UNIT-I

1. What is cryptology?

Cryptology is the study of cryptography and cryptanalysis.

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

- An unconditionally secure cipher is a scheme such that if the cipher text generated by the scheme does not contain enough information to determine uniquely the corresponding plain text, no matter how much cipher text is available.
- A computationally secure scheme is such that the cost of breaking the cipher exceeds the value of the encrypted information and the time required to break the cipher exceeds the useful lifetime of the information.

3. Briefly define the Caesar cipher.

The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example:
Plain: meet me after the toga party
Cipher: PHHW PH DIWHU WKH WRJD SDUWB

4. Briefly define the monoalphabetic cipher?

A monoalphabetic cipher maps from a plain alphabet to cipher alphabet. Here a single cipher alphabet is used per message.

5. Briefly define the playfair cipher.

The best-known multiple-letter encryption cipher is the playfair, which treats diagrams in the plain text as single units and translates these units into cipher text diagrams.

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

1.It makes the problem of making large quantities of random keys.
2.It also makes the problem of key distribution and protection.

7. What is a transposition cipher?

Transposition cipher is a cipher, which is achieved by performing some sort of permutation on the plaintext letters.

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

The two basic functions used in encryption algorithms are

- Substitution
- Transposition

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

If both sender and receiver use the same key, the system is referred to as symmetric, single key, secret key, or conventional encryption. If the sender and receiver each use a different key, the system is referred to as asymmetric, two-key, or public-key encryption.

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

A block cipher processes the input one block of elements at a time, producing an output block for each input block.
A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

11. What are the two approaches to attacking a cipher?
The two approaches to attack a cipher are:
- ❖ Cryptanalysis
- ❖ Brute-force attack

12. What is Steganography?
This conceals the existence of the message.

13. Why is it important to study feistel cipher?
This cipher can be used to approximate the simple substitution cipher by utilizing the concept of a product cipher, which is the performing of two or more basic ciphers in sequence in such a way that the final result or product is cryptographically stronger than any of the component ciphers.

14. Why is it not practical to use an arbitrary reversible substitution cipher?
An arbitrary reversible cipher for a large block size is not practical, however, from an implementation and performance point of view. Here the mapping itself is the key.

15. What is the difference between diffusion and confusion?
In diffusion, the statistical structure of the plain text is dissipated into long-range statistics of the cipher text. This is achieved by permutation.
In confusion, the relationship between the statistics of the cipher text and the value of the encryption key is made complex. It is achieved by substitution.

16. Which parameters and design choices determine the actual algorithm of a feistel cipher?
- ➢ Block size
- ➢ Key size
- ➢ Number of rounds
- ➢ Sub key generation algorithm
- ➢ Round functions
- ➢ Fast software encryption or decryption
- ➢ Ease of analysis

17. What is the purpose of the S-boxes in DES?
Each row of a S-box defines a general reversible substitution. It consists of a set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.

18. Explain the avalanche effect.
It is that a small change in either the plaintext or the key should produce a significant change in the cipher text.

A change in one of the bit of the plaintext or one bit of the key should produce a change in many bits of the cipher text.

19. What is the difference between a mono alphabetic cipher and a poly alphabetic cipher?
Mono alphabetic cipher: Here a single cipher alphabet is used.
Poly alphabetic cipher: Here a set of related mono alphabetic substitution rules is used.

20. List the types of cryptanalytic attacks.
Cipher text only
Known plaintext
Chosen plaintext
Chosen cipher text
Chosen text

21. What are the essential ingredients of a symmetric cipher?
A symmetric cipher encryption has five ingredients. They are:
- Plaintext
- Encryption algorithm
- Secret key
- Cipher text
- Decryption algorithm

UNIT II

1. What is the purpose of the State array?
A single 128-bit block is depicted as a square matrix of bytes. This block is copied into the State array, which is modified at each stage of encryption or decryption. After the final stage, State is copied to an output matrix.

