding to the session may continue, however the session identifier must be cancel, preventing the failed session from being used to establish new connections.
- Each message in this protocol consists of two bytes. The first byte takes the value warning (1) or fatal (2) to convey the severity of the message.
- If the level is fatal, SSL immediately terminates the connection. Other connections on the same session may continue, but no new connections on this session may be established. The second byte contains a code that indicates the specific alert.

4.10.6 Comparison between IPSec and SSL

Sr. No.	Parameters	IPSec	SSL
1.	Position in the OSI model	Internet layer	Between transport and application layers
2.	Configuration	Complex	Simple
3.	NAT	Problematic	No problem
4.	Software location	Kernel area	User area
5.	Firewall	Not friendly	Friendly
6.	Installation	Vender non-specific	Vender specific
7.	Interoperability	Yes	No
8.	Deploy	More expensive to deploy, support and maintain	Less costly to deploy and maintain

4.10.7 Comparison of SSL and TLS

Sr. No.	SSL	TLS
1.	In SSL the minor version is 0 and the major version is 3.	In TLS, the major version is 3 and the minor version is 1.
2.	SSL use HMAC algorithm except that the padding bytes concatenation.	TLS makes use of the same algorithm the padding bytes concatenation.
3.	SSL supports 12 various alert codes.	TLS supports all of the alert codes defined in SSL 3 with the exception of no certificate.

Review Questions

1. *Explain secure socket layer handshake protocol in brief.*
2. *Explain the operation of Secure Socket Layer (SSL) protocol in detail.*
3. *Describe the operation of secure socket layer protocol in detail.*

4.11 Electronic Mail Security

- Email security describes various techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss, or compromise.
- Email remains a key productivity tool for today's organizations, as well as a successful attack vector for cyber criminals.

4.11.1 PGP

- PGP stands for Pretty Good Privacy. It was developed originally by Phil Zimmerman. However, in its incarnation as OpenPGP, it has now become an open standard. PGP is open-source. Although PGP can be used for protecting data in long-term storage, it is used primarily for email security.
- PGP is a complete e-mail security package that provides privacy, authentication, digital signatures, and compression all in an easy to use form.
- The complete package, including all the source code, is distributed free of charge via the Internet. Due to its quality, zero price, and easy availability on UNIX, Linux, Windows and Mac OS platforms, it is widely used today.
- PGP encrypts data by using a block cipher called IDEA, which uses 128-bit keys. IDEA is similar to DES and AES. Key management uses RSA and data integrity uses MDS.

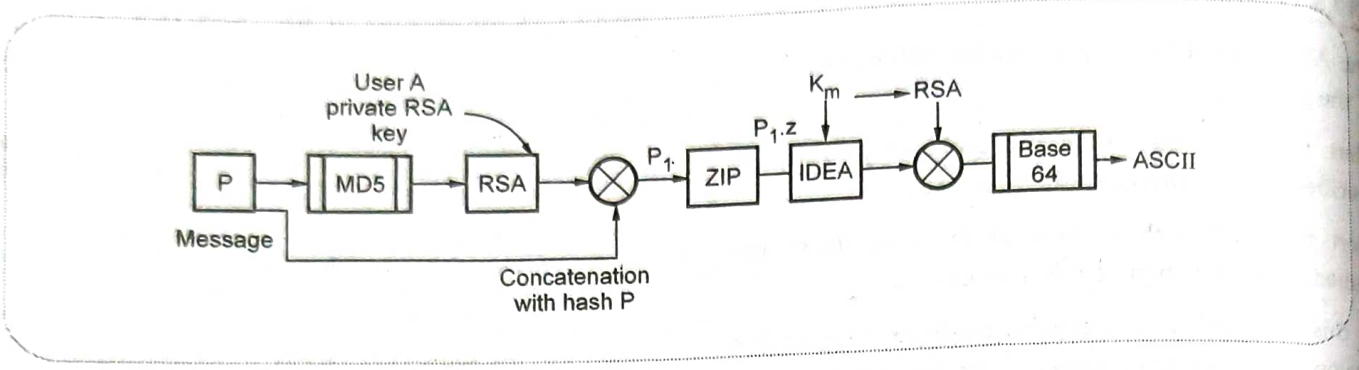


Fig. 4.11.1 PGP process

Characteristics of PGP

1. PGP is available free world wide.
2. PGP can run on various platform windows, UNIX and machintosh.
3. The algorithms used are extremely secure.
4. World wide acceptability.
5. PGP is not developed and controlled by government or standard organization.
6. PGP is on an Internet Standards track.

PGP works as follows

- Suppose user A wants to send a message (P) to user B in a secure way. Both the user have private and public RSA keys. Each user knows the other's user public key. User A uses PGP program for security purpose. At sender side i.e. at user A, PGP apply the hash function to the plain text message using MD5 and that message is encrypted. After encrypting again apply hash function using own private RSA key. Fig. 4.11.1 shows this process.
- When message is received by user B, he decrypts the hash with user A public key and verifies that the hash is correct. MD5 is the difficult to break. The encrypted hash and original message are concatenated into a single message P_1 and compressed using the ZIP program (P_1.Z).
- Using 128-bit IDEA message key (K_m), the ZIP program is encrypted with IDEA. Also K_m is encrypted with user B's public key (B_P). These two components are then concatenated and converted to base64.
- When this is received by user B, he reverses the base64 encoding and decrypts the IDEA key using his private RSA key. Using this key, user B decrypts the message to get P_1.Z. After decompressing P_1.Z, user B gets the plaintext message.
- For getting correct message, user B separates the plaintext from hash and decrypts the hash using user A public key. If the plaintext hash agrees with his own MD5 computation, user B knows that P is the correct message and that message came from user A.

Notation used in PGP

K_S = Session key used in conventional encryption scheme

PR_a = Private key of user A, used in public key encryption scheme

PU_a = Public key of user A, used in public key encryption scheme

EP = Pubilc key encryption

DP = Public key decryption

EC = Conventional encryption

DC = Conventional decryption

H = Hash function

|| = Concatenation

Z = Compression using ZIP algorith

R64 = Conversion to radix 64 ASCII format

4.11.1.1 PGP Operation

- PGP operation involves five different services.
  1. Authentication
  2. Confidentiality
  3. Compression
  4. E-mail compatibility
  5. Segmentation.

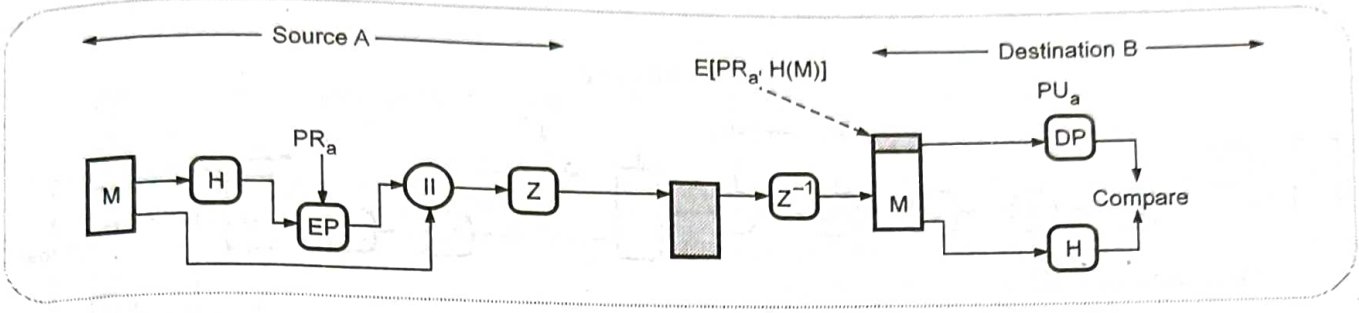


Fig. 4.11.2 Authentication

1. Authentication

- Signatures are attached to the message or file are detached signatures are also supported and are stored and transmitted separately from the message it signs.
- The digital signature is generated by either
  i) SHA-1 and RSA
  ii) DSS/SHA-1
- Sender authentication consists of the sender attaching his/her digital signature to the email and the receiver verifying the signature using public-key cryptography. Here is an example of authentication operations carried out by the sender and the receiver :
  1. At the sender's end, the SHA-1 hash function is used to create a 160-bit message digest of the outgoing email message.
  2. The message digest is encrypted with RSA using the sender's private key and the result prepended to the message. The composite message is transmitted to the recipient.
  3. The receiver uses RSA with the sender's public key to decrypt the message digest.
  4. The receiver compares the locally computed message digest with the received message digest.
- The description was based on using a RSA/SHA based digital signature. PGP also support DSS/SHA based signature. DSS stands for Digital Signature Standard. PGP also supports datached signatures that can be sent separately to the receiver. Detached signatures are also useful when a document must be signed by multiple individuals.
- Fig. 4.11.2 shows an authentication only.

2. Confidentiality

- Confidentiality is provided by encrypting messages to be transmitted. The algorithms used for encrypties are CAST-128, IDEA, 3DES with multiple keys.
- Only a portion of plaintext is encrypted with each key and there is no relationship with keys. Hence, the public key algorithm is secure.
- This service can be used for encrypting disk files. As you'd expect, PGP uses symmetric-key encryption for confidentiality. The user has the choice of three different block-cipher algorithms for this purpose : CAST-128, IDEA, or 3DES, with CAST-128 being the default choice.
  1. Sender generates message and random 128-bit number to be used as session key for this message only.
  2. Message is encrypted, using CAST-128 / IDEA/3DES with session key.
  3. Session key is encrypted using RSA with recipient's pulic key, then attached to message.
  4. Receiver uses RSA with its private key to decrypt and recover session key.
  5. Session key is used to decrypt message.
- Fig. 4.11.3 shows a confidentiality operation.

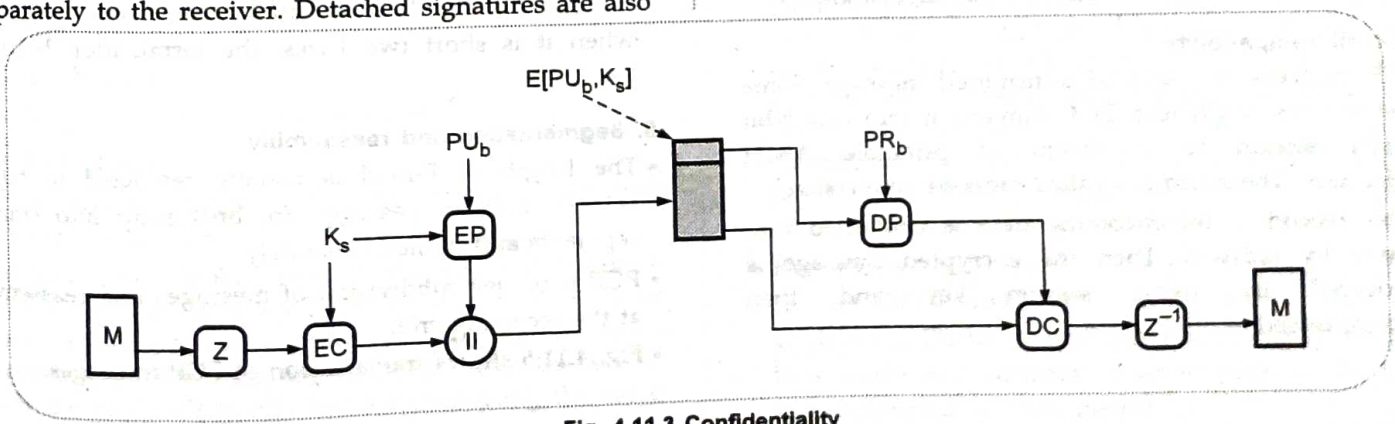


Fig. 4.11.3 Confidentiality

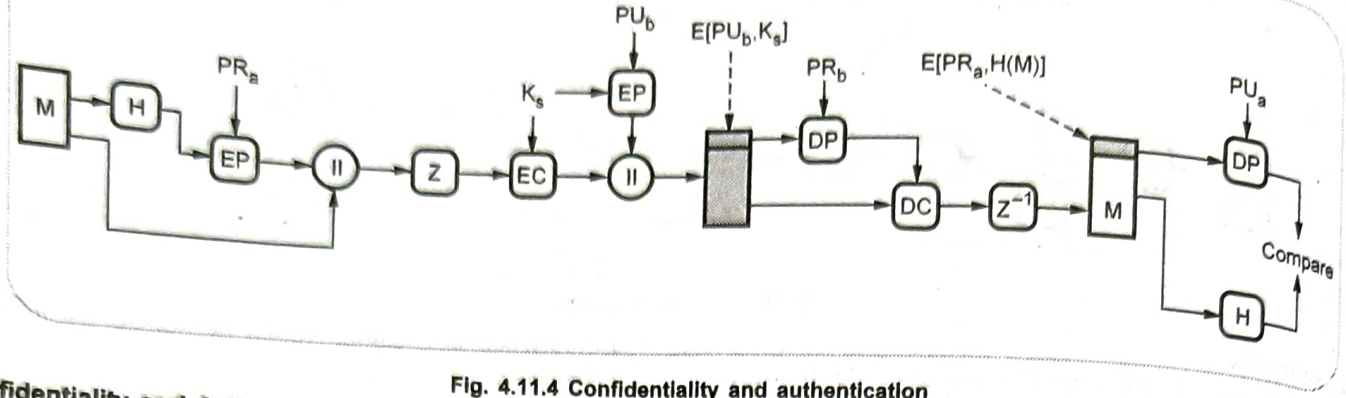


Fig. 4.11.4 Confidentiality and authentication

Confidentiality and Authentication

- May be both services used same message
  a. Create signature for plain text and attach to message
  b. Encrypt both message and signature using CAST - 128 or IDEA or TDEA
  c. Attach RSA encrypted session key
- Fig. 4.11.4 shows confidentiality and authentication.
- When both services are used, the sender first signs the message with its own private key, then encrypts the message with a session key, and then encrypts the session key with the recipient's public key.

3. Compression

- Before encryption, the message alongwith signature is compressed. Compression of message saves space and ease of transmission. PGP makes use of a compression package called ZIP. Another algorithm lampd-ZIV LZ77 is also used in zip compression scheme.
- By default PGP compresses the email message after applying the signature but before encryption. This is to allow for long-term storage of uncompressed messages along with their signatures. This also decouples the encryption algorithm from the message verification procedures.
- Compression is achieved with the ZIP algorithm.

4. E-mail compatibility

- PGP encrypts the block of transmitted message. Some system uses ASCII text, PGP converts it into raw 8-bit binary stream to a stream of printable ASCII characters. The scheme is called radix-64 conversion.
- After receiving, the incoming data is converted into binary by radix-64. Then the encrypted message is recovered by using session key and then decompressed.
- Since encryption, even when it is limited to the signature, results in arbitrary binary strings, and since many email systems only permit the use of ASCII characters, we have to be able to represent binary data with ASCII strings.
- PGP uses radix-64 encoding for this purpose.
- Radix-64 encoding, also known as Base-64 encoding has emerged as probably the most common way to transmit binary data over a network. It first segments the binary stream of bytes (the same thing as bytes) into 6-bit words.
- The 2^6 = 64 different possible 6-bit words are represented by printable characters as follows : The first 26 are mapped to the uppercase letters A through Z, the next 26 to the lowercase a through z, the next 10 to the digits 0 through 9, and the last two to the characters / and +. This causes each triple of adjoining bytes to be mapped into four ASCII characters.
- The Base-64 character set includes a 65th character, '=', to indicate how many characters the binary string is short of being an exact multiple of 3 bytes. When the binary string is short one byte, that is indicated by terminating the Base-64 string with a single '='. And when it is short two bytes, the termination becomes '=='.

5. Segmentation and reassembly

- The length of E-mail is usually restricted to 50,000 octecks. Longer messages are broken-up into smaller segments and mailed separately.
- PGP provides subdivision of messages and reassembly at the receiving end.
- Fig. 4.11.5 shows transmission of PGP messages.

Transmission of PGP message

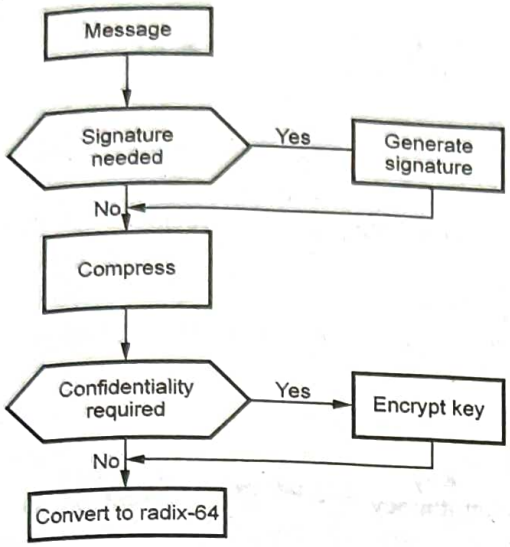


Fig. 4.11.5 Transmission of PGP message

Reception of PGP message

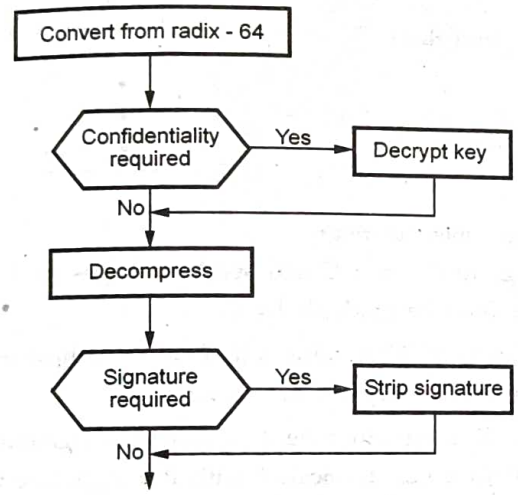


Fig. 4.11.6 Reception of PGP message

4.11.1.2 Cryptographic Keys and Key Rings

- PGP makes use of four types of keys
  1. One time session conventional keys
  2. Public keys
  3. Private keys
  4. Passphrase based conventional keys.

Key Management

- Three separate requirements can be identified with respect to these keys.
- As you have already seen public key encryption is central to PGP. It is used for two purposes : sender uses his/her private key for placing his/her digital signature on the outgoing message, and the sender uses the receiver's public key for encrypting the secret session key.
- We can expect people to have multiple public keys. This could happen because an individual in the process of retiring an old public key, but, to allow for a period of transition, decides to make available both the old and the new for a while. Some people may also choose to public multiple public keys for various reasons.
- So PGP must allow for the possibility that the receiver of message may have multiple public keys. This raises the following procedural questions :
  1. Let's say PGP uses one of the public keys made available keys that the sender has at the recipient know which public key it is.
  2. Let's say that the sender uses one of the multiple private keys that the sender has at his/her disposal for signing the message, how does the recipient know which of the corresponding public keys to use ?
- Both of these problems can be gotten around by the sender also sending along the public key used. The only problem here is that it is wasteful in space because the RSA public keys can be hundreds of decimal digits long.
- The PGP protocol solves this problem by using the notion of a relatively short **key identifiers (key ID)** and requiring that every PGP agent maintain its own list of private / public keys, along with their key identifiers, and a list of public keys, along with their associated key identifiers, for all the email correspondents.
- The former list is known as the private key ring and the latter as the public key right. The keys for a particular user are uniquely identifiable through a comination of the user ID and the key ID. The key ID associated with a public key consists of its least significant 64-bits.
- Going back to private key ring for security reasons, PGP stores the private keys in the table in an encrypted form so that the keys are only accessible to the user who owns them. PGP can use any of the three block ciphers at its disposal, CAST-128, IDEA and 3DES with CAST-128 serving as the default choice, for this encryption. The encryption algorithm asks the user to enter a pass-phrase. The pass-phrase is hashed with SHA-1 to yield a 160-bit hash code. The first 128-bits of the hash code are used as the encryption key by the CAST-128 algorithm. Both the pass-phrase and the hash code are immediately discarded.
- **Key Rings** with regard to the public key ring shown in the Table 4.11.1, the fields Owner Trust, Key Legitimacy, Signature and Signature Trust are to assess how much and siganture trust to place in the public keys belonging to other people.

Private Key IDs

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•
T_i	KU_i mod 2^{64}	KU_i	$E_{H(Pi)}$ [KR_i]	User i
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•

Private Key Ring

Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust (s)
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
T_i	KU_i mod 2^{64}	KU_i	trust_flag i	User i	trust_flag i		
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•

*= Field used to index table

Table 4.11.1 General structure of private and public key rings

- If A has B's public key in the ring, but the key really belongs to C, then C can send messages to A and forge B's signature and any encrypted messages from A to B would be readable by C.
- The values in the key legitimacy field column are computed by PGP. This value tells PGP as to how much trust to place in the public key in the corresponding row to be a valid key for the user ID.
- The entry stored in the public key field is actually a certificate. The signature field contains the signature of one or more certifying authorities on the certificate. Each signature has assoicated with it a signature trust field value that indicated how much trust PGP has in the signer of the certificate. The value for the key legitimacy field is derived from the value stored for the signature trust field.
- The entry in the owner trust field of the public-key-ring table indicates the extent to which the owner of a particular pulic key can be trusted to sign other certificates. This value is assigned by the user to whom the public-key-ring belongs.

4.11.1.3 Message Format

- The Fig. 4.11.7 shows the general format of a PGP message. As the figure shows, a PGP message consists of three components :

a) Session key component b) Signature component c) Actual email message

Notation used in message format

$E(PU_b, \bullet)$ = Encyrption with user b's public key

$E(PR_a, \bullet)$ = Encryption with user a's private key

$E(K_s, \bullet)$ = Encryption with session key

ZIP = Zip compression function

R64 = Radix-64 conversion function

- Perhaps the only unexpected entry is the leading two bytes of message digest. This is to enable the recipient to determine that the correct public key was used to decrypt the message digest for authentication. These two octets also server as a 16-bit frame check sequence for the actual email message. The message digest itself is calculated using SHA-1.
- **Message component** includes the actual data to be stored or transmitted, as well as a filename and a timestamp that specifies the time of creation.

Signature component consists of

a. **Timestamp :** The time at which the signature was made.

b. **Key ID of sender's public key :** Identifies the public key that should be used to decrypt the message digest.

c. **Leading two octets of message digest :** To enable the recipient to determine if the correct public key was used to decrypt the message digest for authentication, by comparing this plain text copy of the first two octets with the first two octets of the decrypted digest.

d. **Message digest :** The 160-bit SHA-1 digest encrypted with the sender's private signature key.

