Chapter 1
Introduction

1.1).What is the OSI security architecture?

The OSI Security Architecture is a framework that provides a systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. The document defines security attacks, mechanisms, and services, and the relationships among these categories.

1.2).What is the difference between passive and active security threats?

Passive attacks have to do with eavesdropping on, or monitoring, transmissions. Electronic mail, file transfers, and client/server exchanges are examples of transmissions that can be monitored.

Active attacks include the modification of transmitted data and attempts to gain unauthorized access to computer systems.

1.3).List and briefly define categories of passive and active security attacks.

Passive attacks: release of message contents and traffic analysis.

Active attacks: masquerade, replay, modification of messages, and denial of service.

1.4).List and briefly define categories of security services.

Authentication: The assurance that the communicating entity is the one that it claims to be.

Access control: The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

Data confidentiality: The protection of data from unauthorized disclosure.

Data integrity: The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Nonrepudiation: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Availability service: The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them).

1.5). List and briefly define categories of security mechanisms.

Encipherment: The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

Digital Signature: Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

Access Control: A variety of mechanisms that enforce access rights to Resources.

Data Integrity: A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange: A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding: The insertion of bits into gaps in a data stream to Frustrate traffic analysis attempts.

Routing Control: Enables selection of particular physically secure Routes for certain data and allows routing changes, especially when a breach of security is suspected.

Notarization: The use of a trusted third party to assure certain Properties of a data exchange.

Chapter 2
Classical Encryption Techniques

2.1).What are the essential ingredients of a symmetric cipher?

- Plaintext
- Encryption algorithm
- Secret key
- Cipher text
- Decryption algorithm

2.2).What are the two basic functions used in encryption algorithms?

- Permutation
- Substitution

2.3). How many keys are required for two people to communicate via a cipher?

- One key for symmetric ciphers
- Two keys for asymmetric ciphers.

2.4).What is the difference between a block cipher and a stream cipher?

A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. A block cipher is one in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length.

2.5).What are the two general approaches to attacking a cipher?

- Cryptanalysis
- Brute force.

2.6).List and briefly define types of cryptanalytic attacks based on what is known to the attacker.

Cipher text only: One possible attack under these circumstances is the brute-force approach of trying all possible keys. If the key space is very large, this becomes impractical. Thus, the opponent must rely on an analysis of the cipher text itself
Known plaintext: The analyst may be able to capture one or more plaintext messages as well as their encryptions. With this knowledge, the analyst may be able to deduce the key on the basis of the way in which the known plaintext is transformed.
Chosen plaintext: If the analyst is able to choose the messages to encrypt, the analyst may deliberately pick patterns that can be expected to reveal the structure of the key.

2.7).What is the difference between an unconditionally secure cipher and a computationally secure cipher?

An encryption scheme is **unconditionally secure** if the cipher text generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much cipher text is available. An encryption scheme is said to be **computationally secure** if: (1) the cost of breaking the cipher exceeds the value of the encrypted information, and (2) the time required to break the cipher exceeds the useful lifetime of the information.

2.8).Briefly defines the Caesar cipher.

The Caesar cipher involves replacing each letter of the alphabet with the letter standing k places further down the alphabet, for k in the range 1 through 25.

2.9).Briefly defines the monoalphabetic cipher.

A monoalphabetic substitution cipher maps a plaintext alphabet to a cipher text alphabet, so that each letter of the plaintext alphabet maps to a single unique letter of the cipher text alphabet.

2.10).Briefly defines the Play fair cipher.

The Play fair algorithm is based on the use of a 5 * 5 matrix of letters constructed using a keyword. Plaintext is encrypted two letters at a time using this matrix.

2.11).What is the difference between a monoalphabetic cipher and a polyalphabetic cipher?

A **polyalphabetic substitution** cipher uses a separate monoalphabetic substitution cipher for each successive letter of plaintext, depending on a key.

2.12).What are two problems with the one-time pad?

1. There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.
2. Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

2.13).What is a transposition cipher?

A transposition cipher involves a permutation of the plaintext letters.

2.14).What is steganography?

Steganography involves concealing the existence of a message.

Chapter 3
Block Ciphers and the Data Encryption Standard

3.1). Why is it important to study the Feistel cipher?

Most symmetric block encryption algorithms in current use are based on the Feistel block cipher structure. A study of the Feistel structure reveals the principles behind these recent ciphers.

3.2).What is the difference between a block cipher and a stream cipher?

A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. A block cipher is one in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length.

3.3).Why is it not practical to use an arbitrary reversible substitution cipher of the kind shown in Table 3.1?

If a small block size, such as n = 4, is used, then the system is equivalent to a classical substitution cipher. For small n, such systems are vulnerable to a statistical analysis of the plaintext. For a large block size, the size of the key, which is on the order of n * 2^n, makes the system impractical.

3.4).What is a product cipher?

In a product cipher, two or more basic ciphers are performed in sequence in such a way that the final result or product is cryptographically stronger than any of the component ciphers.

3.5).What is the difference between diffusion and confusion?

In **diffusion**, the statistical structure of the plaintext is dissipated into long-range statistics of the cipher text. This is achieved by having each plaintext digit affect the value of many cipher text digits, which is equivalent to saying that each cipher text digit is affected by many plaintext digits.

Confusion seeks to make the relationship between the statistics of the cipher text and the value of the encryption key as complex as possible, again to thwart attempts to discover the key. Thus, even if the attacker can get some handle on the statistics of the cipher text, the way in which the key was used to produce that cipher text is so complex as to make it difficult to deduce the key. This is achieved by the use of a complex substitution algorithm.

3.6).Which parameters and design choices determine the actual algorithm of a Feistel cipher?

Block size: Larger block sizes mean greater security (all other things being equal) but reduced encryption/decryption speed.

Key size: Larger key size means greater security but may decrease encryption/decryption speed.

Number of rounds: The essence of the Feistel cipher is that a single round offers inadequate security but that multiple rounds offer increasing security.