2. How is the S-box constructed?
The S-box is constructed in the following fashion:
Initialize the S-box with the byte values in ascending sequence row by row. The first row contains {00}, {01}, {02}, ……., {0F}; the second row contains {10},{11},etc; and so on. Thus, the value of the byte at row x, column y is {x y}.
Map each byte in the S-box to its multiplicative inverse in the finite field GF (28); the value {00} is mapped to itself.
Consider that each byte in the S-box consists of 8 bits labeled (b7,b6,b5,b4,b3,b2,b1,b0).Apply the following transformation to each bit of each byte in the S-box.

3. Briefly describe Sub Bytes.
Sub byte uses an S-box to perform a byte-by-byte substitution of the block. The left most 4 bits of the byte are used as 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 value.

4. What is the difference between differential and linear cryptanalysis?
In differential cryptanalysis, it breaks the DES in less 2^{55} complexities.
In cryptanalysis, it finds the DES key given 2^{47} plaintexts.

5. Define product cipher.
Product cipher performs two or more basic ciphers in sequence in such a way that the final result or product is cryptologically stronger than any of the component ciphers.

6. What was the original set of criteria used by NIST to evaluate candidate AES cipher?
The original set of criteria used by NIST to evaluate candidate AES cipher was:

- 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

7. What was the final set of criteria used by NIST to evaluate candidate AES ciphers?
The final set of criteria used by NIST to evaluate candidate AES ciphers was:
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

8. What is power analysis?
Power analysis is the power consumed by the smart card at any particular time during the cryptographic operation is related to the instruction being executed and to the data being processed.
Eg) Multiplication consumes more power than addition and writing 1s consumes ore power than writing 0s.

9. Briefly describe Shift Rows.
In shift row, a row shift moves an individual byte from one column to another, which is a linear distance of a multiple of 4 bytes. In Forward Shift Row, each row perform circular left shift. Second Row a 1-byte circular left shift is performed. Third Row a 2-byte circular left shift is performed. For the Fourth Row a 3-byte circular left shift is

performed. In Inverse Shift Row, each row perform circular right shift.

10. How many bytes in State are affected by Shift Rows?
Totally 6-bytes in state are affected by Shift Rows.

11. Briefly describe Mix Columns.
Mix Column is substitution that makes use of arithmetic over GF(28).Mix Column 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 the column. The Mix Column Transformation combined with the shift row transformation ensures that after a few rounds, all output bits depend on all input bits.

12. Briefly describe Add Round Key.
In Add Round Key, the 128 bits of State are bit wise XORed with the 128 bits of the round key. The operation is viewed as a column wise operation between the 4 bytes of a State column and one word of the round key; it can also be viewed as a byte-level operation. The Add Round Key transformation is as simple as possible and affects every bit of State.

13. 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). This is sufficient to provide a 4-word round key for the initial Add Round Key stage and each of the 10 rounds of the cipher.

14. What is the difference between Sub Bytes and Sub Word?
Sub Bytes:
Sub Bytes uses an S-box to perform a byte-by-byte substitution of the block.
Sub Word:
Sub Word performs a byte substitution on each byte of its input word,using the Sbox.

15. What is the difference between Shift Rows and Rot Word?
Shift Rows:
Shift Row is simple permutation. It shifts the rows circularly left or right.
Rot Word:Rot word performs a one-byte circular left shift on a word. This means that an input word [b0,b1,b2,b3] is transformed into [b1,b2,b3,b0].

16. What is triple encryption?
Tuchman proposed a triple encryption method that uses only two keys [TUCH79].
The function follows an encrypt – decrypt – encrypt (EDE) sequence.
$C=E_{k1}[D_{k2}[E_{k1}[P]]]$
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:
$C=E_{k1}[D_{k2}[E_{k1}[P]]] = E_{k1}[P]$

17. What is a meet-in-the-middle attack?
Meet-in-the-middle attack, was first described in [DIFF77]. It is based on the

observation that, if we have
$C=E_{k2}[E_{k1}[P]]$
Then
$X=E_{k1}[P]=D_{k2}[C]$
Given a known pair, (P,C), the attack proceeds as follows. First, encrypt P for all 2^{56} possible values of K_1. Store these results in a table and then sort the table by the values of X. Next, decrypt C using all 2^{56} possible values of K_2. As each decryption is produced, check the result against the table for a match. If a match occurs, then test the two resulting keys against a new known plaintext-ciphertext pair. If the two keys produce the correct ciphertext, accept them as the correct keys.

