QUESTION BANK

Name of the Department : Computer Science and Engineering

Subject Code & Name : CS8792 Cryptography And Network Security

Year & Semester : IV & VII

UNIT I INTRODUCTION

PART-A

1. Define cryptography

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

2. Define cryptanalysis.

Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis**. Cryptanalysis is what the layperson calls "breaking the code."

3. Define security Attack, mechanism and service

• **Security attack:** Any action that compromises the security of information owned by an organization.
• **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
• **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

4. Distinguish Threat and Attack

Threat -A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.
Attack -An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

5. Differentiate active attacks and passive attacks.

A passive attack attempts to learn or make use of information from the system but does not affect system resources. Two types of passive attacks are the release of message contents and traffic analysis.

An active attack attempts to alter system resources or affect their operation. It can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

6. Specify the components of encryption algorithm

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

7. Describe security mechanism.

A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

8. Differentiate block and 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.

9. What are the essential ingredients of a symmetric cipher?

- **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
- **Cipher text:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data and, as it stands, is unintelligible.
- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

10. Specify four categories of security threats

- Interruption
- Interception
- Modification

- Fabrication

11. What is brute-force attack?

The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

12. List the types of cryptanalysis attack

- Cipher text only
- Known plain text
- Chosen plaintext
- Chosen cipher text
- Chosen text

13. Compare Substitution and Transposition techniques.

- **A substitution technique** is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.1 If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns. **Example**: Caesar cipher, monoalphabetic cipher, Playfair cipher,
- A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher. **Example**: rail fence

14. Define Steganography.

A plaintext message may be hidden . The methods of **steganography** conceal the existence of the message **Example Techniques:** character marking, invisible ink, pin punctures, type writer correction ribbon

15. Quote Euler's theorem.

Euler's theorem states that for every and that are relatively prime:

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

16. Quote Fermat's theorem.

If ***p*** is prime and **a** is a positive integer not divisible by ***p*** , then

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

17. Write algorithm for testing for primality

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

18. Define primitive root.

it is said that the base integer ***a*** generates (via powers) the set of nonzero integers modulo 19. Each such integer is called a primitive root of the modulus 19.More generally, we can say that the highest possible exponent to which a number can belong (mod n) is pie(n). If a number is of this order, it is referred to as a **primitive root** of n.

PART-B

1. State and Describe
(i) Fermat's theorem.
(ii) Euler's theorem
2. (i) Tabulate the substitution Techniques in detail.
ii) Describe the Transposition Techniques in detail.
3. (i) List the different types of attacks and explain in detail.
(ii) Describe in detail about the types of cryptanalytic attack.
4. Evalute3^21 mod 11 using Fermat's theorem.
5. Generalize the security services classifications and security mechanisms in detail.
6. (i)What is Steganography? Briefly examine any three techniques used.
(ii)What is mono-alphabetic cipher? Examine how it differs from Caesar cipher?
7.(i) Solve using playfair cipher. Encrypt the word "Semester Result" with the keyword "Examination". List the rules used.
(ii) Demonstrate the encryption of the message "PAY" using hill cipher with the following key matrix and show the decryption.

$$K = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix}$$

UNIT II SYMMETRIC KEY CRYPTOGRAPHY

PART-A

1. 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.

2. What is the difference between diffusion and confusion?

In diffusion, the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits; generally, this is equivalent to having each ciphertext digit be affected by many plaintext digits. confusion seeks to make the relationship between the statistics of the ciphertext 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 ciphertext, the way in which the key was used to produce that ciphertext is so complex as to make it difficult to deduce the key.This is achieved by the use of a complex substitution algorithm.

3. Whar are the design parameters of a Feistel cipher?

- Block size
- Key size
- Number of rounds
- Subkey generation algorithm
- Round function F
- Fast software encryption/ Decryption
- Ease of analysis

4. Explain the avalanche effect.

A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the ciphertext. In particular, a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. This is referred to as the avalanche effect. If the change were small, this might provide a way to reduce the size of the plaintext or key space to be searched.

5. What is the strength of DES?

- The use of 56 bit keys
- The nature of DES algorithm
- Timing attacks

6. Define product cipher

product cipher, which is the execution of two or more simple ciphers
in sequence in such a way that the final result or product is cryptographically stronger than any of the component ciphers.

7. What is substitution and permutation?

Substitution: Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.
Permutation: A sequence of plaintext elements is replaced by a permutation of that sequence. That is, no elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed.

8. Give 5 modes of operation in block cipher

- Electronic Codebook(ECB)
- Cipher Block Chaining(CBC)
- Cipher Feedback(CFB)
- Output Feedback(OFB)
- Counter(CTR)

9. State advantages of counter mode.

- Hardware Efficiency
- Software Efficiency
- Preprocessing
- Random Access
- Provable Security
- Simplicity.

10 Define Multiple Encryption.

It is a technique in which the encryption is used multiple times. Eg: Double DES, Triple DES. In the first instance, plaintext is converted to ciphertext using the encryption algorithm. This ciphertext is then used as input and the algorithm is applied again. This process may be repeated through any number of stages.