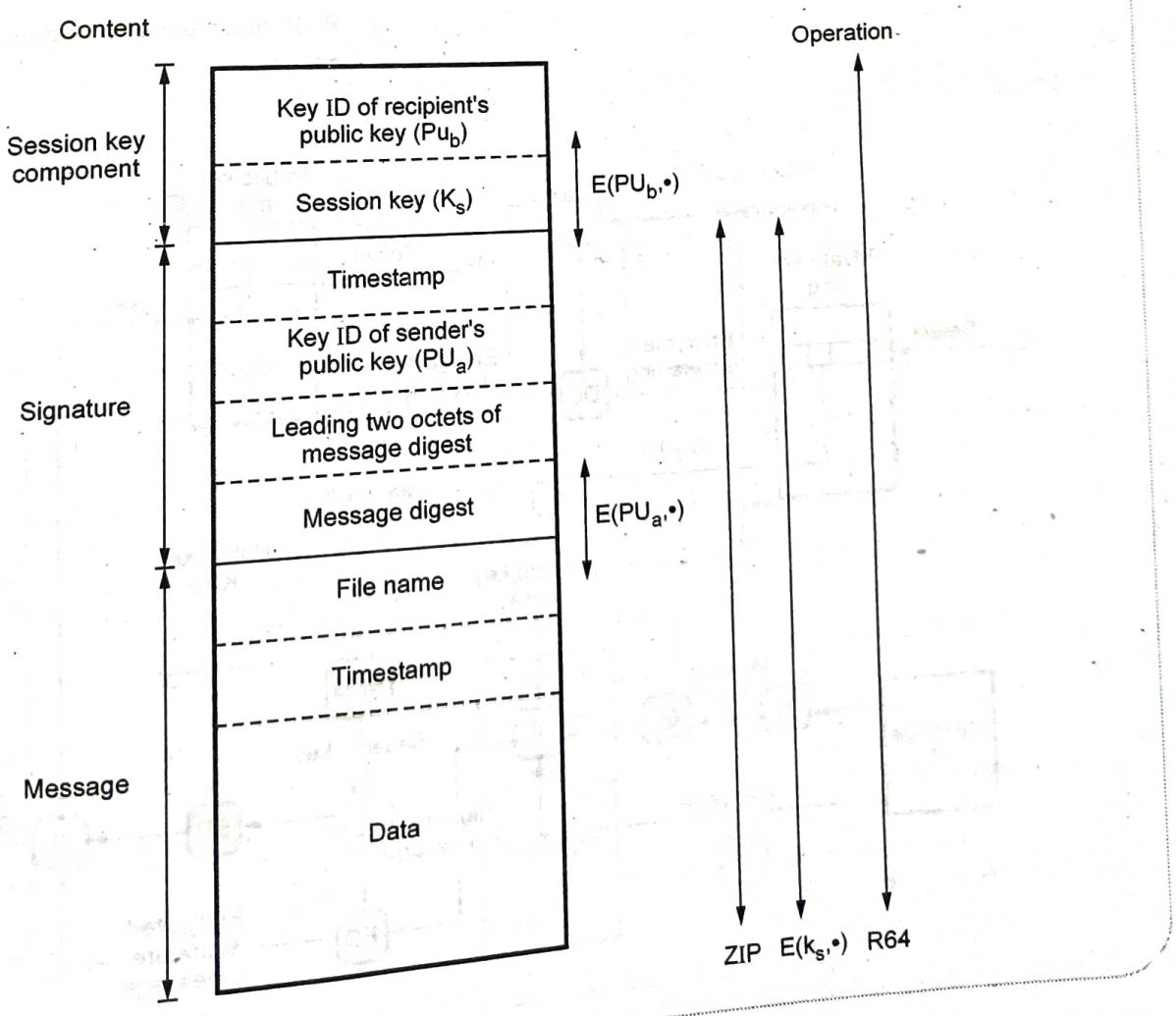


Fig. 4.11.7 General format of PGP message

- Session key component includes the session key and the identifier of the recipient's public key that was used by the sender to encrypt the session key.
- In the table, each row represents one the public / private key pairs owned by this user. Each row contains the following entries :
  1. **Timestamp** : The date or time when this key pair was generated.
  2. **Key ID** : The least significant 64 bits of the public key for this entry.
  3. **Public key** : The public key portion of the pair.
  4. **Private key** : The private key portion of the pair; this field is encrypted.
  5. **User ID** : This will be the user's e-mail address or to reuse the same user ID more than one.
- The private key itself is not stored in the key ring. Rather, this key is encrypted using CAST-128. The procedure is as follows :
  1. The user select a passphrases to be used for encrypting private keys.
  2. When the system generates a new public / private key pair using RSA, it ask the user for the passphrases. A 160-bit hash code is generated from the pass-phrase using SHA-1.
  3. The system encrypts the private key using CAST-128 with the 128-bits of the hash code as the key.
- PGP will retrieve the encrypted private key, generate the hash code of the pass-phrase, and decrypt the encrypted private key using CAST-128 with the hash code.

4.11.1.4 PGP Message Generation

- Fig. 4.11.8 shows PGP message generation.
- The sending PGP entity performs the following steps :

  a) Signs the message :

  i. PGP gets sender's private key from key ring using its user id as an index.

  ii. PGP prompts user for pass-phrase to decrypt private key.

  iii. PGP constructs the signature component of the message.

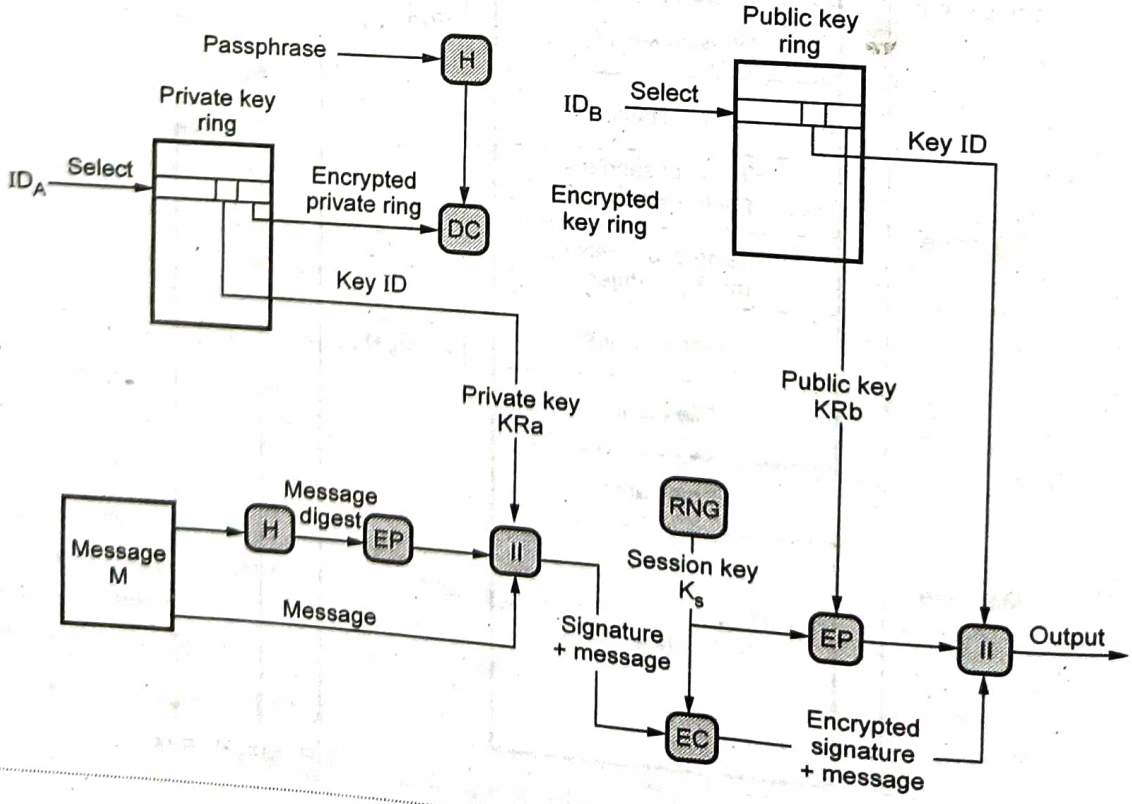


Fig. 4.11.8 PGP message generation

b) Encrypts the message :

i. PGP generates a session key and encrypts the message.

ii. PGP retrieves the receiver public key from the key ring using its user id as an index.

iii. PGP constructs session component of message.

4.11.1.5 PGP Message Reception

Fig. 4.11.9 shows PGP message reception.

The receiving PGP entity performs the following steps :

a) Decrypting the message :

i. PGP get private key from private-key ring using Key ID field in session key component of message as an index.

ii. PGP prompts user for pass-phrase to decrypt private key.

iii. PGP recovers the session key and decrypts the message.

b) Authenticating the message :

i. PGP retrieves the sender's public key from the public-key ring using the Key ID field in the signature key component as index.

ii. PGP recovers the transmitted message digest.

iii. PGP computes the message for the received message and compares it to the transmitted version for authentication.

4.11.1.6 Concept of Trust

- PGP uses trust field for trust information. These fields are
  1. Key legitimate field
  2. Signature trust field
  3. Owner trust field.

1. Key legitimate field : • Key legitimate field indicates the validity of the public key. i.e. extent to which PGP will trust.

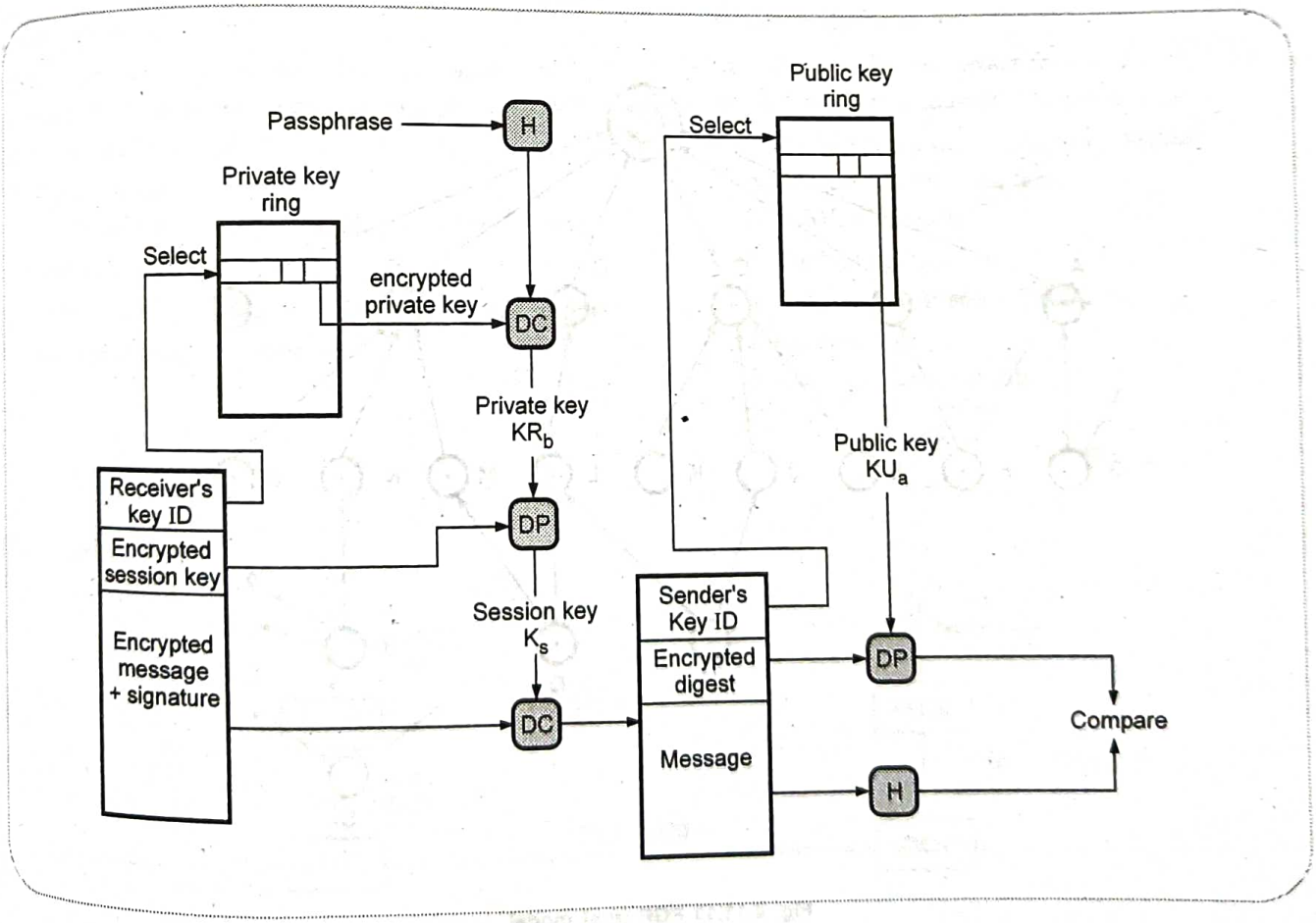


Fig. 4.11.9 PGP message reception

2. Signature trust field : • It indicates the degree to which PGP user trusts the signer to certify public keys.

3. Owner trust field : • It indicates the degree to which the public key is trusted to sign other public key certificates. This level is assigned by user.

4.11.1.7 Trust Processing Operation

- On the public key ring, user A inserts a new public key, then PGP assign a value to the trust flag which is associated with the owner of this public key. If the owner is user A, then this public key also appears in the private key ring and the value of ultimate trust is automatically assigned to the trust field.
- If user A is not the owner, PGP asks user A for his assessment of the trust to be assigned to the owner of this key, and user A must enter the desired level.
- The user can specify that this owner is unknown, untrusted or completely trusted.
- When the new public key is entered, one or more signatures may be attached to it.
- When a signature is inserted into the entry, PGP searches the public key ring to see if the author of this signature is among the known public key owners.
- The value of the key legitimacy field is calculated on the basis of the signature trust fields present in this entry.
- Fig. 4.11.10 shows PGP trust model example. It is an example of the way in which signature trust and key legitimacy are related. The figure shows the structure of a public key ring. The user has acquired a number of public keys.
- The node labeled "You" refers to the entry in the public key ring corresponding to this user. This key is legitimate and the OWNERTRUST value is ultimate trust.
- In this example, this user has specified that it always trusts the following user to sign other keys : D, E, F, L. This user partially trust users A and B to sign other keys.

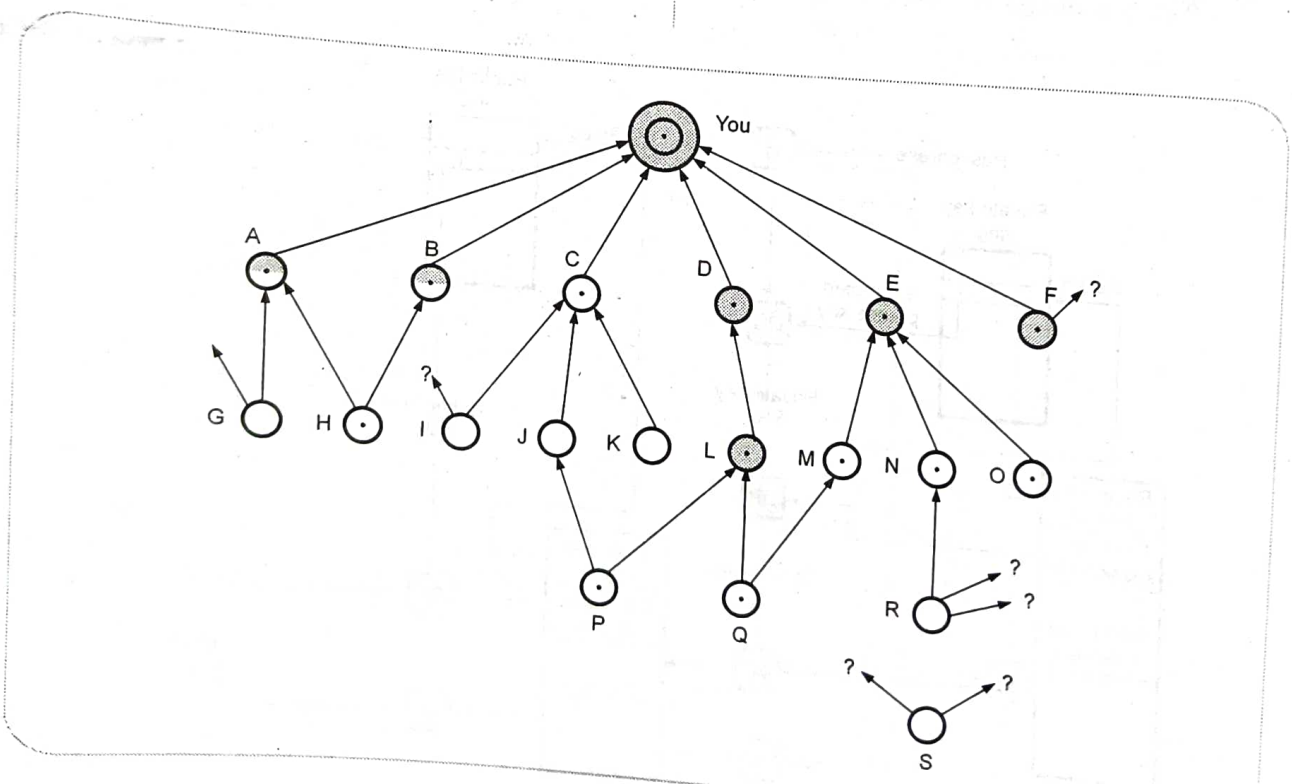
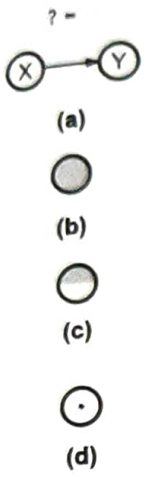


Fig. 4.11.10 PGP trust model

Notation used in above figure



- ? - = Unknown signatory
- X = X is signed by Y
- (b) = Key's owner is trusted by you to sign keys
- (c) = Key's owner is partly trusted by you to sign keys
- (d) = Key is deemed legitimate by you

4.11.2 S/MIME

- S/MIME is a Secure / Multipurpose Internet Mail Extension. It is a security enthancement to the MIME Internet e-mail format standard.
- RFC 822 defines a format for text messages that are sent using electronic mail. The RFC 822 standard applies only to the contents.
- MIME is an extension to the RFC 822 framework that is intended to address some of the problems and limitations of the use of SMTP.
- **SMTP limitations**
  1. SMTP cannot transmit executable files or binary objects.
  2. SMTP cannot transmit text data that includes national language characters.
  3. SMTP servers may reject mail message over a certain size.
  4. SMTP gateways to X.400 electronic mail networks cannot handle nontextual data included in X.400 messages.
  5. SMTP gateways that translate between ASCII and the character code EBCDIC do not use a consistent set of mappings, resulting in translation problems.

4.11.2.1 Multipurpose Internet Mail Extensions

- MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP.
- MIME defined by IETF to allow transmission of non-ASCII data via e-mail.
- It allows arbitary data to be encoded in ASCII for normal transmission.
- All media types that are sent or received over the world wide web (www) are encoded using different MIME types.
- Messages sent using MIME encoding include information that describes the type of data and the encoding that was used.
- RFC822 specifies the exact format for mail header lines as well as their semantic interpretations.
- Fig. 4.11.11 shows the working of MIME.
  - MIME define five headers.
    1. MIME - Version
    2. Content - Type
    3. Content - Transfer - Encoding
    4. Content - Id
    5. Content - Description

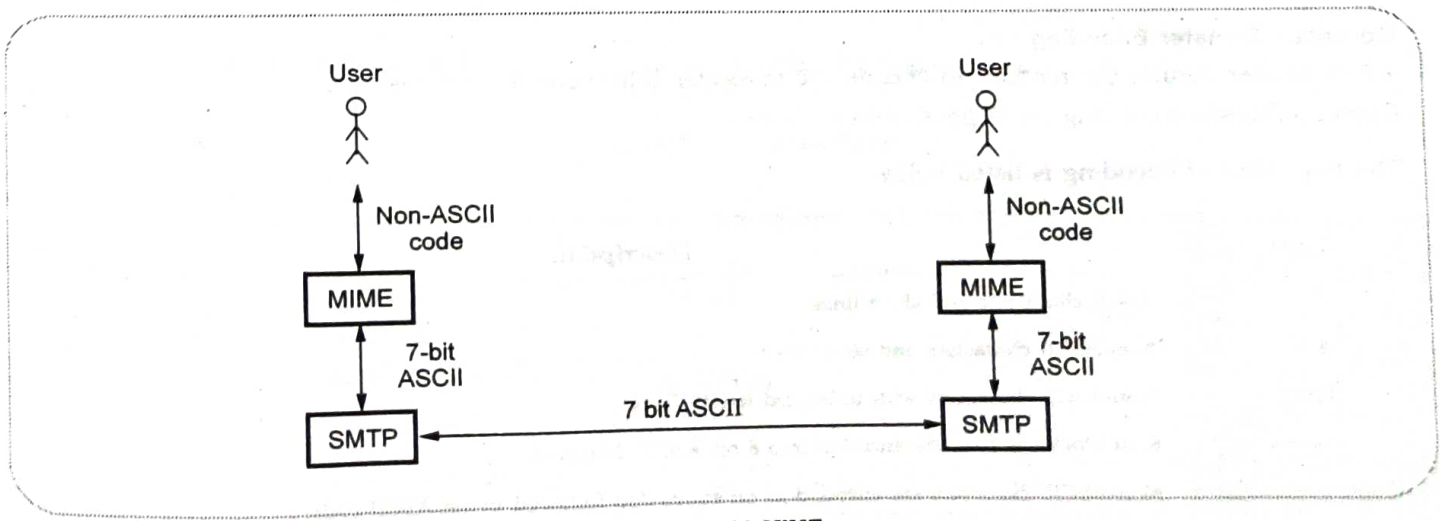


Fig. 4.11.11 MIME

Mail Message Header

- From : iresh@e-mail.com
- To : rupali@sinhgad.edu
- MIME - Version : 1.0
- Content - Type : image/gif
- Content - Transfer - Encoding : base64
- ..... data for the image .....
- ....
- ....

MIME Types and Subtypes

- Each MIME content - type must contain two identifiers :
- - Content type
- - Content subtype
- There are seven standardized content-types that can appear in a MIME content - type declaration.

Type	Subtype	Description
Text	Plain	Unformatted text
Multipart	Mixed	Body contains ordered parts of different data types
	Parallel	Same as above, but no order
	Digest	Similar to mixed, but the default is message
	Alternative	Parts are different versions of the same message
Video	MPEG	Video is in MPEG format
Audio	Basic	Single channel encoding of voice at 8 kHz. (Sound file)
Image	JPEG	Image is in JPGE format
	GIF	Image is in GIF
Message	Partial and external body	An entire e-mail message or an external reference to a message
Application	Postscript	Adobe postscript
	Octet stream	General binary data

Content - Transfer Encoding

- This header defines the method to encode the messages into 0 and 1 for transport.

Content-Transfer-Encoding : < Type >

The five types of encoding is listed below.