18. How many keys are used in triple encryption?
Tuchman proposed a triple encryption method that uses only two keys [TUCH79].

19. What is the key size for Blowfish?
Blowfish makes use of a key that ranges from 32 bits to 448 bits (one to fourteen 32-bit words). That key is used to generate 18 32-bit subkeys and four 8*32 S-boxes containing a total of 1024 32-bit entries. The total is 1042 32-bit values, or 4168 bytes.

20. Why do some block cipher modes of operation only use encryption while others use both encryption and decryption?
Some block cipher modes of operation only use encryption because the input is set to some initialization vector and the leftmost bits of the output of the encryption function are XORed with the first segment of plain text p1 to produce the first unit of cipher text C1 and it is transmitted. While in decryption, the cipher text is XORed with the output of the encryption function to produce the plain text.

UNIT III

1. List important design considerations for a stream cipher.
The encyption sequence should have a large period. The keystream should approximate the properties of a true random number stream as close as possible. The output of the pseudorandom number generator is conditioned on the value of the input key.

2. Why is it not desirable to reuse a stream cipher key?
If two plaintexts are encrypted with the same key using a stream cipher then cryptanalysis is often quite simple. If the two ciphertext streams are XORed together the result is the XOR of the original plaintexts. So it is not desirable to reuse a stream cipher key.

3. What primitive operations are used in Blowfish?
Blowfish uses two primitive operations:
- **Addition:** Addition of words, denoted by +, is performed modulo 2^{32}.

• **Bit wise exclusive-OR:** This operation is denoted by ⊕.

4. What common mathematical constants are used in RC5?
*W :*Word size in bits. RC5 encrypts 2-word
blocks.
16,32,64
r: Number of rounds. 0,1,….,255
B Number of 8-bit bytes (octets) in the secret
key K.
0,1,….,255

5. What primitive operations are used in RC5?
RC5 uses three primitive operations (and their inverse):
• **Addition:** Addition of words, denoted by +, is performed modulo 2^w. The inverse operation, denoted by -, is subtraction modulo 2^w.
• **Bitwise exclusive-OR:** This operation is denoted by "⊕".
• **Left cicular rotation:** The cyclic rotation of word x left by y bits is denoted by x<<<y. The inverse is the right circular rotation of word x by y bits, denoted by x>>>y.

6. What primitive operation is used in RC4?
The primitive operation used in RC4 is bit wise Exclusive-OR (XOR) operation.

7. For a user workstations in a typical business environment, list potential locations for confidentiality attacks.
• LANs in the same building that are interconnected with bridges and routers.
• The wiring closet itself is vulnerable.
• Twisted pair and coaxial cable can be attacked using either invasive taps or inductive devices that monitor electromagnetic emanation.
• In addition to the potential vulnerability of the various communications links, the various processors along the path are themselves subject to attack.

8. What is the difference between link and end-to-end encryption?

Link Encryption	End-to-end Encryption
Applied by sending host	Applied by sending process
Transparent to user	User applies encryption
Host maintains encryption facility	User must determine algorithm
One facility for all users	User selects encryption scheme
Can be done in hardware	Software implementation
All or no messages encrypted	User chooses to encrypt, or not, for each message

9. What types of information might be derived from a traffic analysis attack?
The following types of information can be derived from traffic analysis attack:

- Identities of partners
- How frequently the partners are communicating
- Message pattern, message length, or quantity of messages that suggest important information is being exchanged
- The events that correlate with special conversations between particular partners.