Sub key generation algorithm: Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.

Round function: Again, greater complexity generally means greater resistance to cryptanalysis.

Fast software encryption/decryption: In many cases, encryption is embedded in applications or utility functions in such a way as to preclude a hardware implementation. Accordingly, the speed of execution of the algorithm becomes a concern.

Ease of analysis: Although we would like to make our algorithm as difficult as possible to cryptanalyze, there is great benefit in making the algorithm easy to analyze. That is, if the algorithm can be concisely and clearly explained, it is easier to analyze that algorithm for cryptanalytic vulnerabilities and therefore develop a higher level of assurance as to its strength.

3.7).What is the purpose of the S-boxes in DES?

The S-box is a substitution function that introduces nonlinearity and adds to the complexity of the transformation.

3.8).Explain the avalanche effect.

The avalanche effect is a property of any encryption algorithm such that a small change in either the plaintext or the key produces a significant change in the cipher text.

3.9).What is the difference between differential and linear cryptanalysis?

Differential cryptanalysis is a technique in which chosen plaintexts with particular XOR difference patterns are encrypted. The difference patterns of the resulting cipher text provide information that can be used to determine the encryption key.

Linear cryptanalysis is based on finding linear approximations to describe the transformations performed in a block cipher.

Chapter 4
Finite Fields

4.1).Briefly defines a group.

A group is a set of elements that is closed under a binary operation and that is associative and that includes an identity element and an inverse element.

4.2).Briefly defines a ring.

A ring is a set of elements that is closed under two binary operations, addition and subtraction, with the following: the addition operation is a group that is commutative; the multiplication operation is associative and is distributive over the addition operation.

4.3).Briefly defines a field.

A field is a ring in which the multiplication operation is commutative, has no zero divisors, and includes an identity element and an inverse element.

4.4).What does it mean to say that is a divisor of?

A nonzero b is a divisor of "a" if a = mb for some m, where a, b, and m are integers. That is, b is a divisor of "a" if there is no remainder on division.

4.5).What is the difference between modular arithmetic and ordinary arithmetic?

In modular arithmetic, all arithmetic operations are performed modulo some integer.

4.6).List three classes of polynomial arithmetic.

(1) Ordinary polynomial arithmetic, using the basic rules of algebra.

(2) Polynomial arithmetic in which the arithmetic on the coefficients is performed over a finite field; that is, the coefficients are elements of the finite field.

(3) Polynomial arithmetic in which the coefficients are elements of a finite field, and the polynomials are defined modulo a polynomial M(x) whose highest power is some integer n.

Chapter 5
Advanced Encryption Standard

5.1).What was the original set of criteria used by NIST to evaluate candidate AES ciphers?

Security: Actual security; randomness; soundness, other security factors.

Cost: Licensing requirements; computational efficiency; memory requirements.

Algorithm and Implementation Characteristics: Flexibility; hardware and software suitability; simplicity.

5.2).What was the final set of criteria used by NIST to evaluate candidate AES ciphers?

- General security
- Software implementations
- Restricted-space environments
- Hardware implementations
- Attacks on implementations
- Encryption vs. decryption; key agility
- Other versatility and flexibility
- Potential for instruction-level parallelism

5.3).What is the difference between Rijndael and AES?

Rijndael allows for block lengths of 128, 192, or 256 bits. AES allows only a block length of 128 bits.

5.4).What is the purpose of the State array?

The State array holds the intermediate results on the 128-bit block at each stage in the processing.

5.5). How is the S-box constructed?

1. Initialize the S-box with the byte values in ascending sequence row by row. The first row contains {00}, {01}, {02}, etc., the second row contains {10}, {11}, etc., and so on. Thus, the value of the byte at row x, column y is {xy}.
2. Map each byte in the S-box to its multiplicative inverse in the finite field GF (2^8); the value {00} is mapped to itself.
3. Consider that each byte in the S-box consists of 8 bits labeled (b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0). Apply the following transformation to each bit of each byte in the S-box:

$$b_i' = b_i \oplus b_{(i+4)\text{mod}8} \oplus b_{(i+5)\text{mod}8} \oplus b_{(i+6)\text{mod}8} \oplus b_{(i+7)\text{mod}8} \oplus c_i$$

   Where c_i is the i-th bit of byte c with the value {63}; that is, ($c_7c_6c_5c_4c_3c_2c_1c_0$) = (01100011). The prime (') indicates that the variable is to be updated by the value on the right.

5.6).Briefly describe Sub Bytes.

Each individual byte of State is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value. These row and column values serve as indexes into the S-box to select a unique 8-bit output value.

5.7).Briefly describe Shift Rows.

The first row of State is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2-byte circular left shift is performed. For the third row, a 3-byte circular left shift is performed.

5.8).How many bytes in State are affected by Shift Rows?

- 12 bytes.

5.9).Briefly describe Mix Columns.

Mix Columns operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column.

5.10).Briefly describe AddRoundKey.

The 128 bits of State are bitwise XORed with the 128 bits of the round key.

5.11).Briefly describe the key expansion algorithm.

The AES key expansion algorithm takes as input a 4-word (16-byte) key and produces a linear array of 44 words (156 bytes). The expansion is defined by the pseudo code in AES Cipher.

5.12).What is the difference between Sub Bytes and Sub Word?

Sub Bytes operate on State, with each byte mapped into a new byte using the S-box.
Sub Word operates on an input word, with each byte mapped into a new byte using the S-box.

5.13).What is the difference between Shift Rows and Rot Word?

Shift Rows: The first row of State is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2-byte circular left shift is performed. For the third row, a 3-byte circular left shift is performed.
Rot Word: It performs a one-byte circular left shift on a word; thus it is equivalent to the operation of Shift Rows on the second row of State.

5.14).What is the difference between the AES decryption algorithm and the equivalent inverse cipher?