Type	Description
7 bit	ASCII characters and short lines.
8 bit	Non-ASCII characters and short lines.
Binary	Non-ASCII characters with unlimited length lines.
Base 64	6 bit blocks of data are encoded into 8 bit ASCII characters.
Quoted printable	Non-ASCII characters are encoded as an equal sign followed by an ASCII code.

Mail Message Format

- SMTP requires all data to be 7-bit ASCII characters and all non-ASCII data must be encoded as ASCII strings.
- Additional lines in the message header declare MIME content type.

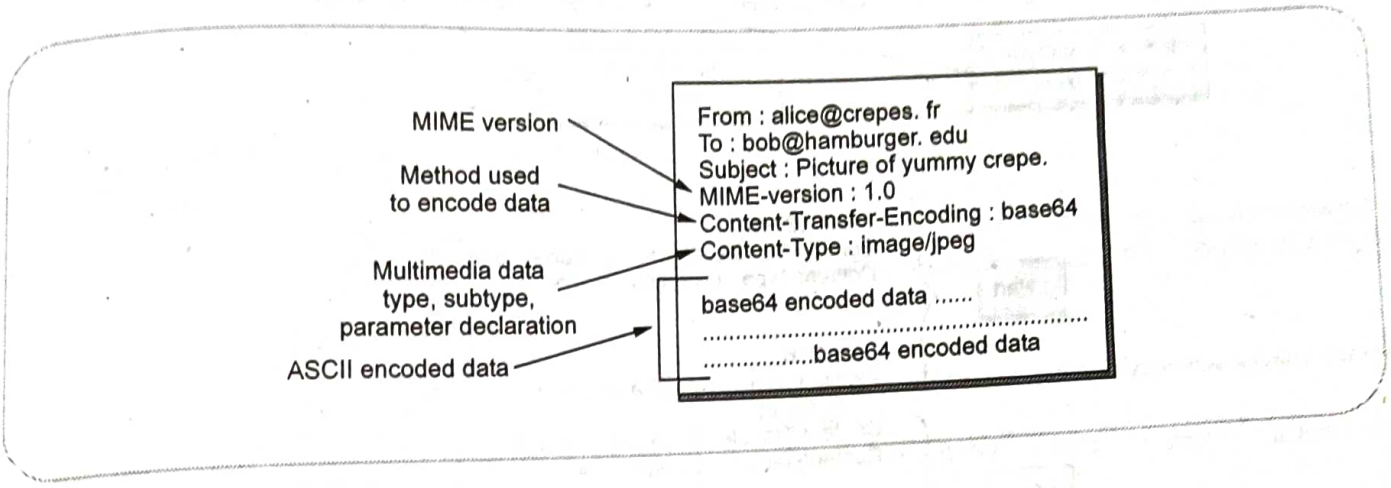


Fig. 4.11.12

4.11.2.2 Message Headers

- The message headers include the addresses of the receiver and the sender. Each header consists of the type of header, a colon, and the content of the header. Following is the sample of the complete header for a message.

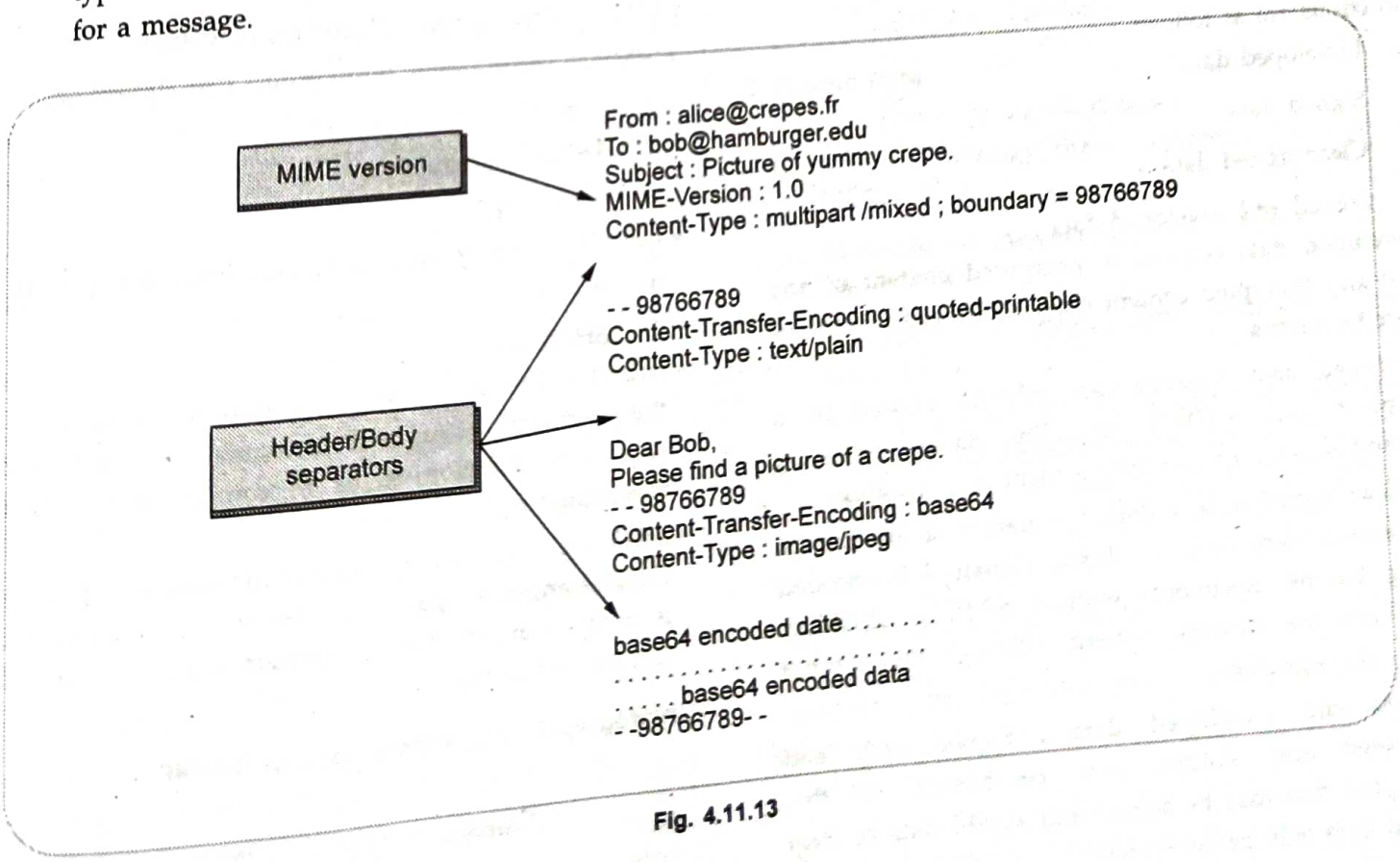


Fig. 4.11.13

Multipart Type

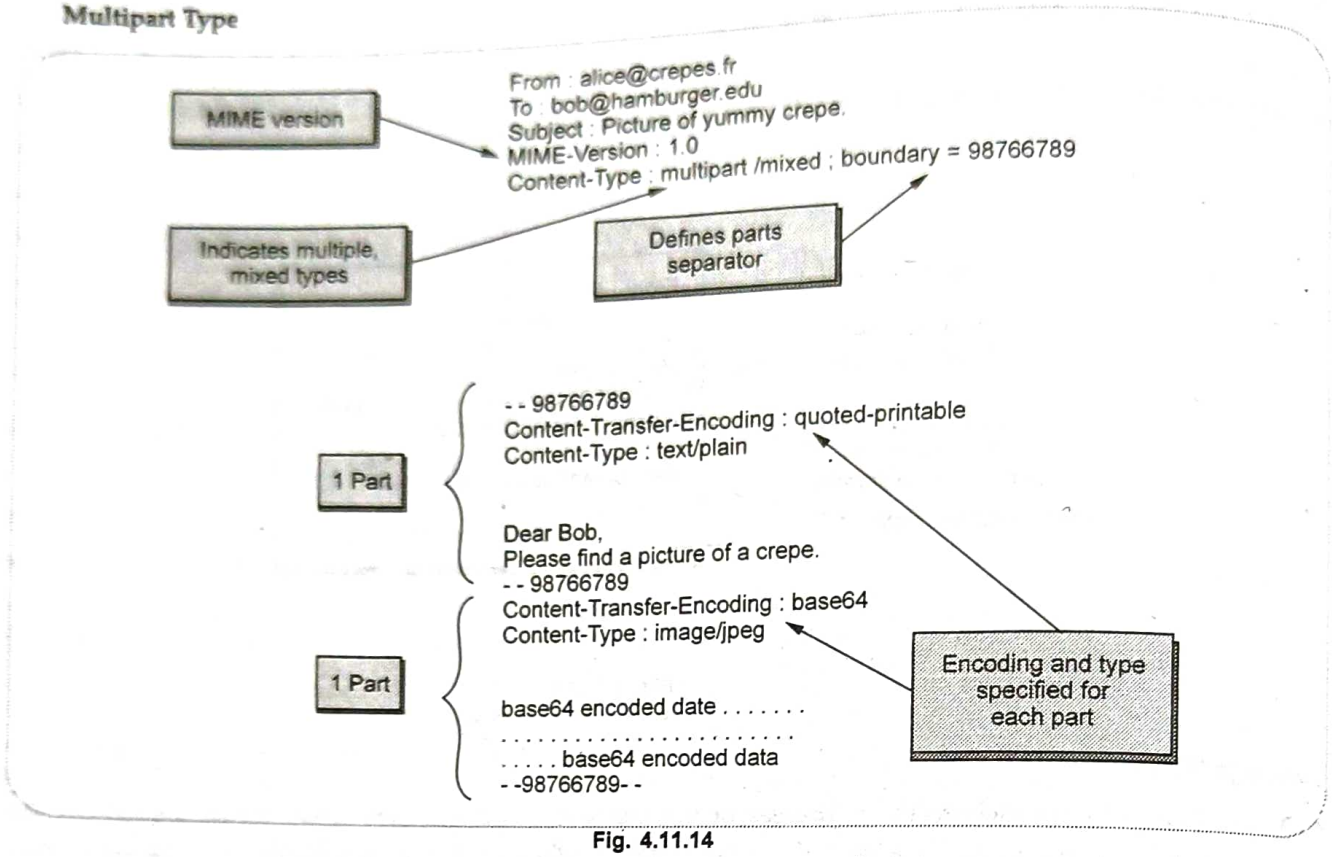


Fig. 4.11.14

4.11.2.3 S/MIME Functionality

- **Functions** are as follows
  1. Enveloped data
  2. Signed data
  3. Clear signed data
  4. Signed and enveloped data
- **Enveloped data** consists of encrypted content of any type and encrypted content encryption keys for one or more recipients.
- A **singed data** message can only be viewed by a recipient with S/MIME capability. Base64 encoding method is used for encoding content and signature.
- In **clear signed data**, a digital signature of the content is formed. Here only the digital signature is encoded using base64. Recipients without S/MIME capability can view the message content, although they cannot verity the signature
- **Signed and enveloped data** : Signed only and encrypted only entities may be nested, so that encrypted data may be signed and signed data or clear signed data may be encrypted.

4.11.2.4 Cryptographic Algorithms in S/MIME

- S/MIME incorporates three public key algorithms.
  1. Digital signature standard
  2. Diffie-Hellman
  3. Triple DES
- RFC 2119 specify the requirement level for S/MIME.
  1. MUST
  2. SHOULD
- **MUST** : The definition is an absolute requirement of the specification. An implementation must include this feature or function to be in comformance with the specification.
- **SHOULD** : There may exist valid reasons in particular circumstances to ignore this feature or function, but it is recommended that in implementation include the feature or function.

Cryptographic Algorithms used in S/MIME

Sr. No.	Function	Requirement
1.	Create message digest to be used in forming a digital signature.	a) MUST support SHA-1 and MD5. b) SHOULD use SHA-A .

2.	Encrypt message digest to form digital signature.	a) Sending and receiving agents MUST support DSS. b) Sending agents SHOULD support RSA encryption. c) Receiving agents SHOULD support verification of RSA signatures with key sizes 512 bits to 1024 bits.
3.	Encrypt session key for transmission with message.	a) Sending and receiving agents MUST support Diffie-Hellman. b) Sending agent SHOULD support RSA encryption with key sizes 512 bits to 1024 bits. c) Receiving agent SHOULD support RSA decryption.
4.	Encrypt message for transmission with one time session key.	a) Sending agents SHOULD support encryption with triple DES and RC2/40. b) Receiving agents SHOULD support decryption using 3DES and MUST support decryption with RC2/40.

4.11.2.5 S/MIME Messages

General procedures for S/MIME message preparation.

1. Securing a MIME Entity

- It secures a MIME entity with a signature, encryption, or both.
- A MIME entity may be an entire message, or if the MIME content type is multipart, then a MIME entity is one or more of the subports of the message.
- The MIME entity is prepared according to the normal rules for MIME message preparation.
- PKCS object is prepared by using MIME entity plus some security related data. Security related data item consists of an algorithm identifiers and certificates.
- The message to be send is converted to canonical form in all cases. For multipart message, the appropriate canonical form is used for each subpart.

) Enveloped Data

Steps for preparing an enveloped data

1. Generate a pseudorandom session key for a particular symmetric encryption algorithm.
2. For each recipient, encrypt the session key with the recipient's public. RSA key.
3. Prepare a block for each recipient. Block is known as RecipientInfo which contains the sender public key certificate, an identifier of the algorithm used to encrypt the session key and the encrypted session key.
4. Encrypt the message content with the session key.

Enveloped Data is encoded into base64. A sample message is as follows :

```
Content-Type : application / pkcs7-mime ;
smime-type=enveloped-data;
name=smime.p7m
Content-Transfer-Encoding : base64
Content-Disposition : attachment; filename=smime.p7m
rfvbn756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF46
7GhIGfHfYT6

7nHHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6j
H7756tbB9H
f8HHGTrfvhJhjH776tbB9HG4VQbnj567GhIGfHfYT6ghyH
hHUujpfyF4
0GhIGfHfQbnj756YT64V
```

- To recover the encrypted message, the recipient first strips off the base64 encoding. Then the recipient's private key is used to recover the session key. Finally, the message content is decrypted with the session key.

3) Signed Data

- Steps for preparing signed data are

1. Select a message digest algorithm i.e. SHA or MD5.
2. Compute the message digest, or hash function, of the content to be signed.
3. Encrypt the message digest with the signer's private key.
4. Prepare a block known as signerInfo. SignerInfo contains the signer's public key certificate, an identifier of the message digest algorithm, an identifier of the algorithm used to encrypt the message digest.

A sample message is as follows

```
Content-Type : application/pkcs7-mime; smime-type =
signed-data;
name=smime.p7m
Content-Transfer-Encoding : base64
Content-Disposition : attachment; filename=smime.p7m
```

567GhIGfHfYT6ghyHhHUujpfyF4f8HHGTrfvhJhjH776tbB
9HG4VQbnj7

77n8HHGT9HG4VQpfyF467GhIGfHfyYT6rfvbnj756tbBgh
yHhHUujhJhjH

HUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H7
n8HHGhyHh

6YT64V0GhIGfHfQbnj75

- The recipient first strips off the base64 encoding then the signer's public key is used to decrypt the message digest.

4) Clear Signing

- Clear signing is achieved using the multipart content type with a signed subtype. Message is sent "in the clear" because recipient with MIME capability but not S/MIME capability are able to read the incoming message.
- A multipart/signed message has two parts.
  1. MIME type 2. MIME content type
- If the first part is not 7 bit, then it needs to be encoded using base64 or quoted printable.
- Second part has a MIME content type of application and a subtype of PKCS7 signature.
- Following is a sample message :

```
Content-Type : multipart / signed;
    protocol="application/pkcs7-signature";
    micalg=shal; boundary=boundary42
---- boundary42
Content-Type : text/plain

This is a clear-signed message.
---- boundary42
Content-Type : application/pkcs7-signature;
name=smime.p7s
Content-Transfer-Encoding:base64
Content-Disposition : attachment;filename=sime.p7s
ghyHhHUujhJhjH77n8HHGTrfvbnj756tb9HG4VQpfyF467
GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756t
bB9HGTrfvbnj
n8HHGTrfvhJhH776tbB9HG4VQbnj7567GhIGfHfYT6ghy
HhUuujpfyF4
----boundary42----
```

5) Registation Request

- The certification request includes

a. Certification Request Info block

b. Identifier of the public key encryption algorithm

c. Signature of the certification RequestInfo block

- The certification RequestInfo blocks includes a name of the certificate subject and a bit-string representation of the users public key.

S/MIME content types

Type	Subtype	SMIME Parameter	Description
Multipart	Signed		A clear signed message in two parts : One is the message and the other is the signature
Application	pkcs 7-mime	Signed data	A signed S/MIME entity
	pkcs 7- mime	Enveloped data	An encrypted S/MIME entity
	pkcs 7-mime	Degenerate signed data	An entity containing only public key certificate
	pkcs 7-signature	–	The content type of the signature subpart of a multipart / signed message
	pkcs 10-mime	–	A certificate registration request message

4.11.2.6 S/MIME Certificate Processing

User Agent

- An S/MIME user has several key managed functions to performs :
  1. **Key generation :** A user agent SHOULD generate RSA key pairs with a length in the range of 768 to 1024 bits and MUST NOT generate a length of less than 512 bits.
  2. **Registration :** A user's public key must be registered with a certification authority in order to receive an X.509 public key certificate.
  3. **Certificate storage and retrivel :** A user requires access to a local list of certificate in order to verify incoming signatures and to encrypt outgoing messages.

Verisign Certificates

- Verisign provides a CA service that is intended to be compatible with S/MIME and a variety of other applications. Verisign issues X.509 certificates with the product name verisign Digital ID.

- Each Digital ID contains the following :
  a) Owner's public key
  b) Owner's name
  c) Expiration data of the Digital ID
  d) Serial number of the Digital ID
  e) Name of the certification authority that issued the Digital ID
  f) Digital signature of the certification authority that issued the Digital ID.

4.11.3 PEM

- Primary goal of PEM is to add security services for e-mail users in the internet community. Began in 1985 as an activity of the Privacy and Security Research Group (PSRG) and defined in RFCs 1421/1422/1423/1424.
- It consists of extensions to existing message processing software plus a key management infrastructure.
- Developed by IETF, to add encryption, source authentication and integrity protection to e-mail. Allows both public and secret long-term keys and message key is always symmetric. It also specifies a detailed certification hierarchy.
- Uses symmetric cryptoraphy to provide (optional) encryption of messages.
- The use of X.509 certificates is the base for public key management in PEM.
- This certification hierarchy supports universal authentication of PEM users.
- PEM can be used in a wider range of messaging environments. PEM represents a major effort to provide security for an application that touches a vast number of users within the Internet and beyond.
- PEM was designed to have backward compatibility with existing mail system.
- PEM depends on a successful establishment of the certification hierarchy that underlies asymmetric key management.
- **Problem :** PEM does not support security services to multimedia files (MIME)

PEM Security Services

1. Integrity, which ensures a message recipient that the message has not been modified en route.
2. Authenticity, which ensures a message recipient that a message was sent by the indicated originator.
3. Non-repudiation, which allows a message to be forwarded to a third party, who can verify the identity of the originator.
4. Confidentiality (optional), which ensures a message originator that the message text will be disclosed only to the desingated recipients.

PEM Message Processing

Step 1 :
- Uses the canonicalization specified by SMTP to ensure a uniform presentation syntax among a heterogeneous collection of computer systems.
- The shortcoming is that it restricts the input to 7-bit ASCII.
- The reason is that the Internet e-mail imposes the same restrictions.

Step 2 :
- A MIC is calculated over the canonicalized message to permit uniform verification in the heterogeneous environments.
- The cannonical (padded as required) message text is then (optionally) encrypted using a per-message symmetric key.
- The encryption action is performed only if the message is of type ENCRYPTED.

Step 3 :
- Renders an ENCRYPTED or MIC-ONLY message into a printable form suitable for transmission via SMTP.
- This encoding step transforms the (optionally encrypted) message text into a restricted 6-bit alphabet.
- A MIC-CLEAR messages are not subject to any portion of the third processing step.

PEM Message Types
- ENCRYPTED is a signed, encrypted and encoded (in step 3) message.
- MIC-ONLY is a signed, but not encrypted, encoded message.
- MIC-ONLY is a signed, but not encrypted, and message that is not encoded.
- Specially so it can be sent to a mixed set of recipients, some of whom use PEM and some do not.

PEM Message Delivery Processing (1)
- Recipient receives a PEM message.
- Scans the PEM header for the version and the type (ENCRYPTED, MIC-ONLY, MIC-CLEAR).

- If ENCRYPTED or MIC-ONLY then decode the 6-bit encoding back to ciphertext or canonical plaintext form.
- If ENCRYPTED then decrypt the symmetric message key using the private component of his public key pair and decrypt the message using the symmetric message key.
- Validate the public key of the sender by validating a chain of certificates.
- Validate the digital signature using the public component of the public key of the sender.
- The canonical form is translated into the local representation and presented to the recipient.

Review Questions

1. *What is backdoors and key Esorow in PGP ?*
2. *Explain working of PGP in detail.*
3. *What is S/MIME ? State operation of S/MIME in detail.*
4. *Explain working of S/MIME with secracy and authenticaiton.*
5. *What are the security services provided by PGP ?*

4.12 Secure Electronic Transaction (SET)

- SET is an encryption and security specification develop to protect credit card transactions through Internet SET is not a payment system but a set of security protocols for secured way for payment transactions
- SET is a complex specification defined in -
  1. Business description
  2. Programmer's guide
  3. Formal protocol definition

4.12.1 Services Provided by SET

1. SET provides a secure communication channel among all parties.
2. Provides trust by using X.509V3 digital certificates.
3. Ensures privacy.

4.12.2 Requirements for SET

- For secured payment processing over Internet following are the requirements of SET protocol specifications :
  1. Provide confidentiality of payment and ordering information.
  2. Ensure the integrity of all transmitted data
  3. Provide authentication about card holder
  4. Provide authentication about merchant
  5. Ensure use of best security practices and system design.
  6. Develop a protocol that does not depend on transport security.
  7. Facilitate interoperability between software and network.

4.12.3 Features of SET

1. Confidentiality of information.
2. Integrity of data.
3. Account authentication of card holder.
4. Merchant authentication.

4.12.4 SET Participants

- Following are the participants of SET system.
  a) Card holder b) Merchant
  c) Issuer d) Acquirer
  e) Payment gateway f) Certification authority
- The sequence of event in SET system is as follows :
  1. Customer opens an account
  2. Customer receives a certificate
  3. Merchant's certificate
  4. Customer places an order
  5. Verification of merchant
  6. Order and payment sent
  7. Request for payment authorization by merchant
  8. Merchant confirms order.
  9. Merchant provides goods or service
  10. Merchant requests payment

4.12.5 Key Technologies of SET

- **Confidentiality of information :** DES.
- **Integrity of data :** RSA digital signatures with SHA-1 hash codes.
- **Cardholder account authentication :** X.509v3 digital certificates with RSA signatures.
- **Merchant authentication :** X.509v3 digital certificates with RSA signatures.
- **Privacy :** Separation of order and payment information using dual signatures.