10. What is traffic padding and what is its purpose?

Traffic padding produces ciphertext output continuously, even in the absence of plaintext. A continuous random data stream is generated. When plaintext is available, it is encrypted and transmitted. When input plaintext is not present, random data are encrypted and transmitted.

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

- A can select a key and physically deliver it to B.
- A third party can select the key and physically deliver it o A and B
- 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
- 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

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

Session key	Master key
Communication between end systems is encrypted using temporary key, often referred to as a session key.	Session keys are transmitted in encrypted form, using master key that is shared by the keys distribution center and an end system.
The session key is used for the duration of a logical connection, such as a frame relay connection or transport connection, and then discarded.	For each end system or user, there is a unique master key that it shares with the key distribution center. These master keys must be distributed in some fashion.

13. What is nonce?

Consider A issues a request to the KDC for a session key to protect a logical connection to B. The message includes the identity of A and B and a unique identifier, N_1, for this transaction, which we refer to as nonce. The nonce may be a timestamp, a counter, or a random number.

14. What is key distribution center?

A key distribution center is responsible for distributing keys to pairs of users such as hosts, processes, applications. Each user must share a unique key with the key distribution center for purposes of key distribution.

15. What is the difference between statistical randomness and unpredictability?

In applications such as reciprocal authentication and session key generation the requirement is not so much that the sequence of numbers be statistically random but that the successive numbers of the sequence are unpredictable. With true random sequences each number is statistically independent of other numbers in the sequence and therefore unpredictable.

16. What is the difference between Rijndael and AES?

AES was developed by NIST .AES is a symmetric block cipher that is intended to replace DES.NIST selected rijndael as the proposed AES algorithm. The two researchers who developed and submitted Rijndael for the AES are the both cryptographers from Belgium.

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

Decryption requires that the keys be applied in reverse order:

$P=D_{k1}[E_{k1}[P]]$

This results in a dramatic increase in cryptographic strength.The use of DES results in a mapping that is not equivalent to a single DES encryption.

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

In AES decryption, we use inverse shift rows inverse sub bytes, add round key, inverse mix columns. But in equivalent inverse cipher, we interchange inverse shift rows and inverse sub bytes.

19. State fermat' s theorem.

For a prime number p and appositive integer a

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

Unit IV

1. Differentiate public key encryption and conventional encryption.

Conventional Encryption	Public key Encryption
1. Same algorithm with same key used for encryption and decryption.	1.Same algorithm is used for encryption & decryption with a pair of keys.
2. Sender & receiver must share the algorithm and key.	2.Sender & receiver have one of the matched pair keys.
3. Key must be kept secret.	3. Any one of the key must be kept secret.

2. Specify the application of public key cryptography.

- Encryption/Decryption.
- Digital signature.
- Key exchange.

3. Determine the gcd(24140,16762) using Euclid's algorithm.

Soln:

We know, gcd(a,b)=gcd(b,a mod b)

gcd(24140,16762)=gcd(16762,7378)

gcd(7378,2006)=gcd(2006,1360)

gcd(1360,646)=gcd(646,68)
gcd(68,34)=34
gcd(24140,16762) = 34.

4.Perform encryption and decryption using RSA alg. For the following.
P=7; q=11; e=17; M=8.

Soln:
n=pq
n=7*11=77
ö(n)=(p-1) (q-1)
=6*10 = 60
e=17
d =27
C= Me mod n
C = 817 mod 77
= 57
M = Cd mod n
= 5727 mod 77
= 8

5. User A & B exchange the key using Diffie Hellman alg. Assume
á=5 q=11 XA=2 XB=3. Find YA, YB, K.

Soln:
YA = áXA mod q
=52 mod 11
= 3
YB = áXB mod q
= 53 mod 11
= 4
KA = YBXA mod q
= 42 mod 11
= 5
KB = YAXB mod q
= 33 mod 11
= 5

6.What is message authentication?

It is a procedure that verifies whether the received message comes from assigned source has not been altered.