For the AES decryption algorithm, the sequence of transformations for decryption differs from that for encryption, although the form of the key schedules for encryption and decryption is the same. The equivalent version has the same sequence of transformations as the encryption algorithm (with transformations replaced by their inverses). To achieve this equivalence, a change in key schedule is needed.

Chapter 6
More on Symmetric Ciphers

6.1).What is triple encryption?

With triple encryption, a plaintext block is encrypted by passing it through an encryption algorithm; the result is then passed through the same encryption algorithm again; the result of the second encryption is passed through the same encryption algorithm a third time. Typically, the second stage uses the decryption algorithm rather than the encryption algorithm.

6.2).What is a meet-in-the-middle attack?

This is an attack used against a double encryption algorithm and requires a known (plaintext, cipher text) pair. In essence, the plaintext is encrypted to produce an intermediate value in the double encryption, and the cipher text is decrypted to produce an intermediation value in the double encryption. Table lookup techniques can be used in such a way to dramatically improve on a brute-force try of all pairs of keys.

6.3). How many keys are used in triple encryption?

Triple encryption can be used with three distinct keys for the three stages; alternatively, the same key can be used for the first and third stage.

6.4).Why is the middle portion of 3DES a decryption rather than an encryption?

There is no cryptographic significance to the use of decryption for the second stage. Its only advantage is that it allows users of 3DES to decrypt data encrypted by users of the older single DES by repeating the key.

6.5).Why do some block cipher modes of operation only use encryption while others use both encryption and decryption?

In some modes, the plaintext does not pass through the encryption function, but is XORed with the output of the encryption function. The math works out that for decryption in these cases, the encryption function must also be used.

Chapter 8
Introduction to Number Theory

8.1).What is a prime number?

An integer $p > 1$ is a prime number if and only if its only divisors are ± 1 and $\pm p$.

8.2).What is the meaning of the expression divides?

We say that a nonzero b divides a if $a = mb$ for some m, where a, b, and m are integers.

8.3).What is Euler’s totient function?

Euler's totient function, written □ (n), is the number of positive integers less than n and relatively prime to n.

8.4).The Miller-Rabin test can determine if a number is not prime but cannot determine if a number is prime. How can such an algorithm be used to test for primality?

The algorithm takes a candidate integer n as input and returns the result "composite" if n is definitely not a prime, and the result "inconclusive" if n may or may not be a prime. If the algorithm is repeatedly applied to a number and repeatedly returns inconclusive, then the probability that the number is actually prime increases with each inconclusive test. The probability required to accept a number as prime can be set as close to 1.0 as desired by increasing the number of tests made.

8.5).What is a primitive root of a number?

If r and n are relatively prime integers with $n > 0$. and if □(n) is the least positive exponent m such that a^m □ 1 mod n, then r is called a primitive root modulo n.

8.6).What is the difference between an index and a discrete logarithm?

The two terms are synonymous.

Chapter 9
Public-Key Cryptography and RSA

9.1).What are the principal elements of a public-key cryptosystem?

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

9.2).What are the roles of the public and private key?

A user's private key is kept private and known only to the user. The user's public key is made available to others to use. The private key can be used to encrypt a signature that can be verified by anyone with the public key. Or the public key can be used to encrypt information that can only be decrypted by the possessor of the private key.

9.3).What are three broad categories of applications of public-key cryptosystems?

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

9.4).What requirements must a public key cryptosystems fulfil to be a secure algorithm?

1. It is computationally easy for a party B to generate a pair (public key PU_b, private key PR_b).
2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding cipher text:
$$C = E(PU_b, M)$$
3. It is computationally easy for the receiver B to decrypt the resulting cipher text 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 opponent, knowing the public key, PU_b, to determine the private key, PR_b.
5. It is computationally infeasible for an opponent, knowing the public key, PU_b, and a cipher text, C, to recover the original message, M.

9.5).What is a one-way function?

A one-way function is one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy whereas the calculation of the inverse is infeasible.

9.6).What is a trap-door one-way function?

A trap-door one-way function is easy to calculate in one direction and infeasible to calculate in the other direction unless certain additional information is known. With the additional information the inverse can be calculated in polynomial time.

9.7). Describe in general terms an efficient procedure for picking a prime number.

1. Pick an odd integer n at random (e.g., using a pseudorandom number generator).
2. Pick an integer a < n at random.
3. Perform the probabilistic primality test, such as Miller-Rabin. If n fails the test, reject the value n and go to step 1.
4. If n has passed a sufficient number of tests, accept n; otherwise, go to step 2.

Chapter 10
Other Public-Key Cryptosystems

10.1).Briefly explain Diffie-Hellman key exchange.

Two parties each create a public-key, private-key pair and communicate the public key to the other party. The keys are designed in such a way that both sides can calculate the same unique secret key based on each side's private key and the other side's public key.

10.2).What is an elliptic curve?

An elliptic curve is one that is described by cubic equations, similar to those used for calculating the circumference of an ellipse. In general, cubic equations for elliptic curves take the form

$$y^2 + axy + by= x^3 + cx^2 + dx + e$$

Where a, b, c, d, and e are real numbers and x and y take on values in the real numbers

10.3).What is the zero point of an elliptic curve?

Also called the point at infinity and designated by O. This value serves as the additive identity in elliptic-curve arithmetic.

10.4).What is the sum of three points on an elliptic curve that lie on a straight line?

If three points on an elliptic curve lie on a straight line, their sum is O.

Chapter 11
Message Authentication and Hash Functions

11.1).What characteristics are needed in a secure hash function?

1. H can be applied to a block of data of any size.
2. H produces a fixed-length output.
3. H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
4. For any given value h, it is computationally infeasible to find x such that H(x) = h. This is sometimes referred to in the literature as the one-way property.
5. For any given block x, it is computationally infeasible to find $y \neq x$ with H(y) = H(x).
6. It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).

11.2).What is the difference between weak and strong collision resistance?

Weak collision resistance:
For any given block x, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$.
Strong collision resistance:
It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$.

11.3).What is the role of a compression function in a hash function?