4.12.6 SET Supported Transactions

1. Card holder registration
2. Merchant registration
3. Purchase request
4. Payment authorization
5. Payment capture
6. Certificate query
7. Purchase inquiry
8. Purchase notification
9. Sale transaction
10. Authorization reversal
11. Capture reversal

4.12.7 Dual Signature

- Dual signature is needed for linking two messages that are intended for two different receiver Order Information and Payment Information (OI and PI).
- The operation of dual signature can be summarized as,

$$DS = E(PRc, [H(H(PI) \| (OI)])$$

where,

PRc, is customer's private signature key

PI is payment information

OI is order information

H is Hash function

|| is concatenation

E is encryption (RSA)

- Dual signature limit the information on need to know basis i.e. merchant does not need credit card number and bank does not need details of customer order. This provides extra protection interms of privacy.
- Fig. 4.12.1 shows implementation of dual signatures.

4.12.7.1 Why Dual Signature ?

- Suppose that customer send the merchant two messages :

1. The signed Order Information (OI)
2. The signed Payment Information (PI)

- In addition, the merchant passes the Payment Information (PI) to the bank. If the merchant can capture another Order Information (OI) from this customer, the merchange could claim this order goes with the Payment Information (PI) rather than the original. Dual signature confirms the payment is made for specific order.

A] DS Verification by Merchant

- The merchant has the public key of the customer obtained from the customer's certificate.
- Now, the merchant can compute two values :

  H(PIMD || H(OI)

  DKUC[DS]
- Should be equal.

B] DS Verification by Bank

- The bank is in possession of DS, PI the message digest for OI [OIMD], and the customer's public key, then the bank can compute the following :

  H(H(PI) || OIMD)

  DKUC[DS]

4.12.8 Process of SET

4.12.8.1 Purchase Request

- Browsing, selecting, and ordering is done.
- Purchasing involves four messages :

  i) Initiate request

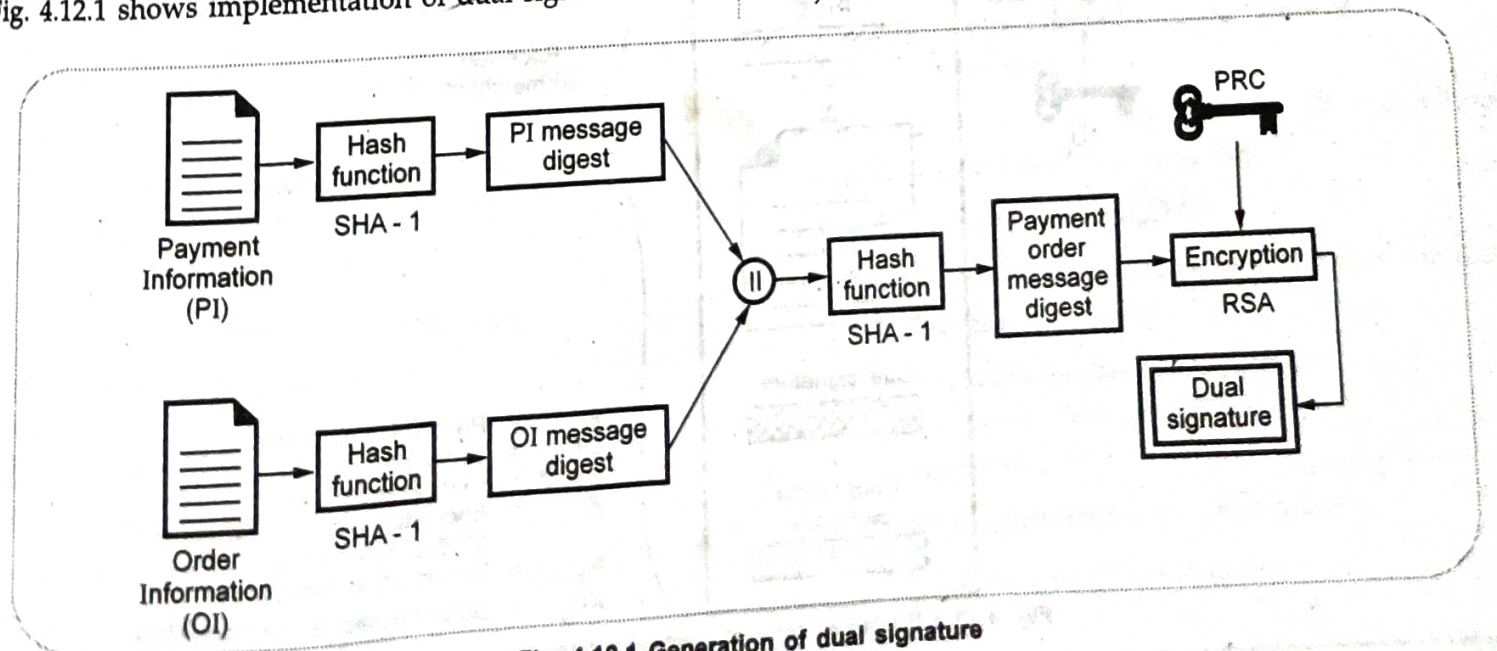


Fig. 4.12.1 Generation of dual signature

ii) Initiate response
iii) Purchase request
iv) Purchase response

i) Initiate Request

- Basic requirements :
  - Cardholder must have copy of certificates for merchant and payment gateway.
- Customer requests the certificates in the initiate request message to merchant.
  - Brand of credit card
  - ID assigned to this request/response pair by customer

ii) Initiate Response

- Merchant generates a response
  - Signs with private signature key
  - Include customer nonce
  - Include merchant nonce (returned in next message)
  - Transaction ID for purchase transaction
- In addition ...
  - Merchant's signature certificate
  - Payment gateway's key exchange certificate

iii) Purchase Request

- Cardholder verifies two certificates using their CA_s and creates the OI and PI
- Message includes :
  - Purchase-related information
  - Order-related information
  - Cardholder certificate
- The cardholder generates a one-time symmetric encryption key KS

Merchant Verifies Purchase Request

- When the merchant receives the purchase request message, it performs the following actions :
  - Verify the cardholder certificates by means of its CA signatures.
  - Verifies the dual signature using the customer's public key signature.

Processes the order and forwards the payment information to the payment gateway for authorization.

Sends a purchase response to the cardholder.

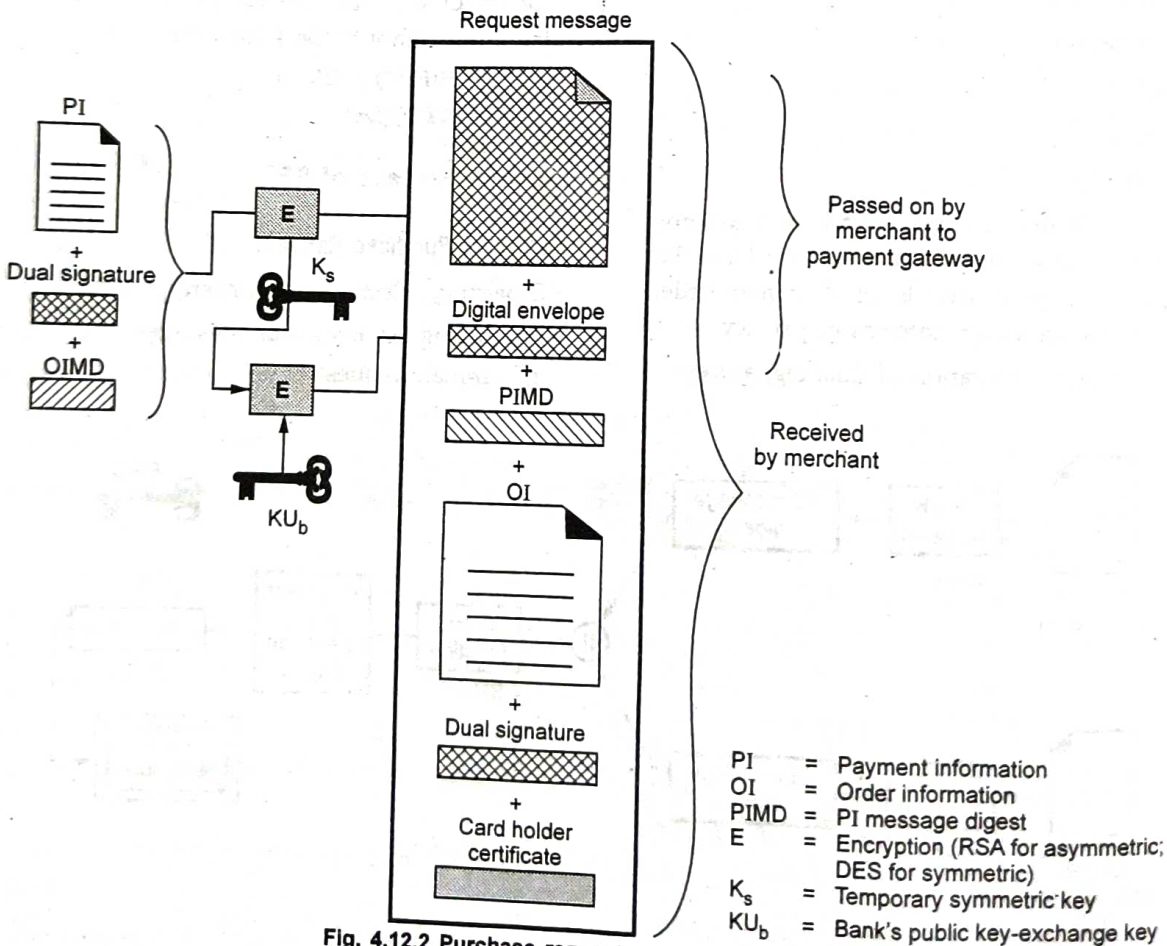


Fig. 4.12.2 Purchase request message generation

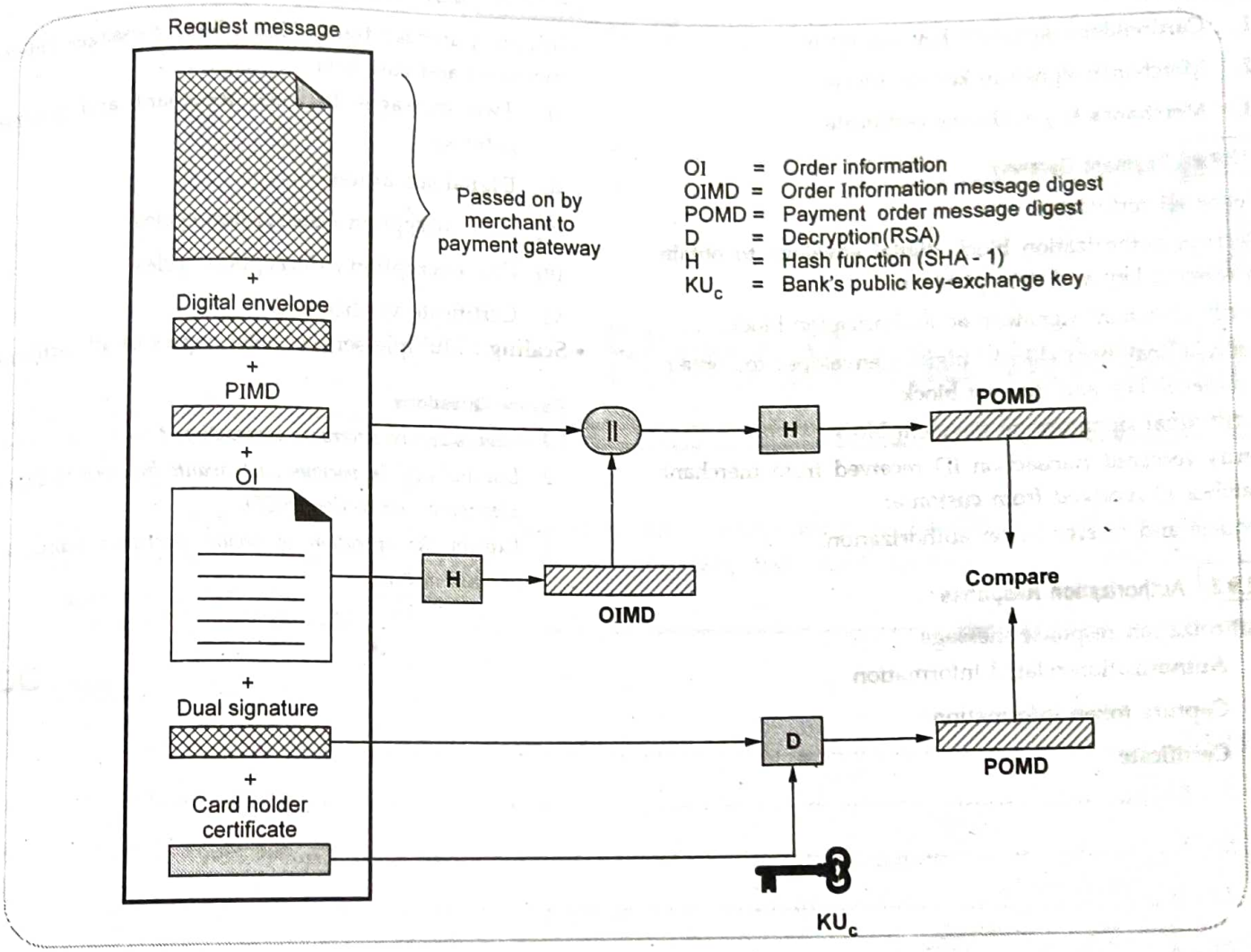


Fig. 4.12.3 Verification of purchase request

iv) Purchase Response Message

- Message that acknowledges the order and references corresponding transaction number.
- Block is,
  - Signed by merchant using its private key
  - Block and signature are sent to customer along with merchant's signature certificate
- Upon reception
  - Verifies merchant certificate
  - Verifies signature on response block
  - Takes the appropriate action

4.12.9 Payment Process

- The payment process is broken down into two steps :

1. Payment authorization
2. Payment capture

4.12.9.1 Payment Authorization

- The merchant sends an authorization request message to the payment gateway consisting of the following :
  - Purchase-related information
- Purchase Information (PI)
- Dual signature calculated over the PI and OI and signed with customer's private key.
- The OI Message Digest (OIMD)
- The digital envelope-authorization-related information
  - Certificates
  - Authorization-related information
- An authorization block including :
  - A transaction ID
  - Signed with merchant's private key
  - Encrypted one-time session key

- Certificates
  1. Cardholder's signature key certificate
  2. Merchant's signature key certificate
  3. Merchant's key exchange certificate

4.12.9.2 Payment Gateway

- Verify all certificates.
- Decrypt authorization block digital envelope to obtain symmetric key and decrypt block.
- Verify merchant signature on authorization block.
- Decrypt payment block digital envelope to obtain symmetric key and decrypt block.
- Verify dual signature on payment block.
- Verify received transaction ID received from merchant matches PI received from customer.
- Request and receive issuer authorization.

4.12.9.3 Authorization Response

- Authroization response message
  - Authorization-related information
  - Capture token information
  - Certificate

4.12.10 SET Overhead

- **Simple purchase transaction :** Four messages between merchant and customer
  i) Two messages between merchant and payment gateway
  ii) Digital signatures
  iii) RSA encryption / decryption cycles
  iv) DES encryption / decryption cycles
  v) Certificate verifications
- **Scaling :** Multiple servers need copies of all certificates

Review Questions

1. *What is secure electronic transaction ?*
2. *List and explain various participants involved in Secure Electronic Transaction (SET).*
3. *Explain the operation of secure electronic transaction protocol in brief.*

❑❑❑

Unit V

5 Firewall and Intrusion

Syllabus

Introduction, Computer Intrusions. Firewall Introduction, Characteristics and types, Benefits and limitations. Firewall architecture, Trusted Systems, Access Control. Intrusion detection, IDS: Need, Methods, Types of IDS, Password Management, Limitations and Challenges.

Contents

5.1 Introduction

- An intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system.
- Three classes of intruders are Masquerader, Misfeasor, and Clandestine user.
  1. **Masquerader** : An unauthorized user who penetrates a computer system's access control and gains access to user accounts.
  2. **Misfeasor** : A legitimate user who accesses resources he is not authorized to access. Who is authorized such access but misuses his privileges.
  3. **Clandestine user** : A user who seizes the supervisory control of the system and uses it to evade auditing and access control.

Intrusion techniques

- **Objective :** An intruder wants to gain access to a system.
- Access is generally protected by passwords. System maintains a file that associates a password with each authorized user.
- Password file can be protected with : **One-way encryption and access control**
  1. **One way function :** A system stores passwords only in encrypted form. When user presents a password, the system transforms that password and compares it with the stored value.
  2. **Access control :** Access to the password file is limited to very few people.

Techniques for guessing passwords

1. Try default passwords. (Used with standard accounts that is shipped with systems.)
2. Try all short words, 1 to 3 characters long.
3. Try all the words in an electronic dictionary.
4. Collect information about the user's hobbies, family names, birthday, etc.
5. Try user's phone number, social security number, street address, etc.
6. Try all license plate numbers (AP 12 AA 4453).
7. Use a trojan horse.
8. Tap the line between a remote user and the host system.

5.2 Computer Intrusions

- Computer intrusions occur when someone tries to gain access to any part of your computer system.
- Computer intruders or hackers typically use automated computer programs when they try to compromise a computer's security.
- A computer intrusion is a set of actions that violate the security of a system. Such a situation must be detected and corrected in order to guarantee the integrity, confidentiality and/or availability of computing resources.
- There are two basic intrusion detection systems : misuse detection and anomaly detection. Misuse detection systems attempt to match computer activities with previously known attacks in their database.
- An important draw-back of this type of system is that it can only detect known attacks, so attacks that are not stored or variants of stored attacks will not be detected.
- Anomaly detection systems learn the normal activity of the system and attempt to detect any computer activity that deviates from normal patterns.

5.3 Firewall Introduction

- Information systems in an organization have changed vary rapidly over the years from centralized data processing, LANs, WANs and Internet connectivity.
- The Internet connectivity is essential for the organization enabling access to outside world. Also it is a threat to the organization if not secured from intrusions (unauthorized access/users).
- A firewall is inserted between the Internet and LAN for security purpose. The firewall protects the LAN from Internet-based attacks and also provides security and audits.
- A firewall may be a hardware or a software program running on a secure host computer. A firewall is placed at junction or gateway between the two networks.
- A firewall must have at least two network interfaces one for the network it is intended to protect and one for the network and other for the network it is exposed to. A firewall placed between a private or corporate network and a public network (Internet) is shown in Fig. 5.3.1.

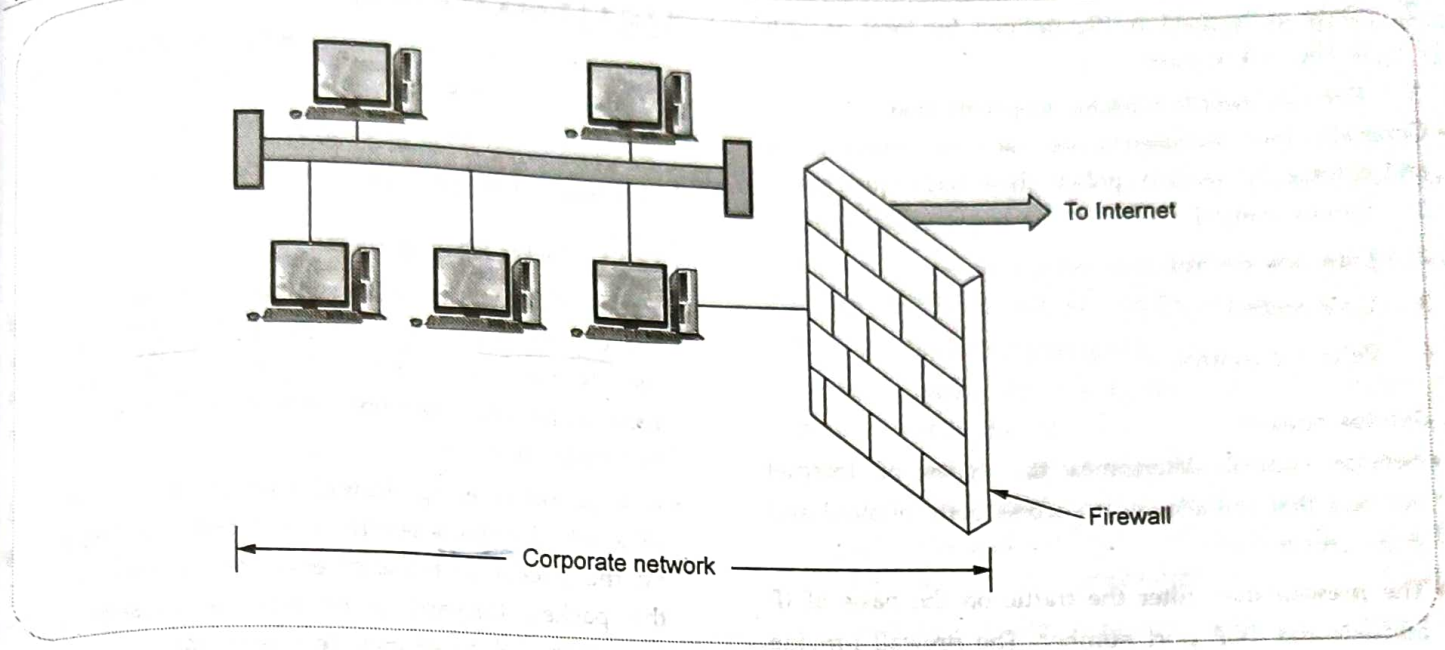


Fig. 5.3.1 Firewall

- The term firewall comes from the fact that by segmenting a network into different physical subnetwork, they limit the damage that could spread from one subnet to other just like firedoors or firewalls.

Capabilites of firewall

- A firewall examines all traffic routed between the two networks to see if it meets the certain criteria. If it does, it is routed between the networks, otherwise it is stopped.
- A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted.
- Firewalls can filter packets based on their source and destination addresses and port numbers. This known as **address filtering**.
- Firewalls can also filter specific types of network called **protocol filtering** because the decision to forward or reject traffic is dependent upon the protocol used. For example, HTTP,FTP, Telnet.
- Firewalls can also filter traffic by packet attribute or state.

Limitations of firewall

- A firewall cannot prevent individual users with modems from dialing into or out of the network, by passing the firewall altogether.
- Employee misconduct or carelessness cannot be controlled by firewalls.
- Policies involving the use and misuse of passwords and user accounts must be strictly enforced. These are management issues that should be raised during the planning of any security policy but that cannot be solved with firewalls alone.