7. Define the classes of message authentication function.

- Message encryption: The entire cipher text would be used for authentication.
- Message Authentication Code: It is a function of message and secret key produce a fixed length value.
- Hash function: Some function that map a message of any length to fixed length which serves as authentication.

8. What you meant by MAC?
MAC is Message Authentication Code. It is a function of message and secret key which produce a fixed length value called as MAC.

9. Specify the techniques for distribution of public key.
- Public announcement.
- Publicly available directory.
- Public key authority.
- Public key certificate.

10. Specify the requirements for message authentication.
i. Disclosure.
ii. Traffic analysis.
iii. Masquerade.
iv. Content Modification.
v. Sequence Modification.
vi. Timing modification.
vii. Repudiation.

11. Differentiate internal and external error control.
Internal error control:
In internal error control, an error detecting code also known as frame check sequence or checksum.
External error control:
In external error control, error detecting codes are appended after encryption.

12. What you meant by hash function?
Hash function accept a variable size message M as input and produces a fixed size hash code H(M) called as message digest as output. It is the variation on the message authentication code.

13. Differentiate MAC and Hash function?
MAC: In Message Authentication Code, the secret key shared by sender and receiver. The MAC is appended to the message at the source at a time which the message is assumed or known to be correct.
Hash Function: The hash value is appended to the message at the source at time when the message is assumed or known to be correct. The hash function itself not considered to be secret.

14.Define Kerberos.
Kerberos is an authentication service developed as part of project Athena at MIT.The problem that Kerberos address is, assume an open distributed environment in which users at work stations wish to access services on servers distributed throughout the network.

15.In the content of Kerberos, what is realm?

A full service Kerberos environment consisting of a Kerberos server, a no. of clients, no.of application server requires the following:

- The Kerberos server must have user ID and hashed password of all participating users in its database.
- The Kerberos server must share a secret key with each server. Such an environment is referred to as "Realm".

17.Assume the client C wants to communicate server S using Kerberos procedure. How can it be achieved?

a) C → AS: [IDC|| PC || IDV]
b) AS → C: Ticket
c) C → V: [IDC || ADC || IDV]
Ticket = EKV [IDC ||ADC || IDV]

18. Any three hash algorithm.

- MD5 (Message Digest version 5) algorithm.
- SHA_1 (Secure Hash Algorithm).
- RIPEMD_160 algorithm.

19. Specify the four categories of security threats

- Interruption
- Interception
- Modification
- Fabrication

20. Differentiate symmetric and Asymmetric Encryption

Symmetric Encryption
Sender and receiver use the same key.
Asymmetric
Sender and receiver uses different key.

Unit V

1. What are the services provided by PGP services

- Digital signature
- Message encryption
- Compression
- E-mail compatibility
- Segmentation

2. Explain the reasons for using PGP?

a) It is available free worldwide in versions that run on a variety of platforms, including DOS/windows, UNIX, Macintosh and many more.
b) It is based on algorithms that have survived extensive public review and are considered extremely secure.

E.g.) RSA, DSS and Diffie-Hellman for public key encryption, CAST-128, IDEA, 3DES for conventional encryption, SHA-1for hash coding.
c) It has a wide range of applicability from corporations that wish to select and enforce a standardized scheme for encrypting files and communication.
d) It was not developed by nor is it controlled by any governmental or standards organization.

3. Why E-mail compatibility function in PGP needed?

Electronic mail systems only permit the use of blocks consisting of ASCII text. To accommodate this restriction PGP provides the service converting the row 8-bit binary stream to a stream of printable ASCII characters. The scheme used for this purpose is Radix-64 conversion.

4. Name any cryptographic keys used in PGP?

a) One-time session conventional keys.
b) Public keys.
c) Private keys.
d) Pass phrase based conventional keys.

5. Define key Identifier?

PGP assigns a key ID to each public key that is very high probability unique with a user ID. It is also required for the PGP digital signature. The key ID associated with each public key consists of its least significant 64bits.