A typical hash function uses a compression function as a basic building block, and involves repeated application of the compression function.

11.4).What is the difference between little-endian and big-endian format?

In **little-endian format**, the least significant byte of a word is in the low-address byte position.
In **big-endian format**, the most significant byte of a word is in the low-address byte position.

11.5).What basic arithmetical and logical functions are used in SHA?

Addition modulo 2^{64} or 2^{32}, circular shift, primitive Boolean functions based on AND, OR, NOT, and XOR.

Chapter 12
Message Authentication Code

12.1).What types of attacks are addressed by message authentication?

- Masquerade
- Content modification
- Sequence modification
- Timing modification

12.2).What two levels of functionality comprise a message authentication or digital signature mechanism?

At the lower level, there must be some sort of function that produces an authenticator: a value to be used to authenticate a message. This lower-level function is then used as primitive in a higher-level authentication protocol that enables a receiver to verify the authenticity of a message.

12.3).What are some approaches to producing message authentication?

Message encryption, message authentication code, digitally signature

12.4).When a combination of symmetric encryption and an error control code is used for message authentication, in what order must the two functions be performed?

First, Error control code is used and then encryption is performed.

12.5).What is a message authentication code?

Message authentication code refers to the mechanism used to ensure that the integrity of the received message has been preserved - that the message has not been altered during transmission. It also assures the receiver that the message has originated from the intended sender and not from any intruder. Thus, a message is said to be authentic if the message has not been altered and has come from the actual sender.

12.6).What is the difference between a message authentication code and a one-way hash function?

A hash function, by itself, does not provide message authentication. A secret key must be used in some fashion with the hash function to produce authentication. A MAC, by definition, uses a secret key to calculated a code used for authentication.

12.7).In what ways can a hash value be secured so as to provide message authentication?

- The message plus concatenated hash code is encrypted using symmetric encryption.The hash code provides the structure required for authentication.
- Only the hash code is encrypted using symmetric encryption. This reduces the processing burden.
- Only the hash code is encrypted using public key encryption and the sender's private key.This provides digital signature.
- The message plus the public key-encrypted hash code may be encrypted using a symmetric secret key.
- A hash function may be used without encryption for message authentication.It assumes that two communicating parties (A and B) share a common key (s). 'A' computes the hash value over the concatenation of M and S.B knows S and therefore can re-compute M.
- The entire message plus the hash code may be encrypted.

12.8).Is it necessary to recover the secret key in order to attack a MAC algorithm?

A number of keys will produce the correct MAC and the opponent has no way of knowing which the correct key is. On an average 2(n-k) keys produce a match. Therefore attacks do not require the discovery of the key.

12.9).What changes in HMAC are required in order to replace one underlying hash function with another?

To replace a given hash function in an HMAC implementation, all that is required is to remove the existing hash function module and drop in the new module.

Chapter 13
Digital Signatures

13.1).List two disputes that can arise in the context of message authentication.

Suppose that John sends an authenticated message to Mary. The following disputes that could arise: 1. Mary may forge a different message and claim that it came from John. Mary would simply have to create message and append an authentication code using the key that John and Mary share. 2. John can deny sending the message. Because it is possible for Mary to forge a message, there is no way to prove that John did in fact send the message.

13.2).What are the properties a digital signature should have?

1. It must be able to verify the author and the date and time of the signature.
2. It must be able to authenticate the contents at the time of the signature.
3. The signature must be verifiable by third parties, to resolve disputes.

13.3).What requirements should a digital signature scheme satisfy?

1. The signature must be a bit pattern that depends on the message being signed.
2. The signature must use some information unique to the sender, to prevent both forgery and denial.
3. It must be relatively easy to produce the digital signature.
4. It must be relatively easy to recognize and verify the digital signature.
5. It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.
6. It must be practical to retain a copy of the digital signature in storage.

13.4).What is the difference between direct and arbitrated digital signature?

A **direct digital signature** involves only the communicating parties (source, destination). It is assumed that the destination knows the public key of the source. A digital signature may be formed by encrypting the entire message with the sender's private key or by encrypting a hash code of the message with the sender's private key.
An **arbitrated digital signature** operates as follows. Every signed message from a sender X to a receiver Y goes first to an arbiter A, who subjects the message and its signature to a number of tests to check its origin and content. The message is then dated and sent to Y with an indication that it has been verified to the satisfaction of the arbiter.

13.5).In what order should the signature function and the confidentiality function be applied to a message, and why?

It is important to perform the signature function first and then an outer confidentiality function. In case of dispute, some third party must view the message and its signature. If the signature is calculated on an encrypted message, then the third party also needs access to the decryption key to read the original message. However, if the signature is the inner operation, then the recipient can store the plaintext message and its signature for later use in dispute resolution.

13.6).What are some threats associated with a direct digital signature scheme?

1. The validity of the scheme depends on the security of the sender's private key. If a sender later wishes to deny sending a particular message, the sender can claim that the private key was lost or stolen and that someone else forged his or her signature.
2. Another threat is that some private key might actually be stolen from X at time T. The opponent can then send a message signed with X's signature and stamped with a time before or equal to T.

Chapter 14
Key Management & Distribution

14.1).List ways in which secret keys can be distributed to two communicating parties.

For two parties A and B, key distribution can be achieved in a number of ways, as follows:

1. A can select a key and physically deliver it to B.

2. A third party can select the key and physically deliver it to A and B.
3. If A and 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 A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B.

14.2).What is the difference between a session key and a master key?

A **session key** is a temporary encryption key used between two principals. A **master key** is a long-lasting key that is used between a key distribution center and a principal for the purpose of encoding the transmission of session keys. Typically, the master keys are distributed by noncryptographic means.

14.3).What is a nonce?

A nonce is a value that is used only once, such as a timestamp, a counter, or a random number; the minimum requirement is that it differs with each transaction.

14.4).What is a key distribution center?