Firewall technology

- Firewall technology generally falls into one of the two categories. Network level and application level.

1. Network level

This guards the entire network from unauthorised intrusion. An example of this technology is packet filtering, which simply reviews all information coming into a network and rejects the data that does not meet a predefined set of criteria.

2. Application level

This technology controls access on an application by application basis. For example, proxy servers can be set up to permit access to some application, such as HTTP, while blocking access to others, such as FTP.

Design goals

- Firewalls are very effective means for network based security threats. The design goals for firewall are as under

1. All the traffic must pass through firewall both from inside to outside and outside to inside.

2. Only authorized traffic defined by local security is allowed to pass.
3. Firewall itself is immune to penetration.

- Generally four techniques are used to control access and enforce the security policy, these techniques are -
  1. Service control
  2. Direction control
  3. User control
  4. Behavior control.

1. Service control

- Service control determines the types of Internet services that are allowed to access both inbound and outbound traffic.
- The firewall may filter the traffic on the basis of IP address and TCP port number. The firewall provide proxy software to receive and interpret each service request before passing it on.

2. Direction control

- Direction control determines the direction in which particular service requests may be initiated and is allowed to flow through the firewall.

3. User control

- User control gives access to a service according to which user is attempting to access it. This feature is usually applied for local user inside the firewall perimeter.

4. Behavior control

- Behavior control allows to control the use of any particular service. For example, the firewall may filter e-mails to eliminate spam.

5.3.1 Types of Firewall

- Commonly used firewalls from threats of security are
  1. Packet filtering router
  2. Application level gateways
  3. Circuit level gateways.

5.3.1.1 Packet Filtering Router

- Packet filtering firewalls work at the network level of the OSI model, or the IP layer of TCP/IP. They are usually part of a router. A router is a device that receives packets from one network and forwards them to another network.
- In a packet filtering firewall each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet, forward it or send a message to the originator. Rules can include source and destination IP address, source and destination port number and protocol used.
- The advantage of packet filtering firewalls is their low cost and low impact on network performance. Most routers support packet filtering. Even if other firewalls are used, implementing packet filtering at the router level affords an initial degree of security at a low network layer. This type of firewall only works at the network layer however and does not support sophisticated rule based models. Network Address Translation (NAT) routers offer the advantages of packet filtering firewalls but can also hide the IP addresses of computers behind the firewall, and offer a level of circuit based filtering.
- Packet filtering router applies rule to each incoming and outgoing IP packet, according forward or discards it. Fig. 5.3.2 shows packet filtering router.

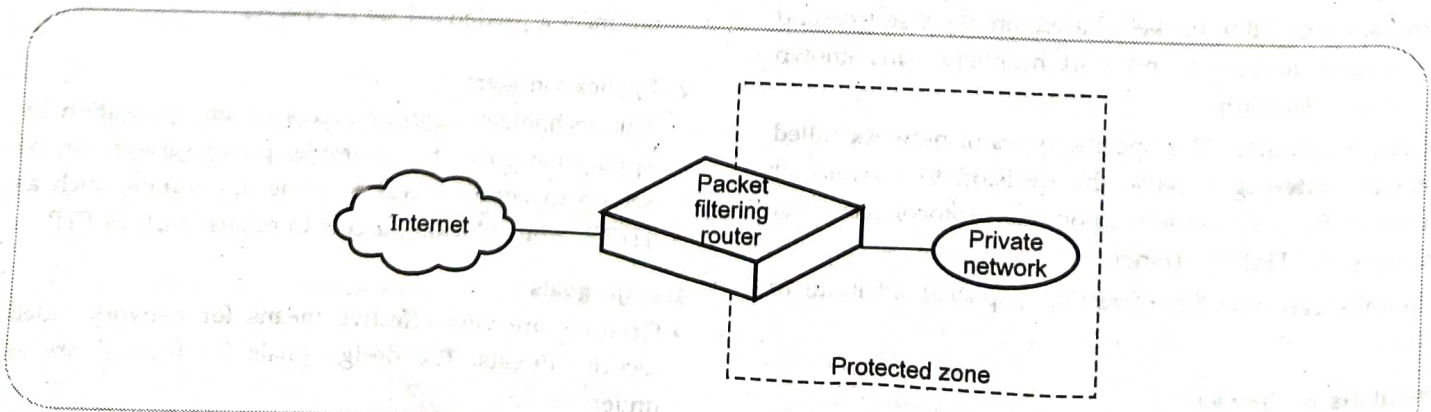


Fig. 5.3.2 Packet filtering router

- Filtering rules are based on information contained in the network packet such as
  i. Source IP address
  ii. Destination IP address
  iii. Source and destination transport level address.
  iv. IP field.
  v. Interface
- Attackers can try and break the security of the packet filter by using following techniques.
  i. IP address spoofing
  ii. Source routing attacks
  iii. Tiny fragment attacks
- Packet filtering provides a useful level of security at low cost. The type of router used in packet filtering is a screening router.

Screening router

- Each packet has two parts : The data that is part of the document and a header. If the packet is an envelope, then the data is the letter inside the envelope and the header is the address information on the outside.
- Here packet filter to refer to the technology or the process that is taking place and the screening router to refer to the thing that's doing it.
- Screening router can be a commercial router or a host-based router with some kind of packet filtering capability. Typical screening routers have the ability to block traffic between networks or specific hosts, on an IP port level. Some firewalls consist of nothing more than a screening router between a private network and the Internet.
- Screening routers operate by comparing the header information with a table of rules set by the network administrator to determine whether or not to send the packet on to its destination. If there is a rule that does not allow the packet to be sent on, the router simply discards it.

Working of packet filters

- Packet filters work by dropping packets based on their source and destination addresses or ports. Configuring a packet filter is a three step process. First of course, one must know what should and what should not be permitted. Next, the allowable types of packets must be specified, in terms of lofical expression on packet fileds. Finally the expression should be rewritten in whatever syntax your vendor supports.
- In general, for each packet, the router applies the rules sequentially, starting with the first one, until the packet fits or until it runs out of rules.
- For examples a router has 3 rules in its table.
- **Rule 1 :** Don't allow packets from a particular host, called TROUBLEHOST.
- **Rule 2 :** Let in connections into out mail gateway (using SMTP), located at port 25 on out host.
- **Rule 3 :** Block everything else.
- When a packet arrives at the screening router, the process works like this
  1. The packet filter extracts the information it needs from the packet header. In this example, it uses the local and external host identification and the local and external port numbers.
  2. The packet filter compares that information with the rules in the table.
  3. If the packet is from TROUBLEHOST, no matter what its destination, discard it.
  4. If the packet makes it past the first rule i.e. it's not from TROUBLEHOST, check to see if it's intended for port 25 on out SMTP-Mail host. If it is, send it on ; otherwise, discard it.
  5. If neither of the first two rules apply, the packet is rejected by rule three.
- Every packet has a set of headers containing certain information. The information is
  * IP source address.
  * IP destination address.
  * Protocol (whether the packet is a TCP, UDP or ICMP packet).
  * TCP or UDP source port.
  * TCP or UDP destination port.
  * TCP ack flag.

1. Inspection module

- If the header information listed above doesn't give you enough elements for setting up rules, you can use a packet filter that has an inspection module. An inspection module looks at more of the header information ; some can even look at the application data itself. For example, by inspecting the application data, the module can deny packets the contain certain application commands, such as the FTP put command or the SNMP set command.

2. State evaluation

- The header of a TCP packet contains an indicator called the ACK flag. When the ACK flag is set, it means that the incoming packet is a response to an earlier outgoing packet. If the flag is not set, the packet is not a response to an earlier outgoing packet, and therefore is suspect. It's common to set a screen rule to allow incoming packets that have the ACK flag set and reject those that don't. UDP doesn't use an ACK flag or any other similar indicator, so there's no way for the screening router to know whether an incoming packet was sent in response to an outgoing packet. The only safe thing to do in that situation is to reject the packet.
- That's where state evaluation comes in a screening router that has the state evaluation capability, "remembers" the original outgoing packet for a certain length of time (set by system administrator).

Advantages of packet filters

1. Low impact on network performance.
2. Packet filters are normally transparent to user.
3. Relatively inexpensive price.

Disadvantages of packet filtering firewall

1. They are vulnerable to attacks aimed at protocol higher than the network layer protocol.
2. They cannot hide the network topology.
3. Packet filtering firewall can not support all Internet applications.
4. These firewalls have very limited auditing capabilities.
5. Sometimes user level authentication do not supported by packet filtering firewall.

5.3.1.2 Application Level Gateways

- Application level gateways, also called proxies, are similar to circuit level gateways except that they are application specific. They can filter packets at the application layer of the OSI model. Incoming or outgoing packets cannot access services for which there is no proxy. In plain terms, an application level gateway that is configured to be a web proxy will not allow any FTP, gopher, Telnet or other traffic through. Because they examine packets at application layer, they can filter application specific commands such as http:post and get, etc. This cannot be accomplished with either packet filtering firewalls or circuit level neither of which know anything about the application level information.
- Application level gateways can also be used to log user activity and logins. They offer a high level of security, but have a significant impact on network performance. This is because of context switches that slow down network access dramatically. They are not transparent to end users and require manual configuration of each client computer.

Fig. 5.3.3 shows application level gateway.

Advantages

1. Application gateway provides high level of security than packet filters.
2. Easy to configure.
3. They can hide the private network topology.
4. It support user level authentication.
5. Capability to examine the all traffic in detail.

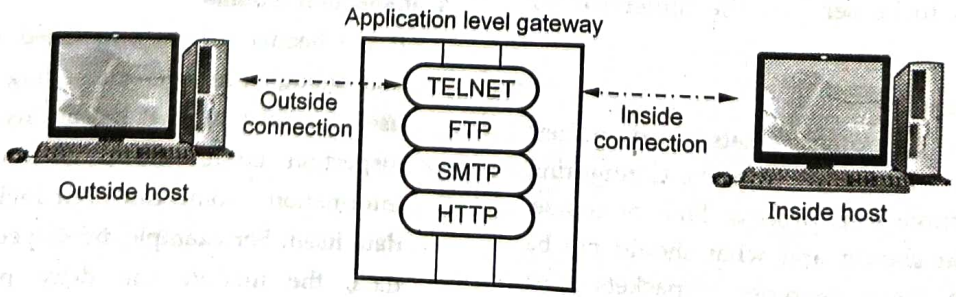


Fig. 5.3.3 Application gateway

Disadvantages

1. High impact on network performance.
2. Slower in operation because of processing overheads.
3. Not transparent to users.

5.3.1.3 Circuit Level Gateways

- Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP. They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to remote computer through a circuit level gateway appears to have originated from the gateway. This is useful for hiding information about protected networks.
- Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect. On the other hand, they do not filter individual packets.
- The circuit level gateway does not permit end-to-end TCP connection but two TCP connections are set-up. A typical use of circuit level gateway is in situations when system administrator trusts the internal users.

5.3.1.4 Comparison between Packet Filter and Proxies

Sr. No.	Packet filter	Proxy (Application level)
1.	Works at network layer of OSI and IP layer of TCP.	Works at application layer of OSI, TCP layer of TCP.
2.	Low impact on network performance.	High impact on network performance.
3.	Low level of security as compare to proxi.	High level of security.
4.	Packet filtering is not effective with the FTP protocol.	FTP and Telnet are allowed into the protected subnet.
5.	Simple level of security and faster than proxy firewall.	Capability to examine the traffic in detail, so slower than packet filtering.
6.	Normally transparent to the users.	Not transparent to the users.
7.	Difficult to configure as compare to proxy.	Easier to configure than packet filtering.
8.	They cannot hide the private network topology.	They can hide the private network topology.

5.3.2 Firewall Location

1. DMZ network (Demilitarized Zone)
2. Virtual Private Network (VPN)
3. Distributed firewall

- A firewall is positioned to provide a protective barrier between an external, potentially untrusted source of traffic and an internal network.

1. DMZ Network (Demilitarized Zone)

- Connections from the internal and the external network to the DMZ are permitted, while connections from the DMZ are only permitted to the external network, hosts in the DMZ may not connect to the internal network.
- This allows the DMZ's hosts to provide services to both the internal and external network while protecting the internal network in case intruders compromise a host in the DMZ. The DMZ is typically used for connecting servers that need to be accessible from the outside world, such as e-mail, web and DNS servers.

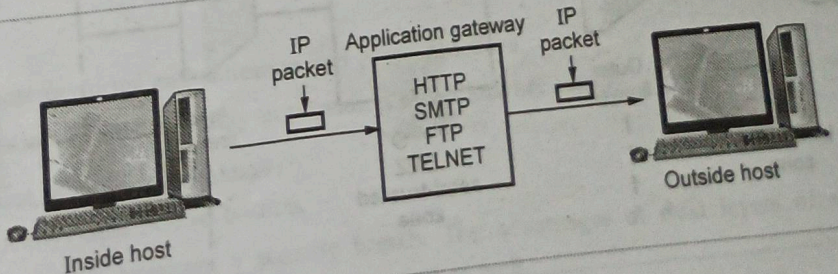


Fig. 5.3.4 Circuit gateway

Disadvantages

1. High impact on network performance.
2. Slower in operation because of processing overheads.
3. Not transparent to users.

5.3.1.3 Circuit Level Gateways

- Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP. They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to remote computer through a circuit level gateway appears to have originated from the gateway. This is useful for hiding information about protected networks.
- Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect. On the other hand, they do not filter individual packets.
- The circuit level gateway does not permit end-to-end TCP connection but two TCP connections are set-up. A typical use of circuit level gateway is in situations when system administrator trusts the internal users.

5.3.1.4 Comparison between Packet Filter and Proxies

Sr. No.	Packet filter	Proxy (Application level)
1.	Works at network layer of OSI and IP layer of TCP.	Works at application layer of OSI, TCP layer of TCP.
2.	Low impact on network performance.	High impact on network performance.
3.	Low level of security as compare to proxi.	High level of security.
4.	Packet filtering is not effective with the FTP protocol.	FTP and Telnet are allowed into the protected subnet.
5.	Simple level of security and faster than proxy firewall.	Capability to examine the traffic in detail, so slower than packet filtering.
6.	Normally transparent to the users.	Not transparent to the users.
7.	Difficult to configure as compare to proxy.	Easier to configure than packet filtering.
8.	They cannot hide the private network topology.	They can hide the private network topology.

5.3.2 Firewall Location

1. DMZ network (Demilitarized Zone)
2. Virtual Private Network (VPN)
3. Distributed firewall

- A firewall is positioned to provide a protective barrier between an external, potentially untrusted source of traffic and an internal network.

1. DMZ Network (Demilitarized Zone)

- Connections from the internal and the external network to the DMZ are permitted, while connections from the DMZ are only permitted to the external network, hosts in the DMZ may not connect to the internal network.
- This allows the DMZ's hosts to provide services to both the internal and external network while protecting the internal network in case intruders compromise a host in the DMZ. The DMZ is typically used for connecting servers that need to be accessible from the outside world, such as e-mail, web and DNS servers.

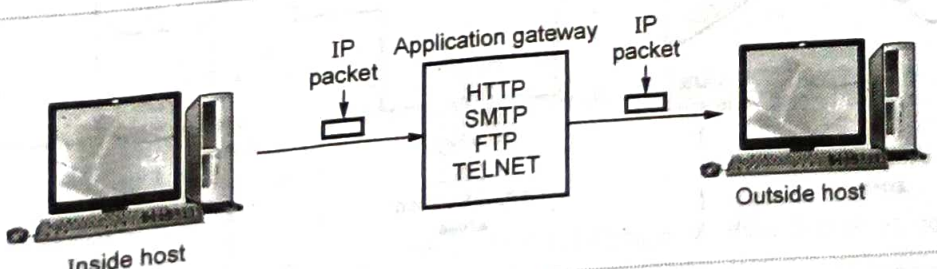


Fig. 5.3.4 Circuit gateway

- Fig. 5.3.5 shows DMZ network.
- Traffic from the Internet is filtered, but some of it is allowed to reach systems in the DMZ i.e. like web servers and mail servers. If an attacker succeeds in breaking into a system in your DMZ, they won't gain access to your internal network as traffic coming from the DMZ is filtered before being allowed into the internal network.
- To create a DMZ, you can use two firewalls. Our illustration shows an outer firewall that separates the DMZ from the Internet and an inner firewall that separates the DMZ from the internal network. The outer firewall controls the traffic from the Internet to the DMZ. The inner firewall controls traffic from the DMZ to the internal network.
- The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity. The external firewall also provides a basic level of protection for the remainder of the enterprise network.
- Internal firewalls serve three purposes :
  i. The internal firewall adds more stringent filtering capability, compared to the external firewall, in order to protect enterprise servers and workstations from external attack.
  ii. The internal firewall provides two-way protection with respect to the DMZ.
  iii. Multiple internal firewalls can be used to protect portions of the internal network from each other.

2. Virtual Private Networks (VPN)

- Virtual Private Networks (VPN) provide an encrypted connection between a user's distributed sites over a public network (e.g., the Internet). By contrast, a private network uses dedicated circuits and possibly encryption.
- Use of a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users. To counter this problem, a VPN is needed.
- VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet. VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption and authentication system at both ends. The encryption may be performed by firewall software or possibly by routers. The most common protocol mechanism used for this purpose is at the IP level and is known as IPsec.

3. Distributed Firewall

- A distributed firewall configuration involves stand-alone firewall devices plus host based firewalls working together under a central administrative control. Security policy is defined centrally and enforcement of policy is done by network endpoint(s).
- Administrators can configure host resident firewalls on hundreds of servers and workstations as well as configure personal firewalls on local and remote user systems.

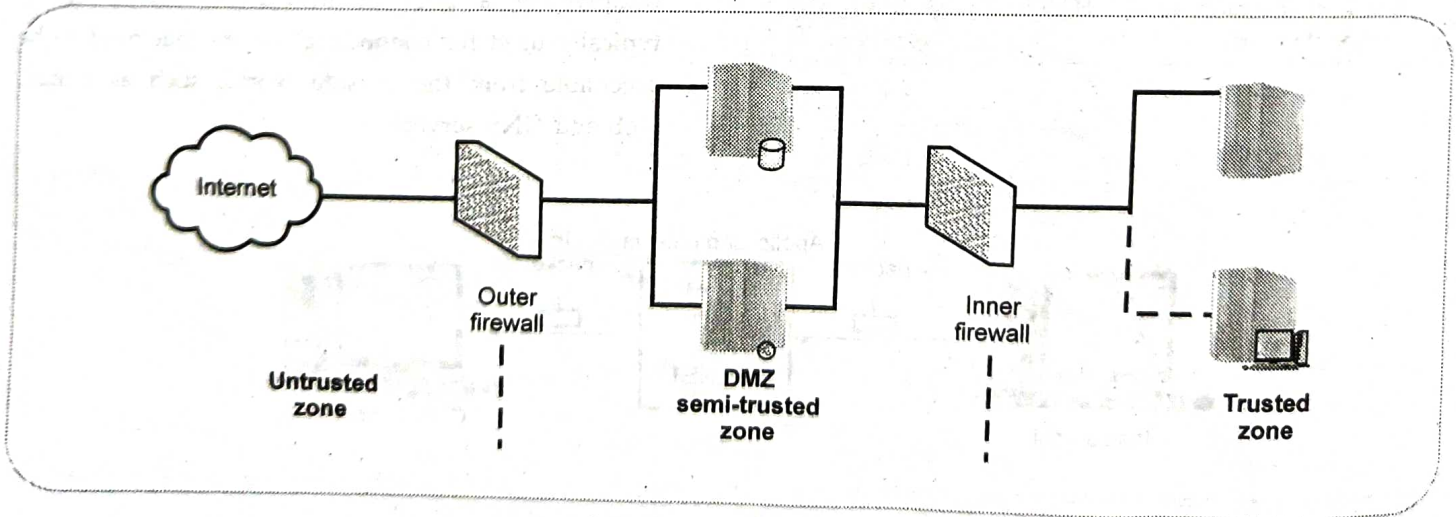


Fig. 5.3.5 DMZ network

- Tools let the network administrator set policies and monitor security across the entire network. These firewalls protect against internal attacks and provide protection tailored to specific machines and applications. Stand-alone firewalls provide global protection, including internal firewalls and an external firewall.

5.3.3 Firewall Configuration

- Firewall configuration are of three types :
  1. Screened host, single homed bastion host
  2. Screened host, dual homed bastion host
  3. Screened subnet.

1. Screened host, single homed bastion host

- In this system, firewall consists of two systems : A packet filtering router and a bastion host.
- The router is configured so that,
  1. For traffic from the Internet, only IP packets destined for the bastion host are allowed in.
  2. For traffic from the internal network, only IP packets from the bastion host are allowed out.
- Fig. 5.3.6 shows screened host, single homed bastion host.

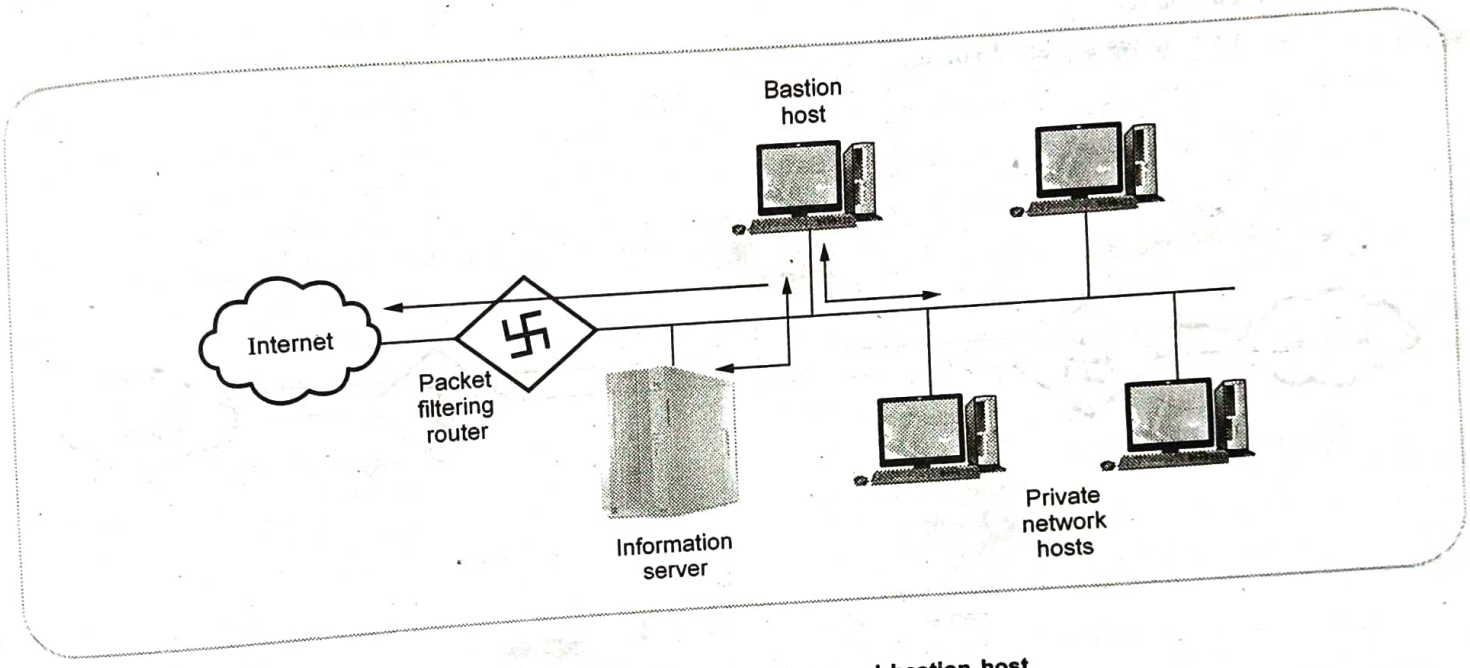


Fig. 5.3.6 Screened host, single homed bastion host

- The bastion host performs authentication and proxy functions.
- This configuration affords flexibility in providing direct internet access.