6. List the limitations of SMTP/RFC 822?

a) SMTP cannot transmit executable files or binary objects.
b) It cannot transmit text data containing national language characters.
c) SMTP servers may reject mail message over certain size.
d) SMTP gateways cause problems while transmitting ASCII and EBCDIC.
e) SMTP gateways to X.400 E-mail network cannot handle non textual data included in X.400 messages.

7. Define S/MIME?

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

8. What are the elements of MIME?

- ✓ Five new message header fields are defined which may be included in an RFC 822 header.
- ✓ A number of content formats are defined.
- ✓ Transfer encodings are defined that enable the conversion of any content format into a form that is protected from alteration by the mail system.

9. What are the headers fields define in MME?

- MIME version.
- Content type.

- Content transfer encoding.
- Content id.
- Content description.

10. What is MIME content type &explain?

It is used to declare general type of data. Subtype define particular format for that type of the data. It has 7 content type & 15 subtypes. They are,

1. Text type
- Plain text.
- Enriched.

2. Multipart type
- Multipart/mixed.
- Multipart/parallel.
- Multipart/alternative.
- Multipart/digest.

3. Message type
- Message/RFC822.
- Message/partial.
- Message/external.

4. Image type
- JPEG.
- CIF.

5. Video type.

6. Audio type.

7. Application type
- Post script.
- Octet stream.

11.What are the key algorithms used in S/MIME?
- Digital signature standards.
- Diffi Hellman.
- RSA algorithm.

12. Give the steps for preparing envelope data MIME?
- Generate K_s.
- Encrypt K_s using recipient's public key.
- RSA algorithm used for encryption.
- Prepare the 'recipient info block'.
- Encrypt the message using K_s.

13. What you mean by versioned certificate?

Mostly used issue X.509 certificate with the product name" versioned digital id". Each digital id contains owner's public key, owner's name and serial number of the digital id.

14. What are the function areas of IP security?
- Authentication
- Confidentiality
- Key management.

15. Give the application of IP security?
- Provide secure communication across private & public LAN.
- Secure remote access over the Internet.
- Secure communication to other organization.

16. Give the benefits of IP security?

- Provide security when IP security implement in router or firewall.
- IP security is below the transport layer is transparent to the application.
- IP security transparent to end-user.
- IP security can provide security for individual user.

17. What are the protocols used to provide IP security?

- Authentication header (AH) protocol.
- Encapsulating Security Payload(ESP).

18. Specify the IP security services?

- Access control.
- Connectionless interpretty.
- Data origin authentication
- Rejection of replayed packet.
- Confidentiality.
- Limited traffic for Confidentiality.

19. What do you mean by Security Association? Specify the parameters that identifies the Security Association?

- An association is a one-way relationship between a sender and receiver that affords security services to the traffic carried on.
- A key concept that appears in both the authentication and confidentiality mechanism for ip is the security association (SA).

A security Association is uniquely identified by 3 parameters:

- Security Parameter Index (SPI).
- IP Destination Address.
- Security Protocol Identifier.

20. What does you mean by Reply 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.
- Each time a packet is send the sequence number is incremented .

21. Explain man in the middle attack?

If A and B exchange message, means E intercept the message and receive the B's public key and b's userId,E sends its own message with its own public key and b's userID based on the private key and Y.B compute the secret key and A compute k2 based on private key of A and Y

22. Steps involved in SS L required protocol?

1. SSL record protocol takes application data as input and fragments it.
2. Apply lossless Compression algorithm.
3. Compute MAC for compressed data.

4. MAC and compression message is encrypted using conventional alg.

23. What is mean by SET? What are the features of SET?
Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transaction on the internet.
Features are:
1. Confidentiality of information
2. Integrity of data
3. Cardholder account authentication
4. Merchant authentication

24. What are the steps involved in SET Transaction?
1. The customer opens an account
2. The customer receives a certificate
3. Merchants have their own certificate
4. The customer places an order.
5. The merchant is verified.
6. The order and payment are sent.
7. The merchant requests payment authorization.
8. The merchant confirm the order.
9. The merchant provides the goods or services.
10. The merchant requests payment.