A key distribution center is a system that is authorized to transmit temporary session keys to principals. Each session key is transmitted in encrypted form, using a master key that the key distribution center shares with the target principal.

14.5).What are two different uses of public-key cryptography related to key distribution?

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

14.6).List four general categories of schemes for the distribution of public keys.

- Public announcement,
- Publicly available directory,
- Public-key authority,
- Public-key certificates.

14.7).What are the essential ingredients of a public-key directory?

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, either because of the desire to replace a public key that has already been used for a large amount of data, or because the corresponding private key has been compromised in some way.
4. Periodically, the authority publishes the entire directory or updates to the directory. For example, a hard-copy version much like a telephone book could be published, or updates could be listed in a widely circulated newspaper.
5. Participants could also access the directory electronically. For this purpose, secure, authenticated communication from the authority to the participant is mandatory.

14.8).What is a public-key certificate?

A public-key certificate contains public key and other information, is created by a certificate authority, and is given to the participant with the matching private key. A participant conveys its key information to another by transmitting its certificate. Other participants can verify that the certificate was created by the authority.

14.9).What are the requirements for the use of a public-key certificate 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.

14.10). What is the purpose of the X.509 standard?

X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. The directory may serve as a repository of public-key certificates. Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority. In addition, X.509 defines alternative authentication protocols based on the use of public-key certificates.

14.11). What is a chain of certificates?

A chain of certificates consists of a sequence of certificates created by different certification authorities (CAs) in which each successive certificate is a certificate by one CA that certifies the public key of the next CA in the chain.

14.12). How is an X.509 certificate revoked?

The owner of a public-key can issue a certificate revocation list that revokes one or more certificates.

Chapter 15
User Authentication

15.1).Give examples of replay attacks.

Simple replay: The opponent simply copies a message and replays it later. **Repetition that can be logged:** An opponent can replay a time stamped message within the valid time window.
Repetition that cannot be detected: This situation could arise because the original message could have been suppressed and thus did not arrive at its destination; only the replay message arrives.
Backward replay without modification: This is a replay back to the message sender. This attack is possible if symmetric encryption is used and the sender cannot easily recognize the difference between messages sent and messages received on the basis of content.

15.2).List three general approaches to dealing with replay attacks.

1. Attach a sequence number to each message used in an authentication exchange. A new message is accepted only if its sequence number is in the proper order.
2. Party A accepts a message as fresh only if the message contains a timestamp that, in A's judgment, is close enough to A's knowledge of current time. This approach requires that clocks among the various participants be synchronized.
3. Party A, expecting a fresh message from B, first sends B a nonce (challenge) and requires that the subsequent message (response) received from B contain the correct nonce value.

15.3).What is a suppress-replay attack?

When a sender's clock is ahead of the intended recipient's clock., an opponent can intercept a message from the sender and replay it later when the timestamp in the message becomes current at the recipient's site. This replay could cause unexpected results.

15.4).What problem was Kerberos designed to address?

The problem that Kerberos addresses is this: Assume an open distributed environment in which users at workstations wish to access services on servers distributed throughout the network. We would like for servers to be able to restrict access to authorized users and to be able to authenticate requests for service. In this environment, a workstation cannot be trusted to identify its users correctly to network services.

15.5).What are three threats associated with user authentication over a network or internet?

1. A user may gain access to a particular workstation and pretend to be another user operating from that workstation.
2. A user may alter the network address of a workstation so that the requests sent from the altered workstation appear to come from the impersonated workstation.
3. A user may eavesdrop on exchanges and use a replay attack to gain entrance to a server or to disrupt operations.

15.6).List three approaches to secure user authentication in a distributed environment.

1. Rely on each individual client workstation to assure the identity of its user or users and rely on each server to enforce a security policy based on user identification (ID).
2. Require that client systems authenticate themselves to servers, but trust the client system concerning the identity of its user.
3. Require the user to prove identity for each service invoked. Also require that servers prove their identity to clients.

15.7).What four requirements were defined for Kerberos?

Secure: A network eavesdropper should not be able to obtain the necessary information to impersonate a user. More generally, Kerberos should be strong enough that a potential opponent does not find it to be the weak link. **Reliable**: For all services that rely on Kerberos for access control, lack of availability of the Kerberos service means lack of availability of the supported services. Hence, Kerberos should be highly reliable and should employ a distributed server architecture, with one system able to back up another.
Transparent: Ideally, the user should not be aware that authentication is taking place, beyond the requirement to enter a password.
Scalable: The system should be capable of supporting large numbers of clients and servers. This suggests a modular, distributed architecture.

15.8).What entities constitute a full-service Kerberos environment?

A full-service Kerberos environment consists of a Kerberos server, a number of clients, and a number of application servers.

15.9).In the context of Kerberos, What is a realm?

A realm is an environment in which: 1. The Kerberos server must have the user ID (UID) and hashed password of all participating users in its database. All users are registered with the

Kerberos server. 2. The Kerberos server must share a secret key with each server. All servers are registered with the Kerberos server.

15.10).what are the principal differences between version 4 and version 5 of Kerberos?

Version 5 overcomes some environmental shortcomings and some technical deficiencies in Version 4.

Chapter 18
Electronic Mail Security

18.1).What are the five principal services provided by PGP?

- Authentication
- Confidentiality
- Compression
- E-mail compatibility
- Segmentation.

18.2).What is the utility of a detached signature?

A detached signature is useful in several contexts. A user may wish to maintain a separate signature log of all messages sent or received. A detached signature of an executable program can detect subsequent virus infection. Finally, detached signatures can be used when more than one party must sign a document, such as a legal contract. Each person's signature is independent and therefore is applied only to the document. Otherwise, signatures would have to be nested, with the second signer signing both the document and the first signature, and so on.