2. Screened host, dual homed bastion

- Fig. 5.3.7 shows dual homed bastion.
- This configuration prevents a security breach. The advantages of dual layers of security that were present in the previous configuration are present as well.

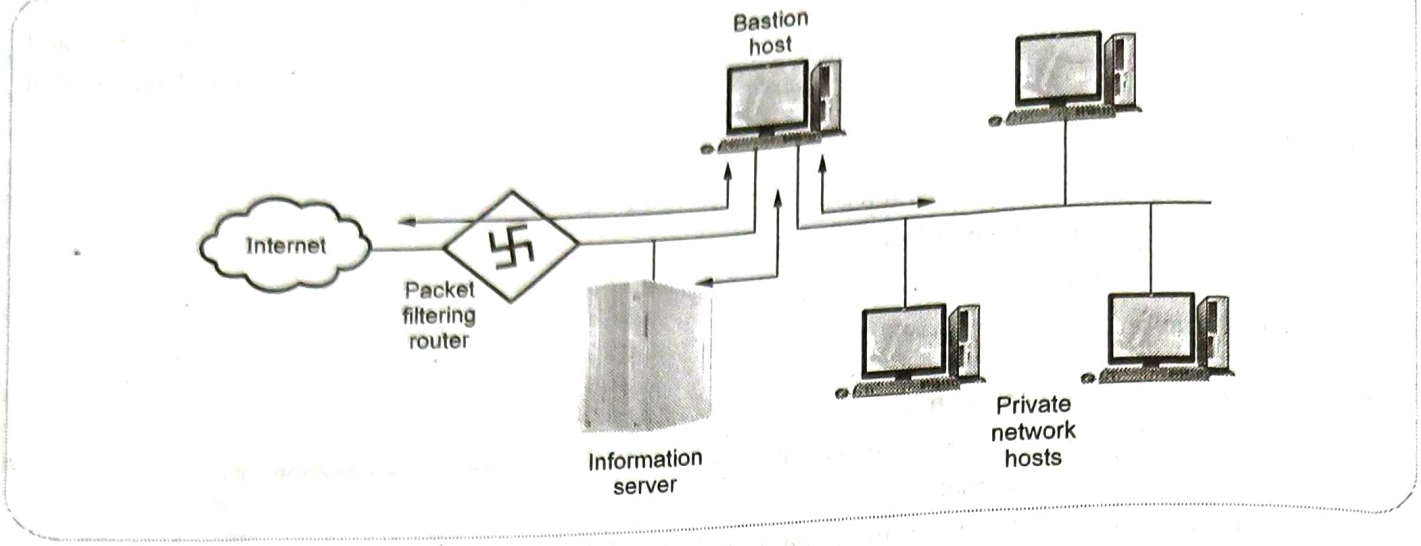


Fig. 5.3.7 Dual homed bastion

- An information server or other hosts can be allowed direct communication with the router if this is in accord with the security policy.

3. Screened subnet

- Fig. 5.3.8 shows screened subnet

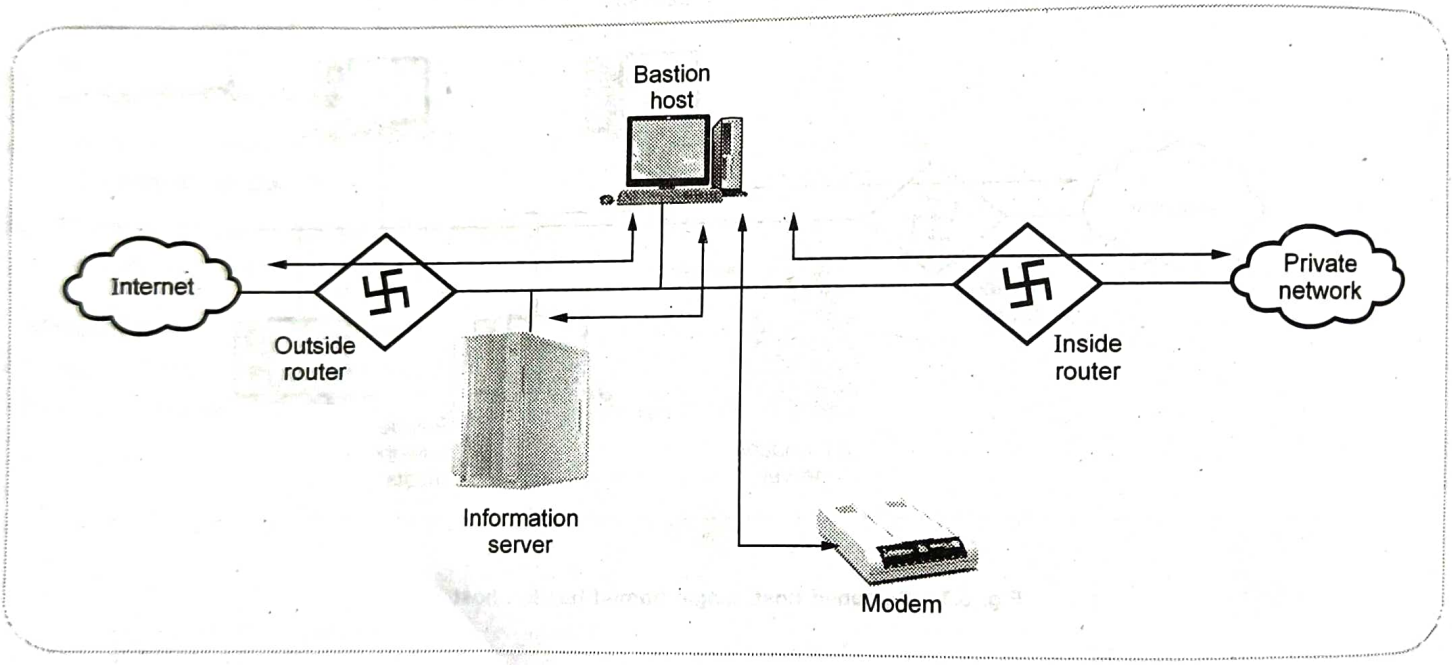


Fig. 5.3.8 Screened subnet

- This configuration creates an isolated subnetwork which may consists of simply the bastion host but may also include one or more information servers and modems for dial-up capability.

Advantages

1. There are now three levels of defense to thwart intruders.
2. Internal network is invisible to the Internet.
3. The systems on the inside network cannot construct direct routes to the internet.

Review Questions

1. *What are the various characteristics of firewall ?*
2. *Explain architecture of firewall.*
3. *Describe types of firewall in detail.*
4. *Describe screened subnet fire wall architecture.*
5. *Explain the firewall types with its operation.*
6. *Explain various types of firewall.*
7. *Describe operation of packet filtering firewall.*

5.4 Trusted Systems

- Another widely applicable requirement is to protect data or resources on the basis of levels of security, as is commonly found in the military where information is categorized as Unclassified (U), Confidential (C), Secret (S), Top Secret (TS) or Higher.
- Here subjects have varying rights of access to objects based on their classifications. This is known as multilevel security. A system that can be proved to enforce this is referred to as a **trusted system.**
- The general statement of the requirement for multilevel security is that a subject at a high level may not convey information to a subject at a lower or incompatible level unless that flow accurately reflects the will of an authorized user. This can be implemented using the **Bell LaPadula Model,** in which a multilevel secure system must enforce :
  1. **No read up :** A subject can only read an object of less or equal security level - Simple Security Property.
  2. **No write down :** A subject can only write into an object of greater or equal security level - * (star) Property.
- These two rules, if properly enforced, provide multilevel security.

Bell LaPadula model

- The BLP model was developed in the 1970s as a formal model for access control. The model relied on the access control concept. In the model, each subject and each object is assigned a security class. In the simplest formulation, security classes form a strict hierarchy and are referred to as security levels. One example is the U.S. military classification scheme : *top secret > secret > confidential > restricted > unclassified.*
- It is possible to also add a set of categories or compartments to each security level, so that a subject must be assigned both the appropriate level and category to access an object.
- This con ept is equally applicable in other areas, where information can be organized into gross levels and categories and users can be granted clearances to access certain categories of data. For example, the highest level of security might be for strategic corporate planning documents and data, accessible by only corporate officers and their staff; next might come sensitive financial and personnel data, accessible only by administration personnel, corporate officers and so on. This suggests a classification scheme such as *strategic > sensitive > confidential > public.*
- A subject is said to have a security clearance of a given level; an object is said to have a security classification of a given level. The security classes control the manner by which a subject may access an object.
- The model defined four access modes
  1. **READ :** The subject is allowed only read access to the object.
  2. **APPEND :** The subject is allowed only write access to the object.
  3. **WRITE :** Tthe subject is allowed both read and write access to the object.
  4. **EXECUTE :** The subject is allowed neither read nor write access to the object but may invoke the object for execution.

Review Questions

1. *What is trusted system ?*
2. *What is trusted system ? Explain in brief.*

5.5 Intrusion Detection

- ***Intrusion*** is the act of gaining unauthorized access to a system so as to cause loss.
- ***Intrusion detection*** is the act of detecting unwanted traffic on a network or a device.
- Intrusion Detection Systems (IDSs) attempt to identify attacks by comparing collected data to predefined signatures known to be malicious or to a model of legal behavior.

- Intrusion detection systems are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems.

Functions of intrusion detection systems

1. Monitoring and analysis of user and system activity
2. Auditing of system configurations and vulnerabilities
3. Assessing the integrity of critical system and data files
4. Recognition of activity patterns reflecting known attacks
5. Statistical analysis for abnormal activity patterns

Benefits of intrusion detection

1. Improving integrity of other parts of the information security infrastructure
2. Improved system monitoring
3. Tracing user activity from the point of entry to point of exit or impact
4. Recognizing and reporting alterations to data files
5. Spotting errors of system configuration and sometimes correcting them
6. Recognizing specific types of attack and alerting appropriate staff for defensive responses
7. Keeping system management personnel up to date on recent corrections to programs
8. Allowing non-expert staff to contribute to system security
9. Providing guidelines in establishing information security policies

Process model

- Many IDSs can be described in terms of following functional components :

1. **Information sources :** The different sources of event information used to determine whether an intrusion has taken place. These sources can be drawn from different levels of the system, with network, host, and application monitoring most common.
2. **Analysis :** The part of intrusion detection systems that actually organizes and makes sense of the events derived from the information sources, deciding when those events indicate that intrusions are occurring or have already taken place. The most common analysis approaches are misuse detection and anomaly detection.
3. **Response :** The set of actions that the system takes once it detects intrusions. These are typically grouped into active and passive measures, with active measures involving some automated intervention on the part of the system, and passive measures involving reporting IDS findings to humans, who are then expected to take action based on those reports.

5.5.1 Prevention

- **Intrusion prevention** is the process of performing intrusion detection and then stopping the detected incidents.
- **An Intrusion Prevention System (IPS)** is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.
- The main function of an IPS is to identify suspicious activity, and then log information, attempt to block the activity, and then finally to report it.
- Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine.
- Following a successful exploit, the attacker can disable the target application (resulting in a denial-of-service state), or can potentially access to all the rights and permissions available to the compromised application.

5.5.2 Detection

- Intrusion detection is the act of detecting unwanted traffic on a network or a device.
- Intrusion Detection Systems (IDSs) attempt to identify attacks by comparing collected data to predefined signatures known to be malicious or to a model of legal behaviour.
- Intrusion detection systems are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems.
- IDS performs three tasks :
  a) An IDS monitors events of interests.
  b) An IDS generates significant data to systems administrators for analysis.
  c) An IDS creates alert for events when occurred.

5.5.3 Function and Strength of IDS

Intrusion detection systems perform the following functions well :

1. Monitoring and analysis of system events and user behaviors.
2. Testing the security states of system configurations.
3. Base lining the security state of a system, then tracking any changes to that baseline.
4. Recognizing patterns of system events that correspond to known attacks.
5. Recognizing patterns of activity that statistically vary from normal activity.
6. Managing operating system audit and logging mechanisms and the data they generate.
7. Alerting appropriate staff by appropriate means when attacks are detected.
8. Measuring enforcement of security policies encoded in the analysis engine.
9. Providing default information security policies.
10. Allowing non-security experts to perform important security monitoring function.

5.5.4 Types of IDS

5.5.4.1 Anomaly Detection

- An anomaly based intrusion detection system is a system for detecting computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous.
- It examines ongoing traffic, activity, transactions, and behaviour in order to identify intrusions by detecting anomalies.
- For instance, anomaly-based IDS will detect that an IP packet is malformed. It does not detect that it is malformed in a specific way, but indicates that it is anomalous.
- The classification is based on heuristics or rules, rather than patterns or signatures, and will detect any type of misuse that falls out of normal system operation.
- Anomaly detectors construct profiles representing normal behavior of users, hosts, or network connections. These profiles are constructed from historical data collected over a period of normal operation.
- The detectors then collect event data and use a variety of measures to determine when monitored activity deviates from the norm.
- Another method is to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as strict anomaly detection.
- The measures and techniques used in anomaly detection include : Threshold detection, statistical measures, and rule-based measures.

Advantages of anomaly detection

1. IDSs based on anomaly detection detect unusual behavior and thus have the ability to detect symptoms of attacks without specific knowledge of details.
2. Anomaly detectors can produce information that can in turn be used to define signatures for misuse detectors.

Disadvantages of anomaly detection

1. Anomaly detection approaches usually produce a large number of false alarms due to the unpredictable behaviors of users and networks.
2. Anomaly detection approaches often require extensive "training sets" of system event records in order to characterize normal behavior patterns.

5.5.4.2 Signature-based Detection

- A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats.
- This is similar to the way most antivirus software detects malware.
- A common strategy for IDS in detecting intrusions is to memorize signatures of known attacks. The inherent weakness in relying on signatures is that the signature patterns must be known first.
- New attacks are often unrecognizable by popular IDS. Signatures can be masked as well. The ongoing race between new attacks and detection systems has been a challenge.
- Also called misuse detection.

Advantages of signature-based detection

1. Signatures are easy to develop.
2. Understand if you know what network behavi you're trying to identify.

Disadvantages of signature-based detection

1. High false positive rate.
2. Largely ineffective at detecting previously unknown threats.
3. Signature database must be continually updated and maintained.

5.5.4.3 Comparison between Signature-based and Anomaly Detection

Parameters	Signature-based detection	Anomaly detection
Technique	Detect patterns of interest	Deviations from learned norms
Generalization	Problematic	Yes
Specific	Yes	No
Sensitivity	High	Moderate
False alarms	Low	Moderate
Adaptation	No	Yes

5.5.4.4 Network Based System

- A Network Intrusion Detection System (NIDS) is tries to detect malicious activity such as denial of service attacks; port scans or even attempts to crack into computers by network security monitoring of network traffic.
- Network intrusion detection systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network.
- The majority of commercial intrusion detection systems are network based.
- These IDSs detect attacks by capturing and analyzing network packets.
- Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment, thereby protecting those hosts.
- Network-based IDSs often consist of a set of single-purpose sensors or hosts placed at various points in a network.
- These units monitor network traffic, performing local analysis of that traffic and reporting attacks to a central management console.
- As the sensors are limited to running the IDS, they can be more easily secured against attack.
- Many of these sensors are designed to run in stealth mode, in order to make it more difficult for an attacker to determine their presence and location.

Advantages of network-based IDSs

1. A few well-placed network-based IDSs can monitor a large network.
2. The deployment of network-based IDSs has little impact upon an existing network.
3. It can be made very secure against attack.

Disadvantages of network-based IDSs

1. Network-based IDSs may have difficulty processing all packets in a large or busy network.
2. Network-based IDSs cannot analyze encrypted information.
3. Most network-based IDSs cannot tell whether or not an attack was successful.
4. Some network-based IDSs have problems dealing with network-based attacks that involve fragmenting packets.

5.5.4.5 Host-based IDSs (HIDS)

- Host based monitors system logs for evidence of malicious or suspicious application activity in real time.
- It requires small programs or agents to be installed on individual systems to be monitored. The agents supervise the OS and write data to log files and activate alarm.
- Host-based IDSs operate on information collected from within an individual computer system.
- This allows host-based IDSs to analyze activities with great reliability and precision, determining exactly which processes and users are involved in a particular attack on the operating system.
- Host-based IDSs normally utilize information sources of two types, operating system audit trails, and system logs.
- Operating system audit trails are usually generated at the innermost (kernel) level of the operating system, and are therefore more detailed and better protected than system logs.
- System logs are much less obtuse and much smaller than audit trails, and are furthermore far easier to comprehend.

Advantages

1. With their ability to monitor events local to a host, can detect attacks that cannot be seen by network-based IDS.
2. It can often operate in an environment in which network traffic is encrypted.
3. When host-based IDSs operate on OS audit trails; they can help detect Trojan horse or other attacks that involve software integrity breaches.

Disadvantages

1. Host-based IDSs are harder to manage, as information must be configured and managed for every host monitored.
2. Since at least the information sources for host-based IDSs reside on the host targeted by attacks, the IDS may be attacked and disabled as part of the attack.
3. Host-based IDSs are not well suited for detecting network scans or other such surveillance that targets an entire network.
4. Host-based IDSs can be disabled by certain denial-of-service attacks.
5. When host-based IDSs use OS audit trails as an information source, the amount of information can be immense, requiring additional local storage on the system.

5.5.4.6 Differences between HIDS and NIDS

Sr. No.	NIDS	HIDS
1.	Broad in scope, (watching all network activities).	Narrow in scope (watching only specific host activities).
2.	Easier setup.	More complex setup.
3.	Better for detecting attacks from the outside.	Better for detecting attacks from the inside.
4.	Less expensive to implement.	More expensive to implement.
5.	Detection is based on what can be recorded on the entire network.	Detection is based on what any single host can record.
6.	Examines packet headers.	Does not see packet headers.
7.	Near real-time response.	Usually only responds after a suspicious log entry has been made.
8.	OS-independent.	OS-specific.
9.	Detects network attacks as payload is analyzed.	Detects local attacks before they hit the network.
10.	Detects unsuccessful attack attempts.	Verifies success or failure of attacks.

5.5.5 Limitations of IDS

Intrusion detection systems cannot perform the following functions :

1. Compensating for weak or missing security mechanisms in the protection infrastructure. Such mechanisms include firewalls, identification and authentication, link encryption, access control mechanisms, and virus detection and eradication.
2. Instantaneously detecting, reporting, and responding to an attack, when there is a heavy network or processing load.
3. Detecting newly published attacks or variants of existing attacks.
4. Effectively responding to attacks launched by sophisticated attackers.
5. Automatically investigating attacks without human intervention.
6. Resisting attacks that are intended to defeat or circumvent them.
7. Compensating for problems with the fidelity of information sources.
8. Dealing effectively with switched networks.

5.5.6 Difference between IDS and IPS

Sr. No.	IDS	IPS
1.	Installed on network segments (NIDS) and on host (HIDS).	Installed on network segments (NIPS) and on host (HIPS).
2.	Sits on network passively .	Sits inline (not passive).
3.	Cannot parse encrypted traffic.	Better at protecting applications.

4.	Central management control.	Central management control.
5.	Better at detecting hacking attacks.	Ideal for blocking web defacement.
6.	Alerting product (reactive).	Blocking product (proactive).

5.5.7 Intrusion Detection Techniques

- Intrusion detection techniques are as follows :

1. **Threshold detection :** It records each occurrence of suspicious events and compares it with a threshold number. Threshold detection involves counting no occurrences of a specific event type over an interval of time, if count surpasses a reasonable number, then intrusion is assumed establishing threshold number is difficult.
2. **Anomaly detection :** It requires little knowledge of the actual system beforehand. Usage patterns are established automatically by means of neural networks.
3. **Rule based detection :** Observe events on system and apply rules to decide if activity is suspicious or not. Analyze historical audit records to identify usage patterns and auto-generate rules for them. Then observe current behavior and match against rules to see if conforms. Like statistical anomaly detection does not require prior knowledge of security flaws.

5.5.8 Tools for Intrusion Detection

- Audit record is a fundamental tool for intrusion detecting. Two forms of audit records are used.

1. **Native audit records**

   In all multiuser operating system accounting software collects information about user activity.

2. **Detective specific audit records**

   A system that collects information need by intrusion detection system.

Audit record format

- Each audit record contains following field.

1. Subject
2. Action
3. Object

4. Exception - condition
5. Resource - usage
6. Time stamp.

Fig. 5.5.1 shows audit record format.

Subject	Action	Object	Exception condition	Resource-usage	Time-stamp

Fig. 5.5.1 Audit record format

5.5.9 Distributed IDS

- A distributed collection of hosts supported by a LAN or internetwork is called distributed intrusion detection system.

Components of distributed IDS

- The distributed IDS consists of three major components.