25. What is dual signature? What it is purpose?
The purpose of the dual signature is to link two messages that intended for two different recipients.
To avoid misplacement of orders

26. List the 3 classes of intruder?
Classes of Intruders
1) Masquerader
2) Misfeasor
3) Clandestine user

27. Define virus. Specify the types of viruses?
A virus is a program that can infect other program by modifying them the modification includes a copy of the virus program, which can then go on to infect other program.
Types:
1) Parasitic virus
2) Memory-resident virus
3) Boot sector virus
4) Stealth virus
5) Polymorphic virus

28. What is application level gateway?
An application level gateway also called a proxy server; act as a relay of

application-level traffic. The user contacts the gateway using a TCP\IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.

29. List the design goals of firewalls?

1. All traffic from inside to outside, and vise versa, must pass through the firewall.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass.
3. The firewall itself is immune to penetration.

UNIT 1

1.Explain the OSI Architecture.

- Notes
- Diagram
- Illustration

2.Explain Classical Encryption Techniques.

- ❖ Symmetric Ciphers
- ❖ Caesar Cipher
- ❖ Mono alphabetic
- ❖ Poly alphabetic

3.Explain DES Algorithm.

- Notes
- Diagram
- Illustration
- Algorithm

4.Explain AES.

- Notes
- Diagram
- Illustration
- Algorithm

5.Describe about Traffic Confidentiality.

Cryptanalytic methods in traffic analysis and ciphers achieving confidentiality.

UNIT 2

1.Explain about the various Key management techniques.

- public announcement
- Publicly available directory
- public-key authority
- public-key certificates

2.Describe Diffie-Hellman Key Exchange.

- ➢ Algorithm
- ➢ Illustration
- ➢ Notes

3.Explain RSA algorithm.

- ✓ Algorithm
- ✓ Illustration
- ✓ Diagram
- ✓ Notes

4.Describe Public Key Cryptography.

- ❑ Two Keys
- ❑ Private key
- ❑ public key
- ❑ distribution

5.Explain Elliptic Curve Architecture.

- Architecture
- Algebraic description
- Geometric description

UNIT 3

1.Explain Authentication Functions.

- Message Encryption
- MAC
- Hash function

2.Describe HMAC algorithm.

- ○ Algorithm
- ○ Diagram
- ○ Notes

3.Describe RIPEMD-160.

- ➢ Algorithm
- ➢ Diagram
- ➢ Notes

4.Explain Hash Functions.

- ❖ Security features
- ❖ Algorithms used
- ❖ Illustration

5.Explain Digital Signature Standard.

- Algorithm
- Analysis
- Diagram

UNIT 4

1.Explain Kerberos.

- ❖ Algorithm

- ❖ Explanation
- ❖ Diagram

2.Explain X.509 Authentication Services.

- ○ Algorithm
- ○ Explanation
- ○ Diagram

3.Describe Electronic Mail Security.

- ❖ Algorithm
- ❖ Explanation
- ❖ Diagram

4.Explain about PGP services.

- ❑ Algorithm
- ❑ Explanation
- ❑ Diagram

5.Describe S/MIME.

- ✓ Algorithm
- ✓ Explanation
- ✓ Diagram

UNIT 5

1.Explain Intrusion Detection.

- ✓ Audit records
- ✓ Statistical Anomaly Detection
- ✓ Rule Based Intrusion Detection
- ✓ Base-Rate Valley
- ✓ Distributed
- ✓ Honey pot
- ✓ Exchange format

2.State and Explain Password Management.

- ○ Password Protection
- ○ Password Selection Strategies

3.Explain the Firewall Design Principles.

- ▪ Firewall characteristics
- ▪ Types
- ▪ Firewall Configuration

4.Describe about Trusted Systems.

- ❑ Data Access Control

- Concept
- Trojan Horse Defense

5.Name some Viruses and Explain it.

- Malicious Programs
- Nature
- Types
- Macro viruses
- E-mail Viruses
- Worms