18.3).Why does PGP generate a signature before applying compression?

a. It is preferable to sign an uncompressed message so that one can store only the uncompressed message together with the signature for future verification. If one signed a compressed document, then it would be necessary either to store a compressed version of the message for later verification or to recompress the message when verification is required.
b. Even if one were willing to generate dynamically a recompressed message for verification, PGP's compression algorithm presents a difficulty. The algorithm is not deterministic; various implementations of the algorithm achieve different trade-offs in running speed versus compression ratio and, as a result, produce different compressed forms. However, these different compression algorithms are interoperable because any version of the algorithm can correctly decompress the output of any other version. Applying the hash function and signature after compression would constrain all PGP implementations to the same version of the compression algorithm.

18.4).What is R64 conversion?

R64 converts a raw 8-bit binary stream to a stream of printable ASCII characters. Each group of three octets of binary data is mapped into four ASCII characters.

18.5).Why is R64 conversion useful for an e-mail application?

When PGP is used, at least part of the block to be transmitted is encrypted. If only the signature service is used, then the message digest is encrypted (with the sender's private key). If the confidentiality service is used, the message plus signature (if present) are encrypted (with a one-time symmetric key). Thus, part or all of the resulting block consists of a stream of arbitrary 8-bit octets. However, many electronic mail systems only permit the use of blocks consisting of ASCII text.

18.6).Why is the segmentation and reassembly function in PGP needed?

E-mail facilities often are restricted to a maximum message length.

18.7).How does PGP use the concept of trust?

PGP includes a facility for assigning a level of trust to individual signers and to keys.

18.8).What is RFC 822?

RFC 822 defines a format for text messages that are sent using electronic mail.

18.9).What is MIME?

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 (Simple Mail Transfer Protocol) or some other mail transfer protocol and RFC 822 for electronic mail.

18.10).What is S/MIME?

S/MIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security.

Chapter 19
IP Security

19.1).Give examples of applications of IP Security.

Secure branch office connectivity over the Internet: A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead. Secure remote access over the Internet: An end user whose system is equipped with IP security protocols can make a local call to an Internet service provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters. Establishing extranet and intranet connectivity with partners: IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism. Enhancing electronic commerce security: Even though some Web and electronic commerce applications have built-in security protocols, the use of IPSec enhances that security.

19.2).What services are provided by IPSec?

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets (a form of partial sequence integrity)
- Confidentiality (encryption)
- Limited traffic flow confidentiality

19.3).What parameters identify an SA and what parameters characterize the nature of a particular SA?

A security association is uniquely identified by three parameters:

Security Parameters Index (SPI): A bit string assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.

IP Destination Address: Currently, only unicast addresses are allowed; this is the address of the destination endpoint of the SA, which may be an end user system or a network system such as a firewall or router.

Security Protocol Identifier: This indicates whether the association is an AH or ESP security association.

A security association is normally defined by the following parameters:

Sequence Number Counter: A 32-bit value used to generate the Sequence Number field in AH or ESP headers, described in Section 16.3 (required for all implementations).

Sequence Counter Overflow: A flag indicating whether overflow of the Sequence Number Counter should generate an auditable event and prevent further transmission of packets on this SA (required for all implementations).

Anti-Replay Window: Used to determine whether an inbound AH or ESP packet is a replay, described in Section 16.3 (required for all implementations).

AH Information: Authentication algorithm, keys, key lifetimes, and related parameters being used with AH (required for AH implementations). **ESP Information:** Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP (required for ESP implementations).

Lifetime of this Security Association: A time interval or byte count after which an SA must be replaced with a new SA (and new SPI) or terminated, plus an indication of which of these actions should occur (required for all implementations).

IPSec Protocol Mode: Tunnel, transport, or wildcard (required for all implementations). These modes are discussed later in this section.

Path MTU: Any observed path maximum transmission unit (maximum size of a packet that can be transmitted without fragmentation) and aging variables (required for all implementations).

19.4).What is the difference between transport mode and tunnel mode?

Transport mode provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet. Tunnel mode provides protection to the entire IP packet.

19.5).What is replay attack?

A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence.

19.6).Why does ESP include a padding field?

1. If an encryption algorithm requires the plaintext to be a multiple of some number of bytes (e.g., the multiple of a single block for a block cipher), the Padding field is used to expand the plaintext (consisting of the Payload Data, Padding, Pad Length, and Next Header fields) to the required length. 2. The ESP format requires that the Pad Length and Next Header fields be right aligned within a 32-bit word. Equivalently, the ciphertext must be an integer multiple of 32 bits. The Padding field is used to assure this alignment.

3. Additional padding may be added to provide partial traffic flow confidentiality by concealing the actual length of the payload.

19.7).What are the basic approaches to bundling SAs?

Transport adjacency: Refers to applying more than one security protocol to the same IP packet, without invoking tunneling. This approach to combining AH and ESP allows for only one level of combination; further nesting yields no added benefit since the processing is performed at one IPSec instance: the (ultimate) destination.
Iterated tunneling: Refers to the application of multiple layers of security protocols effected through IP tunneling. This approach allows for multiple levels of nesting, since each tunnel can originate or terminate at a different IPSec site along the path.

19.8).What are the roles of the Oakley key determination protocol and ISAKMP in IPSec?

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. Oakley is the specific key exchange algorithm mandated for use with the initial version of ISAKMP.

Chapter 17
Web Security

17.1).What are the advantage of each of the three approaches shown in Figure 17.1?

The advantage of using IPSec (Figure 17.1a) is that it is transparent to end users and applications and provides a general-purpose solution. Further, IPSec includes a filtering capability so that only selected traffic need incur the overhead of IPSec processing. The advantage of using SSL is that it makes use of the reliability and flow control mechanisms of TCP. The advantage application-specific security services (Figure 17.1c) is that the service can be tailored to the specific needs of a given application.

17.2).What protocols comprise SSL?

- SSL handshake protocol
- SSL change cipher spec protocol
- SSL alert protocol
- SSL record protocol.

17.3).What is the difference between an SSL connection and an SSL session?

Connection: A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session.
Session: An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

17.4).List and briefly define the parameters that define an SSL session state.