1. Host agent module
2. LAN monitor agent module
3. Central manager module.

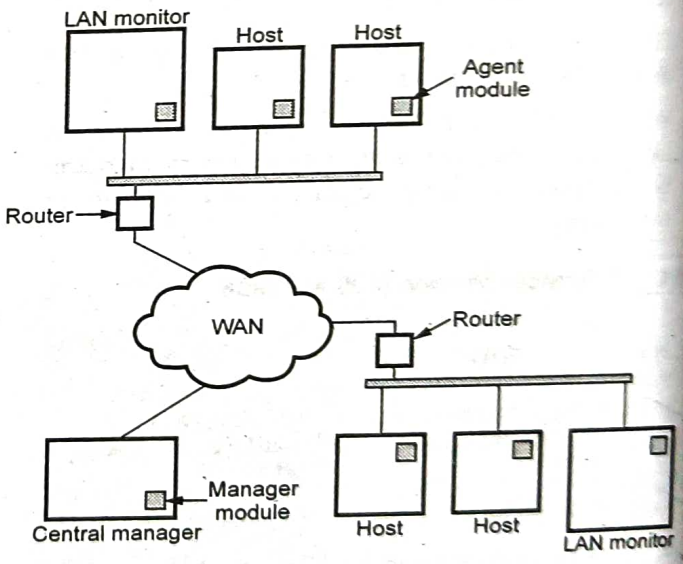


Fig. 5.5.2 Distributed ID architecture

Review Questions

1. *What are the challenges of intrusion detection ?*
2. *Explain anomaly-based intrusion detection system.*
3. *Explain types of Intrusion Detection System (IDS) ?*
4. *List and explain types of Intrusion Detection System (IDS).*
5. *Explain operation of anomaly based intrusion detection system in detail.*
6. *Explain the operaton of mis used - based intrusion detection system.*

5.6 Access Control

- Access control is an important tool of security to protect data and other resources.
- The access control mechanism refers to prevention of unauthorized use of a resource.
- Access control includes :
  1. Authentication of users
  2. Authorization of their privileges
  3. Auditing to monitor and record user actions
- Three types of access controls system are :
  1. Discretionary access control
  2. Mandatory access control
  3. Role-based access control

5.6.1 Discretionary Access Control (DAC)

- When user set an access control mechanism to allow or deny access to an object (system resource), such a mechanism is a Discretionary Access Control (DAC).
- The Discretionary Access Control (DAC) is also called as an Identity-Based Access Control (IBAC).
- A Discretionary Access Control (DAC) policy is a means of assigning access rights based on rules specified by users.
- The DAC policies include the file permissions model implemented by nearly all operating systems. In Unix, for example, a directory listing might yield "... rw, xr-xr-x ... file.txt", meaning that the owner of file.txt may read, write, or execute it, and that other users may read or execute the file but not write it. The set of access rights in this example is {read, write, execute}, and the operating system mediates all requests to perform any of these actions. Users may change the permissions on files they own, making this a discretionary policy.
- Discretionary Access Control List (DACL) determines which users and groups can access the object (system resource) for operations. It consists of a list of Access Control Entries (ACEs).

5.6.1.1 Drawbacks of DAC

- DAC system has two significant drawbacks :
1. It relies on decisions by the end user to set the proper level of security. As a result, incorrect permissions might be granted to a subject or permissions might be given to an unauthorized subject.
2. The subject's permissions will be inherited by any programs that the subject executes.

5.6.2 Mandatory Access Control (MAC)

- When a system mechanism controls access to an object and an individual user cannot alter that access, then such a control is called as Mandatory Access Control (MAC).
- Mandatory Access Control (MAC) is also called as rule-based access control.
- Mandatory access control is a more restrictive scheme that does not allow users to define permissions on files, regardless of ownership. Instead, security decisions are made by a central policy administrator.
- Each security rule consists of a subject, which represents the party attempting to gain access, an object, referring to the resource being accessed, and a series of permissions that define the extent to which that resource can be accessed.

5.6.2.1 Elements of MAC

- MAC has two key elements :

1. Labels :

- In a system using MAC, every entity is an object (laptops, files, projects, etc.) and is assigned a classification label.
- These labels represent the relative importance of the object, such as confidential, secret, and top secret. Subjects (users, processes, etc.) are assigned a privilege label (sometimes called a clearance).

2. Levels :

- A hierarchy based on the labels is also used, both for objects and subjects.
- Top secret has a higher level than secret, which has a higher level than confidential.

5.6.2.2 MAC Implementations

- Major implementations of MAC are :
1. **Lattice model :** Security levels for objects and subjects are ordered as a lattice.
2. **Bell-LaPadula confidentiality model :** Advanced version of the lattice model (actually this uses a mix of MAC and DAC).

5.6.3 Role-Based Access Control (RBAC)

- A user is an entity that wishes to access resources of the organization to perform a task. Usually, users are actual human users, but a user can also be a machine or application.
- A role is defined as a collection of users with similar functions and responsibilities in the organization. Examples of roles in a university may include "student," "alum," "faculty," "dean," "staff," and "contractor." In general, a user may have multiple roles.
  - Roles and their functions are often specified in the written documents of the organization.
  - The assignment of users to roles follows resolutions by the organization, such as employment actions (e.g. hiring and resignation) and academic actions (e.g., admission and graduation).
- Role-Based Access Control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise.
- In RBAC, the rights and permissions are assigned to roles instead of individual users.
- RBAC is also called as Non-Discretionary Access Control (NDAC).
- This added layer of abstraction permits easier and more flexible administration and enforcement of access controls.
- The RBAC framework provides administrators with the capability to regulate who can perform what actions, when, from where, in what order, and in some cases under what relational circumstances.
- RBAC is important because it provides customers a greater degree of control over cloud resource utilization with the added layer of system security.
- RBAC should be implemented in the following situations :

1. In an effort to minimize downtime and accidental changes to the cloud resources, the account owner would like to restrict access to the accounts to only a few people.
2. In an effort to synchronize cloud product access to the functions of an employee's job, the account owner would like to grant access to employees based on the nature of their position.
3. In an effort to help prevent unauthorized access to cloud products through the sharing of admin credentials, the account owner would like each user of the cloud accounts to have their own credentials.

5.6.3.1 Difference between DAC and RBAC

1. DAC is based on personal permissions, while RBAC is based on group-level permissions.
2. DAC is set by the data owner, while RBAC by the system owner/s (usually the developer defines the access given to each role, and the operational admin puts users into roles).
3. DAC definitions are typically attached to the data/resource, whereas RBAC is usually defined in two places : in code/configuration/metadata (the roles access), and on the user object (or table - the roles each user has).
4. DAC is administered "on the resource" (i.e. you administer each resource individually), whereas RBAC roles are centrally administered (who is associated with which roles).
5. DAC should be seen as enumerating "who has access to my data", and RBAC defines "what can this user do".
6. The definition of permissions per role is typically static in RBAC, and users are only granted roles; in DAC the permissions per resource are often changed at runtime.

5.6.4 Access Control Matrix

- A password scheme used to allow access to a user's computer account may be viewed as the simplest instance of an access control matrix : each resource has a list of identities associated with it (e.g. a computer account which authorized entities may access), and successful corroboration of an identity allows access to the authorized resources as listed for that entity.
- The simplest framework for describing a protection system is the access control matrix model.
- Two fundamental concepts in field authorization are :
  1. Access Control Lists (ACLs)
  2. Capabilities (C-lists)

5.6.4.1 ACLs and Capabilities Lists

- Access Control List (ACL) is a set of rules that define security policy. These ACLs contain one or more Access Control Entries (ACEs), which are the actual rule definitions themselves.
- These rules can restrict access by specific user, time of day, IP address, function (department, management level, etc.), or specific system from which a logon or access attempt is being made.
- The VPN secure connection can be easily cracked by Ophcrack.
- Session keys and encryption are poorly implemented and vulnerable to attacks.
- The control channel is open to snooping and denial of service.

Counter measures

- Discontinue IKE aggressive mode use, use token based authentication scheme.

VoIP hacking

- VoIP on an IP network rely on multiple protocols, one for signaling and one for transport of encoded voice traffic.
- Two most common protocols are H.323 and SIP.

Most common VoIP attacks

1. Denial of service.
2. Spoofing the CLID (caller ID).
3. Injecting data into established call.
4. Attacking through services linked to VoIP, such as -
   - Advanced voice mail
   - Instant messaging
   - Calender services
   - User management
5. Accessing repository of recorded calls.

Counter measures

- Network segment between voice and data LANs.
- Authentication and encryption for all SIP communication.
- Replay IDS/IPS.

Review Question

1. *What is access control security service ?*

❑❑❑

Unit VI

6 Cyber Forensic, Hacking and its Counter Measures

Syllabus

Personally Identifiable Information (PII), Cyber Stalking, Cybercrime, PII Confidentiality Safeguards, Information Protection Law : Indian Perspective. Hacking : Remote connectivity and VoIP hacking, Wireless Hacking, Mobile Hacking, countermeasures.

Contents

6.1 Introduction to Personally Identifiable Information (PII)

- Personally Identifiable Information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for anonymous data can be considered PII.
- It consists of a broad range of information that can identify individuals, including dates of birth, addresses, driver's license numbers, credit card numbers, bank account numbers, health and insurance records and much more.
- Privacy concerns exist wherever personally identifiable information or other sensitive information is collected and stored - in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues can arise in response to information from a wide range of sources, such as :
  1. Healthcare records
  2. Criminal justice investigations and proceedings
  3. Financial institutions and transactions
  4. Biological traits, such as genetic material
  5. Residence and geographic records
  6. Ethnicity
  7. Privacy breach
  8. Location-based service
- Privacy rules set out obligations in respect of two classes of information: "Personal Information", which includes any information that relates to a natural person, which directly or indirectly, is capable of identifying a person; and a smaller subset of Personal Information known as SPDI (Sensitive Personal Data or Information), which is information relating to passwords, financial information, health information, sexual orientation, medical records and biometric information. This accounts to the sensitive data which needs to be protected.
- For example, in a hospital, the patient records which is private information should be accessed only by the Doctor who is treating the patient and the Nurse who is on duty with the patient. Any other nurse or doctor in the hospital should not have access to those medical records.
- Any collection, processing, storage, use or transfer of personal information or SPDI which takes place through a computer or computer network located in India would have to comply with the IT Act and Privacy Rules.
- Protecting PII example scenario : A HR manager needs to provide important papers to a pension company. The company's network security solution must provide :
  1. Encryption that will keep the data safe if the manager's laptop is lost or stolen.
  2. Threat protection to keep his PC safe from viruses, phishing and other threats.
  3. Data loss prevention that will warn him he is about to send a file with PII.
  4. Policy compliance that will block him from using a browser with a known security vulnerability or stop him from saving the file to an unencrypted USB stick.
  5. Blocking of anonymous proxies for web searches, because they allow personal information to be accessed by administrators of the proxy server.

6.2 Cyber Stalking

Definition of stalking : *Threatening behavior or unwanted advances directed at another using the Internet and other forms of online and computer communications.*

- Cyber stalking is defined as the repeated use of the Internet, e-mail, or related digital electronic communication devices to annoy, alarm, or threaten a specific individual or group of individuals.
- Stories of criminal intimidation, harassment, fear, and suggestive violence where individuals use the Internet as a tool to stalk another person.
- Stalkers use victim information like mobile numbers, telephone numbers, addresses, and personal preferences to impinge upon their normal life. Some time cyber stalkers can learn what sorts of things upset their victims and can use this knowledge to harass the victims further.
- Stalkers target victims through chat rooms, WhatsApp, Hangouts, e-mail, facebook etc.
- Different forms of cyber stalking : Threatening e-mails, spam, and online verbal abuse, inappropriate messages on message boards, computer viruses, tracing internet activity, and identity theft.
- Effects of cyber stalking on person :
  1. Changes in sleeping and eating patterns
  2. Nightmares

3. Hyper vigilance
4. Anxiety
5. Helplessness
6. Fear for safety
7. Shock and disbelief

- Cyber stalking damages multiple aspects of victims' lives, from study to professional activity to their relationships with others. Survey respondents reported changing or losing jobs, isolating themselves by giving up social activities, and having important relationships break up.
- The Delhi police registered India's first case of cyber stalking. A case was registered under section 509 of the Indian Penal Code. One Mrs. Neha (Name changed) complained to the police against a person who was using her identity to chat over the Internet. She also complained that the person was chatting on the Net, using her name and giving her address and was talking obscene language. The same person was giving her telephone number to other chatters encouraging them to call her at odd hours.
- Stalkers usually make harassing phone calls, leave written messages or objects, or vandalize a person's property. Cyber stalkers meet or target their victims by using different search engines, bulletin and discussion boards, and online forums.
- Cyber stalkers use different social network sites and self publishing media such as Facebook, Twitter, Friendster, Bebo, Myspace and Indymedia etc. They try to damage the reputation of their victims by posting false information on websites, blogs or user pages. Many cyber stalkers use third parties to encourage them to join in their pursuit.
- They may order pornographic materials and sex toys, having them sent to their victim's address. Some cyber stalkers may arrange to meet their victims, especially young people who are at high risk of becoming their victims.
- Most stalking behavior is not a crime, at least not by itself. Calling someone over and over, texting numerous messages and leaving gifts are common behaviors that, on their own, do not constitute a crime.
- Section 354D says that anyone who monitors an individual's electronic communication and causes fear or distress is guilty of stalking, just as they are if they follow or attempt to contact them in the real world. The offender could get a fine and three years in jail.
- India is finally waking up to cyber stalking with the Criminal Law (Amendment) Bill, 2013, saying that stalking includes monitoring of a person's use of internet, email and electronic communication.
- Section 66A of the IT Act deals with cyber stalking. "A person who repeatedly sends emails can be booked under 66A, but not many know this."
- Two different kinds of cyber stalking situations which can occur.
  1. Online harassment and cyber stalking that occurs and continues on the internet.
  2. Online harassment and stalking that begins to be carried on offline too. This is when a stalker may attempt to trace a telephone number or a street address. Always be careful what details you give out over the web and to whom.
- The increasing use of the Internet and the ease with which it allows others unusual access to personal information, have made this form of stalking ever more accessible. Potential stalkers may find it easier to stalk via a remote device such as the Internet rather than to confront an actual person. You cannot stop the contact with a request. In fact, the more you protest or respond, the more rewarded the cyber stalker feels. The best response to cyber stalking is not to respond to the contact.

6.2.1 Motivates of Cyber Stalker

1. **Sexual harassment** : Sexual harassment is also a very common experience offline. The internet reflects real life and consists of real people. It's not a separate, regulated or sanctified world. A common form of sexual harassment on the Internet occurs when a harasser sends unwanted, abusive, threatening, or obscene messages to a victim via e-mail or instant messaging.
2. **Obsession for love** : This category is characterized by stalkers who develop a love obsession or fixation on another person with whom they have no personal relationship. It could also be an online romance that moves to real life, only to break-up once the persons really meet.
3. **Ego and power trips** : stalkers online showing off their skills to themselves and their friends. They do not have any grudge against you - they are rather using you to 'show-off' their power to their friends or doing it just for fun and you have been unlucky enough to have been chosen.

- Some other forms of cyber stalking are listed below :
  1. Sending inappropriate electronic greeting cards.
  2. Sending viruses.
  3. Sending harassing messages to the victim's.
  4. Hacking into the victim's computer.
  5. Posting personal advertisements in the victim's name.

6.2.2 Types of Stalkers

- There are three main types of stalkers :
  1. Simple obsessional
  2. Delusional
  3. Vengeful

Simple obsessional stalkers or domestic

- This is the most common type of stalker.
- Stalker, usually male, knows victim as an ex-spouse, ex-lover, or former boss, who they attempt to establish a relationship with and when rebuffed begin a campaign of harassment.
- This category represents 70-80 % of all stalking cases and is distinguished by the fact that some previous personal or romantic relationship existed between the stalker and the victim before the stalking behavior began.
- This kind of stalker may or may not have psychological disorders, all clearly have personality disorders. They refuse to believe that the relationship is over despite being told several times. They may have a history of other criminal behaviors.
- The love-obsessional stalker, who is typically a psychotic stalker targeting famous people or total strangers; and, most common. Stalker is a stranger to the victim but is obsessed with the victim and when rejected mounts a campaign of harassment to make the victim aware of the stalker's feelings.

Delusional stalkers

- Often have little contact with their victims
- Could have a mental disorder
- Often are unmarried, socially immature, isolated loners
- Typically choose a victim that is unattainable or who has shown them kindness in some way...a therapist, celebrity, clergy, teacher, doctor, etc.
- Can be dangerous and usually the rarest category of stalker.
- False belief that the victim shares the stalker's feelings and desire for a relationship.
- Here relationship based on stalker's psychological fixation. It also based on idealized love or spiritual union rather than sexual attraction.
- Target is usually a person with high visibility and a higher status.
- The danger period for a delusional is when they are falling out of love with one victim and in love with another victim.

Vengeful stalkers

- **Vengeful stalkers** may or may not have contact with their victims. They become angry with their victims over some real or perceived event or insult.
- They are as dangerous as delusional stalkers and are violent.
- Vengeful stalkers thinks you did them wrong and they want to make you pay for it.
- These stalkers may be stalking to get even and take revenge and believe that "they" have been victimized. Ex-spouses can turn into this type of stalker.

6.2.3 Typology of Cyber Stalking

- The typology of the stalker is defined by what the relationship is/was between the suspect and the victim. Stalker, usually female, falsely believes that the victim, usually someone famous or wealth is in love with them. The target is usually unobtainable by the suspect.
- Primarily, there are three ways of cyber stalking :
  1. E-mail stalking : Direct communication through e-mail
  2. Internet stalking : Global communication through internet
  3. Computer stalking : Unauthorized control of another person's computer
- Cyber stalkers use email as the primary means to harass and threaten victims, far more than any other electronic communication device.
- Emailing allows an offender to repeatedly transmit harassing, threatening, hateful, or obscene messages, including pictures, videos, or audio

Preventing cyber stalking

1. Do not post your personal information online.
2. Do not use your real name as a screen name.

Find out if your chat client or ISP network has a policy against cyber stalking.

Be careful about meeting friends that you have talked to online.

6.2.4 Types of Stalkers

The resentful / rejected stalker : The rejected suitor is when someone stalks their ex lover because in their mind they think that it is the only relationship they will ever have and believe that there is no other possibility except for that one relationship. In some cases these types of stalkers have some type of psychological disorder.

The intimacy seeker is similar to the rejected suitor except that this stalker is trying to create a relationship with what he or she believes is their one and only and the rejected suitor is a person that is trying to get back an old recent relationship.

The incompetent suitor is usually a man that has been turned down by a woman that they would like to develop a relationship with. After being turned down the stalker begins to repeatedly bother her and hope that his actions with let the women see that he is willing to work for the relationship and she will change her mind.

The perdatory stalker is a stalker that usually chooses victims at random with intent to commit a sexual crime with their victim. The initial motivation is to gather information about the potential victim and gain access to their life. This is to most dangerous type of stalker.

6.2.5 Investigating Cyber Stalking

Following are the some of the methods for investigating the cyber stalking :

1. Take interview of victim person.
2. Take interview of other persons.
3. Check Risk assessment
4. Find out any other additional digital evidence
5. Purpose of the crime or characteristics
6. Motivation
7. Repeat the steps until

Take interview of victim person : Victim has to submit the proof about cyber stalking. The investigator has to check proof before taking any action. Collect the initial information from victim and develop victimology.

- After gathering all information, investigation will move forward. The whole story needs to be heard from the perspective of the complainant's history with the suspect in order to properly.
- **Take interview of other persons :** If suppose other persons involved in this case, investigator will take interview of all that peoples. It will help to understand the case.
- **Check risk assessment :** Check the relationship between victim and an offender.
- **Find out any other additional digital evidence :** What is known about the victim and cyber stalker to perform a thorough search of the Internet ? Aim of this stage is to collect detail information about victim, cyber stalker and crime.
- **Purpose of the crime or characteristics :** Find out the depth of crime scenes. Find the location where the cyber stalker and victim meet. There is any physical location and over the internet they meet without knowing to each other.
- **Motivation :** Determine personal interest of cyber stalker.
- Repeat the steps until you reach to the cyber stalker.

6.3 PII Impact Levels with Examples

- The following describe the three impact levels : low, moderate and high

1. Low

- The potential impact is LOW if the loss of confidentiality, integrity or availability could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.
- A limited adverse effect means that, for example, the loss of confidentiality, integrity or availability might
  (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
  (ii) result in minor damage to organizational assets;
  (iii) result in minor financial loss;
  (iv) result in minor harm to individuals.

2. Moderate

- The potential impact is MODERATE if the loss of confidentiality, integrity or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- A serious adverse effect means that, for example, the loss of confidentiality, integrity or availability might
  (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
  (ii) result in significant damage to organizational assets;
  (iii) result in significant financial loss;
  (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

3. High

- The potential impact is HIGH if the loss of confidentiality, integrity or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.
- A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity or availability might
  i. cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
  ii. result in major damage to organizational assets;
  iii. result in major financial loss; or
  iv. result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

6.4 Cybercrime

- Cyber safety is a common term used to describe a set of practices, measures and/or actions you can take to protect personal information and your computer from attacks.
- There is no standard definition for "**CYBER**". This word is used to describe the virtual world of computers e.g. an object in cyberspace refers to a block of data floating around a computer system or network.
- The word "cyberspace" is credited to William Gibson, who used it in his book, Neuromancer, written in 1984.
- Cyberspace : The impression of space and community formed by computers, computer networks, and their users ; the virtual "world" that Internet users inhabit when they are online.
- The term 'cyber' is derived from the word 'cybernetics' which means science of communication and control over machine and man.
- Cyberspace is the new horizon which is controlled by machine for information and communication between human beings across the world.
- Therefore, crimes committed in cyberspace are to be treated as cyber crimes. In wider sense, cyber crime is a crime on the Internet which includes hacking, terrorism, fraud, gambling, cyber stalking, cyber theft, cyber pornography, flowing of viruses etc.
- Over the past few years, the global cyber crime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security.
- Until recently, malware, spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer 'geniuses' showcasing their talent.
- Cyber criminals are now moving beyond computers, and attacking mobile handheld devices, such as smart phones and tablet personal computers. In 2010, the number of malicious software programs specifically targeting mobile devices, rose 46 %, according to information technology security group McAfee.
- **Cybercrime** is defined as crimes committed on the internet using the computer as either a tool or a targeted victim.
- **Cybercrime** is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).
- Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime.

6.4.1 Types of Cyber Crimes

There are many types of cyber crimes and the most common ones are explained below :

1. **Hacking** : This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed.
2. **Theft** : This crime occurs when a person violates copyrights and downloads music, movies, games and software.
3. **Cyberstalking** : This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails.
4. **Identity theft** : This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, debit card and other sensitive information to siphon money or to buy things online in the victim's name.
5. **Malicious software** : These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.
6. **Child soliciting and abuse** : This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography.

Example of Cyber Crime :

1. Online banking fraud
2. Fake antivirus
3. 'Stranded traveler' scams
4. 'Fake escrow' scams
5. Advanced fee fraud
6. Infringing pharmaceuticals
7. Copyright-infringing software
8. Copyright-infringing music and video
9. Online payment card fraud
10. In-person payment card fraud
11. Industrial cyber-espionage and extortion
12. Welfare fraud

- The trafficking, distribution, posting, and dissemination of obscene material including pornography, indecent exposure, and child pornography, constitutes one of the most important Cybercrimes known today.
- Stealing the significant information, data, account number, credit card number transmit the data from one place to another. Hacking and cracking are amongst the gravest Cybercrimes known till date.

6.4.2 Botnets

- A botnet is an interconnected network of computers infected with malware without the user's knowledge and controlled by cybercriminals.
- They're typically used to send spam emails, transmit viruses and engage in other acts of cybercrime. Sometimes known as a zombie army, botnets are often considered one of the biggest online threats today.
- Computers in a botnet, called nodes or zombies, are often ordinary computers sitting on desktops in homes and offices around the world.
- Typically, computers become nodes in a botnet when attackers illicitly install malware that secretly connects the computers to the botnet and they perform tasks such as sending spam, hosting or distributing malware or other illegal files, or attacking other computers.
- Fig. 6.4.1 shows botnet.

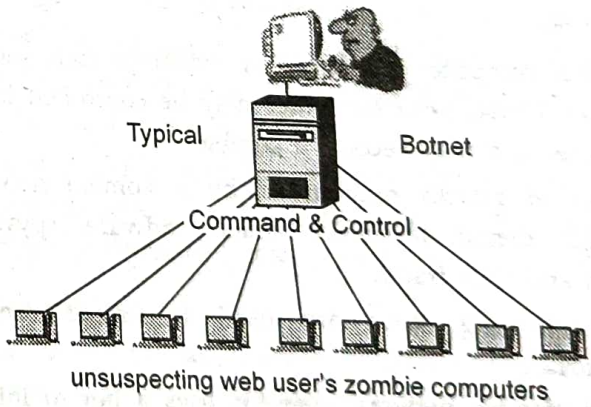


Fig. 6.4.1 Botnet

- Attackers usually install bots by exploiting vulnerabilities in software or by using social engineering tactics to trick users into installing the malware. Users are often unaware that their computers are being used for malicious purposes.
- The word Botnet is formed from the words 'robot' and 'network'. Cybercriminals use special Trojan viruses to breach the security of several users' computers, take control of each computer, and organize all of the

infected machines into a network of 'bots' that the criminal can remotely manage.

- A zombie or bot is often created through an Internet port that has been left open and through which a small Trojan horse program can be left for future activation. At a certain time, the zombie army "controller" can unleash the effects of the army by sending a single command, possibly from an Internet Relay Channel (IRC) site.
- Botnets can be used to :
  1. Send out spam emails
  2. Launch a Distributed Denial of Service Attack
  3. Commit advertising fraud
  4. Distribute malware, or spyware
- Keep phishing websites active and frequently change their domains to remain anonymous and undetected by law enforcement.

6.4.3 Zombie

- Zombie computer is a computer connected to the Internet that has been compromised and controlled by an attacker without user's consent.
- Zombie network (Botnet) refers to a network of zombie computers under the remote control by an attacker. Attackers control their botnets through some command and control centers to perform illegal activities.
- If your computer is infected by malicious code such as Trojan Horse, your computer may be controlled by an attacker and may become a zombie.
- Types of attacks perpetrated by a zombie network include denial of service attacks, adware, spyware, spam and click fraud.
- The following steps are used to create zombie networks :
  1. A zombie network operator uses a bot to infect thousands of computers with worms or viruses that carry a deadly payload.
  2. The bot inside an infected computer logs on to an online server - usually IRC but sometimes Web.
  3. The zombie network operator leases zombie network services to a customer.
  4. The customer provides the zombie network operator with spam or any other material, which is run through the zombie network.
- Another botnet called, Gameover Zeus Botnet, allows cyber criminals to retrieve banking passwords from infected machines, or use the botnet to infect more computers.

How and Why Do Cyber Criminals Use Botnets ?

- The value of bots and botnets to criminals comes from aggregating massive numbers of computers they can control simultaneously to perform malicious activities.
- Cyber criminals may use the botnets to send spam, phishing emails, or other scams to trick consumers into giving up their financial information.
- Cyber criminals may also collect information from the bot-infected machines and use it to steal identities, incurring loans, and purchase charges under the user's name.
- Cyber criminals may use botnets to create denial-of-service (DoS) attacks that flood a legitimate service or network with a crushing volume of traffic. The volume may severely slow down, or even shut down, the organization's business operations.
- Revenue from DoS attacks come through extortion and leasing botnets. The criminals will rent botnets to groups interested in inflicting damage to another entity.
- The "renters" will use the botnet for sending spam and phishing emails or attacking legitimate websites and networks.

6.4.4 Classification of Cybercrime

1. Cyber pornography

- Pornography on the internet may take various forms. It may include hosting of website containing some obscene or prohibited material or use of computer for producing obscene materials. Such material tends to pervert the thinking of adolescents and corrupt their mind set.
- A person who publishes or transmits or causes to be published in the electronic form any material which is lascivious, or if its effects in such as to tend to deprave or corrupt the persons who are likely to see, wad or hear the matter contained or embodied in it, is liable to punishment.
- The important ingredients of such an offence are publication and transmission through any electronic medium, of pornographic material in any electronic form.

- Cyber pornography is in simple words defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials. With the advent of cyberspace, traditional pornographic content has now been largely replaced by online/digital pornographic content.
- Pornography has no legal or consistent definition. The definition of pornography depends how the society, norms and their values are reacting to the pornographic content.

2. Email spoofing

- A hacker logging in to a computer of under was to his victim often will login under a different identity. This is called spoofing. The hacker able to the by, having previously actual password or having created a new identity by fooling the computer into thinking he is the system's operator.
- A spoofed a may email may be said to be one which the be miss represent its origin. That is, it shows its online to be different from which it actually originates.
- For example, where A sends a threatening a email to the president of the students a union threatening to detente a nuclear sent from the college compos and this email was sent from the account of some other student "A" would a be quality of email spoofing.

3. Identity theft

- Identity theft and fraud is one of the most common types of cybercrime. The term Identity Theft is used, when a person purports to be some other person, with a view to creating a fraud for financial gains.
- When this is done online on the Internet, its is called Online Identity Theft.
- The most common source to steal identity information of others, are data breaches affecting government or federal websites.
- It can be data breaches of private websites too, that contain important information such as, credit card information, address, email ID's, etc.

4. Data diddling

- This offence involves changing or reusing of data in sub till of ways which makes of it different to put the data subtitle ways which data back of or be curtain of its accuracy.
- This is resorted to for the purpose of illegal monetary gains or for community of fraud of financial scam. In case of scan the criminal are change of data which is related on the scan.
- In this data are changed of computer system, record are destroy of and alterations of information of and other type of frauds.

5. Email bombing

- This is another form of internet misuse where individuals directs amass numbers of mail to the victim or an address in attempt to overflow the mailbox, which may be an individual or a company or even mail servers there by ultimately resulting into crashing. There are two methods of perpetrating an email bomb which include mass mailing and list linking.

6. Internet time thefts

- This form is kinds of embezzlements where the fraudulent uses the Internet surfing hours of the victim as their own which can be complete by obtaining access to the login ID and the password, an example is Colonel Bajwa's case- in this incident the Internet hours were used up by a unauthorized person.

7. Salami attacks

- This kind of crime is normally consisting of a number of smaller data security attacks together end resulting in one major attack.
- This method normally takes place in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed.
- This form of cybercrime is very common in banks where employees can steal small amount and it's very difficult to detect or trace.

8. Web jacking

- This is where the hacker obtains access and can control web site of another person, where he or she can destroy or alter the information on the site as they see fit to them. This type of method of cybercrime is done for satisfying political agendas or for purely monetary means.

9. Hacking

- In other words can be referred to as the unauthorize access to any computer systems or network. Th method can occur if computer hardware and softwa has any weaknesses which can be infiltrated if su

- Cyber pornography is in simple words defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials. With the advent of cyberspace, traditional pornographic content has now been largely replaced by online/digital pornographic content.
- Pornography has no legal or consistent definition. The definition of pornography depends how the society, norms and their values are reacting to the pornographic content.

2. Email spoofing

- A hacker logging in to a computer of under was to his victim often will login under a different identity. This is called spoofing. The hacker able to the by, having previously actual password or having created a new identity by fooling the computer into thinking he is the system's operator.
- A spoofed a may email may be said to be one which the be miss represent its origin. That is, it shows its online to be different from which it actually originates.
- For example, where A sends a threatening a email to the president of the students a union threatening to detente a nuclear sent from the college compos and this email was sent from the account of some other student "A" would a be quality of email spoofing.

3. Identity theft

- Identity theft and fraud is one of the most common types of cybercrime. The term Identity Theft is used, when a person purports to be some other person, with a view to creating a fraud for financial gains.
- When this is done online on the Internet, its is called Online Identity Theft.
- The most common source to steal identity information of others, are data breaches affecting government or federal websites.
- It can be data breaches of private websites too, that contain important information such as, credit card information, address, email ID's, etc.

4. Data diddling

- This offence involves changing or reusing of data in sub till of ways which makes of it different to put the data subtitle ways which data back of or be curtain of its accuracy.
- This is resorted to for the purpose of illegal monetary gains or for community of fraud of financial scam. In case of scan the criminal are change of data which is related on the scan.
- In this data are changed of computer system, record are destroy of and alterations of information of and other type of frauds.

5. Email bombing

- This is another form of internet misuse where individuals directs amass numbers of mail to the victim or an address in attempt to overflow the mailbox, which may be an individual or a company or even mail servers there by ultimately resulting into crashing. There are two methods of perpetrating an email bomb which include mass mailing and list linking.

6. Internet time thefts

- This form is kinds of embezzlements where the fraudulent uses the Internet surfing hours of the victim as their own which can be complete by obtaining access to the login ID and the password, an example is Colonel Bajwa's case- in this incident the Internet hours were used up by a unauthorized person.

7. Salami attacks

- This kind of crime is normally consisting of a number of smaller data security attacks together end resulting in one major attack.
- This method normally takes place in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed.
- This form of cybercrime is very common in banks where employees can steal small amount and it's very difficult to detect or trace.

8. Web jacking

- This is where the hacker obtains access and can control web site of another person, where he or she can destroy or alter the information on the site as they see fit to them. This type of method of cybercrime is done for satisfying political agendas or for purely monetary means.

9. Hacking

- In other words can be referred to as the unauthorized access to any computer systems or network. This method can occur if computer hardware and software has any weaknesses which can be infiltrated if such

hardware or software has a lack in patching, security control, configuration or poor password choice.

10. Software piracy

- Software piracy is the illegal copying, distribution, or use of software. It is such a profitable "business" that it has caught the attention of organized crime groups in a number of countries.
- Piracy includes casual copying of particular software by an individual or business.
- Using pirated software is also risky for users. Aside from the legal consequences of using pirated software, users of pirated software forfeit some practical benefits as well. Those who use pirate software:
  a) Increase the chances that the software will not function correctly or will fail completely;
  b) Forfeit access to customer support, upgrades, technical documentation, training, and bug fixes;
  c) Have no warranty to protect themselves;
  d) Increase their risk of exposure to a debilitating virus that can destroy valuable data;
  e) May find that the software is actually an outdated version, a beta (test) version, or a nonfunctioning copy;
  f) Are subject to significant fines for copyright infringement; and
  g) Risk potential negative publicity and public and private embarrassment.
- The software licensure agreement is a contract between the software user and the software developer. Usually, this agreement has certain terms and conditions the software user must follow.
- When the user doesn't follow the rules and regulations, they are guilty of software piracy. Some of these terms and conditions prohibit:
  1. Using multiple copies of a single software package on several computers
  2. Passing out copies of software to others without the proper documentation
  3. Downloading or uploading pieces of software via bulletin boards for others to copy
  4. Downloading and installing shareware without paying for it.
- Examples of documents that support the information security program include a configuration management plan, a contingency plan, an incident response plan, a security awareness and training plan, rules of behavior, a risk assessment, a security test and evaluation results, system interconnection agreements, security authorizations and accreditations, and a plan of action and milestones.
- This step provides the necessary security authorization of an information system to process, store, or transmit information that is required.
- This authorization is granted by a senior organization official and is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified residual risk to agency assets or operations.
- **Monitoring** ensures that controls continue to be effective in their application through periodic testing and evaluation.
- Security control monitoring, such as verifying the continued effectiveness of those controls over time, and reporting the security status of the information system to appropriate agency officials are essential activities of a comprehensive information security program.
- Assessment may be internal or external. The internal assessment is a controlled network attack simulation that is used to gauge the exposure present on internal systems, applications, and network devices.
- The assessment provides a more structured approach to identifying vulnerabilities that may go undetected.
- The goal of an external assessment is to quantify the security risk that is associated with Internet-connected systems.
- Preliminary risk assessment : This step results in an initial description of the security needs of the system. A preliminary risk assessment should define the threat environment in which the system will operate.

6.5 PII Confidentiality Safeguards

- Confidential data refers to any data pertaining to individuals or the University that is sensitive, private or of a personal nature or data that is protected under a confidentiality agreement, regulation, law or University procedure.
- The confidentiality of PII should be protected based on its impact level.
- Confidential information means any information not exempted in specific legislation and identified as personal, sensitive or confidential such as

personally - identifiable information, individuali; - identifiable health information, education records and non-public information as specified in all applicable federal or state laws.

- Organizations should evaluate how easily PII can be used to identify specific individuals. For example, PII data composed of individuals' names, fingerprints or SSNs uniquely and directly identify individuals, whereas PII data composed of individuals' ZIP codes and dates of birth can indirectly identify individuals or can significantly narrow large datasets.
- However, data composed of only individuals' area codes and gender usually would not provide for direct or indirect identification of an individual depending upon the context and sample size.
- Thus, PII that is uniquely and directly identifiable may warrant a higher impact level than PII that is not directly identifiable by itself.
- Organizations should evaluate the sensitivity of each individual PII data field, as well as the sensitivity of the PII data fields together.
- For example, an individual's SSN, medical history, or financial account information is generally considered more sensitive than an individual's phone number or ZIP code.
- Organizations often require the PII confidentiality impact level to be set at least to moderate if a certain data field, such as SSN, is present.
- Organizations may also consider certain combinations of PII data fields to be more sensitive, such as name and credit card number, than each data field would be considered without the existence of the others.
- Data fields may also be considered more sensitive based on potential harm when used in contexts other than their intended use.
- For example, basic background information, such as place of birth or parent's middle name, is often used as an authentication factor for password recovery at many web sites.

6.6 Information Protection Law : Indian Perspective

- The Indian government has created the necessary legal and administrative framework through the enactment of Information Technology Act 2000, which combines the e-commerce transactions and computer misuse and frauds rolled into an Omnibus Act.
- While on the one hand it seeks to create the Public Key Infrastructure for electronic authentication through the digital signatures, on the other hand, it seeks to build confidence among the public that the frauds in the cyber space will not go unpunished.
- The Controller of Certifying Authority (CCA) has been put in place for the effective implementation of the IT Act, 2000.
- The Act also enables e-governance applications for the electronic delivery of services to the public, business and government.
- The Information technology Act, 2000 has been enacted by the legislators with the prime intention of ensuring that the communication through electronic medium is facilitated and all sorts of ambiguity regarding the authenticity of the communication is fixed for once and all.

6.6.1 Indian IT Act

- In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000.
- This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand the various perspectives of the IT Act, 2000 and what it offers.
- The Information Technology Act, 2000 also aims to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.
- Some highlights of the Act are listed below :
  a. Chapter-II of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.

b. Chapter-III of the Act details about Electronic Governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is -

- rendered or made available in an electronic form; and
- accessible so as to be usable for a subsequent reference

The said chapter also details the legal recognition of Digital Signatures.

c. Chapter-IV of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates.

d. Chapter-VII of the Act details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also enshrined in the said Act.

e. Chapter-IX of the said Act talks about penalties and adjudication for various offences. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation not exceeding ₹ 1,00,00,000 to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under. The said Adjudicating Officer has been given the powers of a Civil Court.

f. Chapter-X of the Act talks of the establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.

g. Chapter-XI of the Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information, which is obscene in electronic form and hacking.

The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act.

The said Act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

6.6.2 Cyber Laws and Crimes as per the Indian IT Act

- The IT Act covers cyber laws and crimes, which are subject to the Indian Penal Code. Such cyber crimes include :
  - Crimes related to technical aspects, such as unauthorized access and hacking, trojan attack, virus and worm attack, email related attacks (email spoofing and email spamming, email bombing) and Denial Of Service attacks (DOS). DOS include :
    1. Consumption of limited or non-renewable resources like NW bandwidth and RAM, alteration or destruction of configuration information, destruction or alteration of network components and pornography.
    2. Forgery
    3. IPR violations, which include software piracy, copyright infringement, trademark violations, etc. This also includes cyber terrorism, Banking and credit card related crimes, e-Commerce and investment frauds, sale of illegal articles, defamation.
    4. Cyber stacking, identity theft, data diddling, theft of internet hours.
    5. Breach of privacy and confidentiality.

6.6.3 Advantages of Cyber Law

- The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. Such laws are required so that people can perform purchase transactions over the Net through credit cards without fear of misuse.
- The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.
- In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format.
- The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.
- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects.
- Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
- Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.
- The Act now allows Government to issue notification on the web thus heralding e-governance.
- The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.
- Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding ₹ 1 crore.

6.6.4 A Global Perspective on Cybercrimes

- The rapid development of Internet and Computer technology globally has led to the growth of new forms of transnational crime especially Internet related.
- These crimes have virtually no boundaries and may affect any country across the globe.
- Thus, there is a need for awareness and performing of necessary legislation in all countries for the prevention of computer related crime.
- Globally Internet and Computer based commerce and communications cut across territorial boundaries, thereby creating a new realm of human activity and undermining the feasibility and legitimacy of applying laws based on geographic boundaries.
- This new boundary, which is made up of the screens and passwords, separate the "Cyber world" from the "real world" of atoms. Territorially based law- making and law-enforcing authorities find this new environment deeply threatening.

6.7 IT Act

- The present laws governing Information and Communication Technology have been derived from the Indian Telegraph Act 1885, Indian Wireless Telegraphy Act 1933, The Telegraph Wire Unlawful Possession Act 1950 and the Cable Television Networks (Regulation) Act 1995.
- In the recent past the Telecom Regulatory Authority of India Act 1997 (TRAI Act) was enacted, paving way for the constitution of the first ever telecom regulatory body in India, known as Telecom Regulatory Authority of India (TRAI).
- The TRAI apart from telecom has recently been entrusted with the task of regulating and drafting of policies relating to broadcasting sector.
- The growth of IT industry and e-commerce, lead the government to enact the Information Technology Act 2000 (IT Act 2000).
- The issues relating to cyber crimes, data security, digital signatures, electronic commerce etc are covered under the IT Act 2000.

- The IT Act 2000 grants legal sanction to e-commerce transactions and also prohibits breach of confidentiality and privacy.

6.7.1 Aim and Objectives of IT Act, 2000

- The important aims and objectives of the IT Act, 2000 are :

1. To suitably amend existing laws in India to facilitate e-commerce.
2. To provide legal recognition of electronic records and digital signatures.
3. To provide legal recognition to the transactions carried out by means of Electronic Data Interchange (EDI) and other means of electronic communication.
4. To provide legal recognition to business contacts and creation of rights and obligations through electronic media.
5. To establish a regulatory body to supervise the certifying authorities issuing digital signature certificates.
6. To create civil and criminal liabilities for contravention of the provisions of the Act and to prevent misuse of the e-business transactions.
7. To facilitate e-governance and to encourage the use and acceptance of electronic records and digital signatures in government offices and agencies. This would also make the citizen-government interaction more hassle free.
8. To make consequential amendments in the Indian Penal Code, 1860 and the Indian Evidence Act, 1872 to provide for necessary changes in the various provisions which deal with offences relating to documents and paper based transactions.
9. To amend the Reserve Bank of India Act, 1934 so as to facilitate electronic fund transfers between the financial institutions.
10. To amend the Banker's Books Evidence Act, 1891 so as to give legal sanctity for books of accounts maintained in the electronic form by the banks.
11. To make law in tune with Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) adopted by the General Assembly of the United Nations.

6.7.2 Importance of IT Act

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects.

a) Firstly, the implication of these provisions for the e-businesses is that email is now a valid and legal form of communication in our country that can be duly produced and approved in a court of law.

b) Companies are now able to carry out electronic commerce using the legal infrastructure provided by the Act.

c) Digital signatures have been given legal validity and sanction in the Act.

d) The Act opens the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signature Certificates.

e) The Act now allows Government to issue notification on the web thus heralding e-governance.

f) The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate. Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

g) The IT Act also addresses the important issues of security, which are critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to be passed through a system of a security procedure, as stipulated by the Government at a later date.

Under the IT Act, 2000, it is possible for corporate to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding ₹ 5 crores.

6.8 Remote Connectivity and VoIP Hacking

- Various categories of remote hacking include :
  1. Dial-up hacking
  2. PBX (Private Branch Exchange) hacking
  3. Voice mail hacking
  4. VPN hacking
  5. VoIP attacks

1. Dial-up hacking

- Dial-up hacking is possible by both ways analog dial-up hacking and wardialing. This can be done by phone number footprinting, social engineering and corporate websites.

2. PBX hacking

- A PBX connects the internal telephones of a company and saves money on intra-company calls.
- PBX vendor usually tells their customers that they need dial-in access for external support. But it is done often insecurly, leaving a modem always on and connected to PBX. It should be turned off except when needed.

3. Voice-mail hacking

- Voice mail is often important confidential and poorly secured.
- Executives often neglect to pick an unique code for voice mail.
- People often use simple geometrical patterns on the keypads.

4. VPN hacking

- VPN has replaced dial-up as the remote access mechanism.
- VPN connects two computers using tunneling.

6.9 Wireless Hacking

- Different security mechanisms in wireless networks are :
  1. Basic level : MAC filtering
  2. Authentication : WPA-PSK, WPA enterprise, hand shake
  3. Encryption at layer-2 : WEP, TKIP, AES
- Equipments used for haking :
  1. Wireless adapters : Chipset, band support, antenna support, interface.
  2. OS : Windows, Linux
- Discovering and monitoring wireless networks has two steps :
  1. Finding wireless networks : Active or passive discovery
  2. Sniffing wireless traffic : Thwarting wireless shiffing.
- Various attacks are
  1. Devial of service attacks
  2. Encryption attacks
  3. Authentication attacks (WPAPSK, WPA enterprise)

6.10 Mobile Hacking

- Rooting Android to get administrative privileges such as full control of device.
- Common Android rooting tools are : Superone click, Z4Root
- Apps for rooted Android devices :
  1. Super user
  2. ROM manager
  3. Market enabler
  4. ConnectBot
  5. ScreenShot
  6. Set CPU
  7. Juice Defender
- Tools for modify an app :
  1. apk tool : unzip and repack android application (apk) file
  2. signAPK : Verify the repacked file
- Vulnerabilities in android :
  1. Remote shell via webkit
  2. Root an android remotely
  3. Data stealing through PHP file
  4. Remote shell with zero permissions
  5. Exploiting capability leaks
  6. URL sourced malware (side-load applications)
  7. Skype data exposure
  8. Cracking the google wallet PIN.

Review Questions

1. *What is cyber stalking ? Explain types of cyber stalkers.*
2. *Explain PII impact levels with examples.*
3. *Explain cyber crime.*
4. *Explain Indian IT Act.*