Session identifier: An arbitrary byte sequence chosen by the server to identify an active or resumable session state.
Peer certificate: An X509.v3 certificate of the peer.
Compression method: The algorithm used to compress data prior to encryption.

Cipher spec: Specifies the bulk data encryption algorithm (such as null, DES, etc.) and a hash algorithm (such as MD5 or SHA-1) used for MAC calculation. It also defines cryptographic attributes such as the hash size.
Master secret: 48-byte secret shared between the client and server.
Is resumable: A flag indicating whether the session can be used to initiate new connections.

17.5).List and briefly define the parameters that define an SSL session connection.

Server and client random: Byte sequences that are chosen by the server and client for each connection.
Server write MAC secret: The secret key used in MAC operations on data sent by the server.
Client write MAC secret: The secret key used in MAC operations on data sent by the client.
Server write key: The conventional encryption key for data encrypted by the server and decrypted by the client.
Client write key: The conventional encryption key for data encrypted by the client and decrypted by the server.
Initialization vectors: When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key. This field is first initialized by the SSL Handshake Protocol. Thereafter the final cipher text block from each record is preserved for use as the IV with the following record.
Sequence numbers: Each party maintains separate sequence numbers for transmitted and received messages for each connection. When a party sends or receives a change cipher spec message, the appropriate sequence number is set to zero. Sequence numbers may not exceed $2^{64} – 1$.

17.6).What services are provided by the SSL Record protocol?

Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.
Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

17.7).What steps are involved in the SSL record protocol transmission?

- Fragmentation
- Compression
- Add MAC
- Encrypt
- Append SSL record header.

17.8).List and briefly define the principal categories of SET participants.

Cardholder: In the electronic environment, consumers and corporate purchasers interact with merchants from personal computers over the Internet. A cardholder is an authorized holder of a payment card (e.g., MasterCard, Visa) that has been issued by an issuer.
Merchant: A merchant is a person or organization that has goods or services to sell to the cardholder. Typically, these goods and services are offered via a Web site or by electronic mail. A merchant that accepts payment cards must have a relationship with an acquirer.
Issuer: This is a financial institution, such as a bank, that provides the cardholder with the payment card. Typically, accounts are applied for and opened by mail or in person. Ultimately, it is the issuer that is responsible for the payment of the debt of the cardholder.
Acquirer: This is a financial institution that establishes an account with a merchant and processes payment card authorizations and payments. Merchants will usually accept more than one credit card brand but do not want to deal with multiple bankcard associations or with multiple individual issuers. The acquirer provides authorization to the merchant that a given

card accounts is active and that the proposed purchase does not exceed the credit limit. The acquirer also provides electronic transfer of payments to the merchant's account. Subsequently, the acquirer is reimbursed by the issuer over some sort of payment network for electronic funds transfer.

Payment gateway: This is a function operated by the acquirer or a designated third party that processes merchant payment messages. The payment gateway interfaces between SET and the existing bankcard payment networks for authorization and payment functions. The merchant exchanges SET messages with the payment gateway over the Internet, while the payment gateway has some direct or network connection to the acquirer's financial processing system.

Certification authority (CA): This is an entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways. The success of SET will depend on the existence of a CA infrastructure available for this purpose. As was discussed in previous chapters, a hierarchy of CAs is used, so that participants need not be directly certified by a root authority.

17.9).What is a dual signature and what is its purpose?

A dual signature is used to sign two concatenated documents each with its own hash code. The purpose of the dual signature is to link two messages that are intended for two different recipients. In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank. The merchant does not need to know the customer's credit card number, and the bank does not need to know the details of the customer's order.

Chapter 20
Intruders

20.1).List and briefly define three classes of intruders.

Masquerader: An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.

Misfeasor: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.

Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

20.2).What are two common techniques used to protect a password file?

One-way encryption: The system stores only an encrypted form of the user's password. When the user presents a password, the system encrypts that password and compares it with the stored value. In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the encryption function and in which a fixed-length output is produced.

Access control: Access to the password file is limited to one or a very few accounts.

20.3).What are three benefits that can be provided by an intrusion detection system?

1. If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to pre-empt the intruder, the sooner that the intrusion is detected, the less the amount of damage and the more quickly that recovery can be achieved.
2. An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions.
3. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

20.4).What is the difference between statistical anomaly detection and rule-based intrusion detection?

Statistical anomaly detection involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.
Rule-Based Detection involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

20.5).What metrics are useful for profile-based intrusion detection?

Counter: A nonnegative integer that may be incremented but not decremented until it is reset by management action. Typically, a count of certain event types is kept over a particular period of time.
Gauge: A nonnegative integer that may be incremented or decremented. Typically, a gauge is used to measure the current value of some entity. **Interval timer:** The length of time between two related events.
Resource utilization: Quantity of resources consumed during a specified period.

20.6).What is the difference between rule-based anomaly detection and rule-based penetration identification?

With **rule-based anomaly detection**, historical audit records are analysed to identify usage patterns and to generate automatically rules that describe those patterns. Rules may represent past behavior patterns of users, programs, privileges, time slots, terminals, and so on. Current behavior is then observed, and each transaction is matched against the set of rules to determine if it conforms to any historically observed pattern of behavior. **Rule-based penetration identification** uses rules for identifying known penetrations or penetrations that would exploit known weaknesses. Rules can also be defined that identify suspicious behavior, even when the behavior is within the bounds of established patterns of usage. Typically, the rules used in these systems are specific to the machine and operating system. Also, such rules are generated by "experts" rather than by means of an automated analysis of audit records.

20.7).What is a honeypot?

Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.

20.8).What is a salt in the context of UNIX password management?

The salt is combined with the password at the input to the one-way encryption routine.

20.9).List and briefly define four techniques used to avoid guessable passwords.

User education: Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords.
Computer-generated passwords: Users are provided passwords generated by a computer algorithm.
Reactive password checking: the system periodically runs its own password cracker to find guessable passwords. The system cancels any passwords that are guessed and notifies the user.

Proactive password checking: a user is allowed to select his or her own password. However, at the time of selection, the system checks to see if the password is allowable and, if not, rejects it.

Chapter 21
Malicious Software

21.1).What is the role of compression in the operation of a virus?

A virus may use compression so that the infected program is exactly the same length as an uninfected version.

21.2).What is the role of encryption in the operation of a virus?

A portion of the virus, generally called a mutation engine, creates a random encryption key to encrypt the remainder of the virus. The key is stored with the virus, and the mutation engine itself is altered. When an infected program is invoked, the virus uses the stored random key to decrypt the virus. When the virus replicates, a different random key is selected.

21.3).What are typical phases of operation of a virus or worm?

- A dormant phase
- A propagation phase
- A triggering phase
- An execution phase.

21.4).In general terms, how does a worm propagate?

1. Search for other systems to infect by examining host tables or similar repositories of remote system addresses.
2. Establish a connection with a remote system.
3. Copy itself to the remote system and cause the copy to be run.

21.5).What is a digital immune system?

This system provides a general-purpose emulation and virus-detection system. The objective is to provide rapid response time so that viruses can be stamped out almost as soon as they are introduced. When a new virus enters an organization, the immune system automatically captures it, analyses it, adds detection and shielding for it, removes it, and passes information about that virus to systems running a general antivirus program so that it can be detected before it is allowed to run elsewhere.

21.6).How does behavior-blocking software work?

Behavior-blocking software integrates with the operating system of a host computer and monitors program behavior in real-time for malicious actions. The behavior blocking software then blocks potentially malicious actions before they have a chance to affect the system.

21.7).What is DDoS?

A denial of service (DoS) attack is an attempt to prevent legitimate users of a service from using that service. When this attack comes from a single host or network node, then it is simply referred to as a DoS attack. A more serious threat is posed by a DDoS attack. In a DDoS attack, an attacker is able to recruit a number of hosts throughout the Internet to simultaneously or in a coordinated fashion launch an attack upon the target.

Chapter 22
Firewalls

22.1).List three design goals for a firewall.

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible, as explained later in this section.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies, as explained later in this section.
3. The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

22.2).List four techniques used by firewalls to control access and enforce a security policy.

Service control: Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address and TCP port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.
Direction control: Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.
User control: Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology, such as is provided in IPSec.
Behavior control: Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

22.3).What information is used by a typical packet-filtering router?

Source IP address: The IP address of the system that originated the IP packet.
Destination IP address: The IP address of the system the IP packet is trying to reach.
Source and destination transport-level address: The transport level (e.g., TCP or UDP) port number, which defines applications such as SNMP or TELNET. IP protocol field: Defines the transport protocol.
Interface: For a router with three or more ports, which interface of the router the packet came from or which interface of the router the packet is destined for.

22.4).What are some weakness of a packet-filtering router?

1. Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions. For example, a packet filter firewall cannot block specific application commands; if a packet filter firewall allows a given application, all functions available within that application will be permitted.
2. Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited. Packet filter logs normally contain the same information used to make access control decisions (source address, destination address, and traffic type).
3. Most packet filter firewalls do not support advanced user authentication schemes. Once again, this limitation is mostly due to the lack of upper-layer functionality by the firewall.
4. They are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing. Many packet filter firewalls cannot detect a network packet in which the OSI Layer 3

addressing information has been altered. Spoofing attacks are generally employed by intruders to bypass the security controls implemented in a firewall platform.

5. Finally, due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations.

22.5).what is the difference between a packet-filtering router and a stateful inspection firewall?

A **traditional packet filter** makes filtering decisions on an individual packet basis and does not take into consideration any higher layer context. A **stateful inspection packet filter** tightens up the rules for TCP traffic by creating a directory of outbound TCP connections, as shown in Table 22.2. There is an entry for each currently established connection. The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.

22.6).What is an application-level gateway?

An application-level gateway, also called a proxy server, acts as a relay of application-level traffic.

22.7).What is a circuit-level gateway?

A circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.

22.8).What are the differences among the three configuration of Figure 22.2?

The **screened host firewall, single-homed bastion** configuration (Figure 22.2a), the firewall consists of two systems: a packet-filtering router and a bastion host; the latter performs authentication and proxy functions. In the single-homed configuration just described, if the packet-filtering router is completely compromised, traffic could flow directly through the router between the Internet and other hosts on the private network.

The **screened host firewall, dual-homed bastion** configuration physically prevents such a security breach.

In the **screened subnet firewall** configuration, two packet-filtering routers are used, one between the bastion host and the Internet and one between the bastion host and the internal network. This configuration creates an isolated sub network, which may consist of simply the bastion host but may also include one or more information servers and modems for dial-in capability.

22.9).In the context of access control, what is the difference between a subject and an object?

A **subject** is an entity capable of accessing objects. Generally, the concept of subject equates with that of process. Any user or application actually gains access to an object by means of a process that represents that user or application.

An **object** is anything to which access is controlled. Examples include files, portions of files, programs, and segments of memory.

22.10).What is the difference between an access control list and a capability ticket?

For each object, an **access control list** lists users and their permitted access rights.
A **capability ticket** specifies authorized objects and operations for a user.

22.11).What are the two rules that a reference monitor enforces?

No read up: A subject can only read an object of less or equal security level.
No write down: A subject can only write into an object of greater or equal security level.

22.12).What properties are required of a reference monitor?

Complete mediation: The security rules are enforced on every access, not just, for example, when a file is opened.
Isolation: The reference monitor and database are protected from unauthorized modification.
Verifiability: The reference monitor's correctness must be provable. That is, it must be possible to demonstrate mathematically that the reference monitor enforces the security rules and provides complete mediation and isolation.

22.13).What are the common criteria?

The Common Criteria (CC) for Information Technology and Security Evaluation is an international initiative by standards bodies in a number of countries to develop international standards for specifying security requirements and defining evaluation criteria.