11. Specify the design criteria of block cipher.

- Number of rounds
- Design of the function F
- Key scheduling

12 Define Reversible mapping.

Each plain text is maps with the unique cipher text. This transformation is called reversible mapping.

13. What is Triple Encryption? How many keys are used in triple encryption?

Triple Encryption is a technique in which encryption algorithm is performed three times using three keys.

14 List the schemes for the distribution of public keys.

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

15. Drawback of 3-DES.

- Algorithm is sluggish in software
- The number of rounds in thrice as that of DES
- 3DES uses 64 bit block size
- To have higher efficiency and security a larger block size is needed.

16 List out the attacks to RSA.

- **Brute force** - Trying all possible private keys.
- **Mathematical attacks** - The approaches to factor the product of two prime numbers.
- **Timing attack** - Depends on the running time of the decryption algorithm.

17. What is traffic Padding? What is its purpose?

Traffic padding produces ciphertext output continuously, even in the absence of the plain text. A continuous random data stream is generated. When plain text is available, it is encrypted and transmitted. When input plaintext is not present, random data are encrypted and transmitted. This makes it impossible to for an attacker to distinguish between true dataflow and padding and therefore impossible to deduce the amount of traffic.

18 List the evaluation criteria defined by NIST for AES?

The evaluation criteria for AES is as follows:

- Security
- Cost
- Algorithm and implementation characteristics

PART-B

1. Summarize the following in detail.

(i) Modular Exponentiation.

(ii) Finite fields.

2. Discuss briefly the Discrete Algorithms.
3. Discuss about the Groups, Rings and Field.
4. Explain in detail about working of AES
5. Explain briefly about the block cipher modes of operations Diagram , adv and disadv for each Users A and B use the Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root α=7.

a. If user A has private key Xa = 5, what is A's public key Ya ?

b. If user B has private key Xb=12, what is B's public key Yb ?

c. What is the shared secret key?

6. Evaluate using Diffie-Hellman key exchange technique. Users A and B use a common prime q=11 and a primitive root alpha=7. (16)
7. (i) If user A has private key XA=3.What is A's public key YA? (ii)If user B has private key XB=6. What is B's public key YB? (iii) What is the shared secret key? Also write the algorithm.
8. Explain in detail about RC5 algorithm
9. Brief about Blowfish algorithm

UNIT III PUBLIC KEY CRYPTOGRAPHY

PART-A

1. Differentiate public key and conventional encryption?

Conventional Encryption Public key Encryption

1. The same algorithm with the same 1.One algorithm is used for encryption Key is used for encryption and decryption and decryption with a pair of keys, one for encryption and another for decryption

2. The sender and receiver must share 2.The sender and receiver
The algorithm and the key must each have one of the Matched pair of keys

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

Link Encryption End to End Encryption

1. With link encryption, each vulnerable 1.With end to end encryption, the Communications link is equipped on encryption process is carried out at Both ends with an encryption device the two end systems
2. Message exposed in sending host 2.Message encrypted in sending and and in intermediate nodes intermediate nodes
3. Transperant to user 3.User applies encryption
4 .Host maintains encryption facility 4.Users must determine algorithm
5. One facility for all users 5.Users selects encryption scheme
6. Can be done in hardware 6.Software implementations
7. Provides host authentication 7.Provides user authentication
8. Requires one key per(host-intermediate) 8.Requires one key per user pair Pair and (intermediate-intermediate)pair

3. What is traffic Padding? What is its purpose?

Traffic padding produces ciphertext output continuously, even in the absence of the plain text. A continuous random data stream is generated. When plain text is available, it is encrypted and transmitted. When input plaintext is not present, random data are encrypted and transmitted. This makes it impossible to for an attacker to distinguish between true dataflow and padding and therefore impossible to deduce the amount of traffic.

4. What are roles of public and private key?

The two keys used for public-key encryption are referred to as the public key and the private key. Invariably, the private key is kept secret and the public key is known publicly. Usually the public key is used for encryption purpose and the private key is used in the decryption side.

5. Specify the applications of the public key cryptosystem?

The applications of the public-key cryptosystem can classified as follows

1. Encryption/Decryption: The sender encrypts a message with the recipient's public key.
2. Digital signature: The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to a message or to a small block of data that is a function of the message.
3. 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.

6. What requirements must a public key cryptosystem to fulfill to a secured algorithm?

The requirements of public-key cryptosystem are as follows:

1. It is computationally easy for a party B to generate a pair(Public key KUb, Private key KRb)
2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted , M, to generate the corresponding ciphertext: C=EKUb(M)
3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message : M=DKRb(C)=DKRb[EKUb(M)]
4. It is computationally infeasible for an opponent , knowing the public key,KUb,to determine the private key,KRb.
5. It is computationally infeasible for an opponent , knowing the public key,KUb, and a ciphertext, C, to recover the original message,M.

7 What is a one way function?

One way function is one that map the domain into a range such that every function value has a unique inverse with a condition that the calculation of the function is easy where as the calculations of the inverse is infeasible.

8. What is a trapdoor one way function?

It is function which is easy to calculate in one direction and infeasible to calculate in other direction in the other direction unless certain additional information is known. With the additional information the inverse can be calculated in polynomial time. It can be summarized as: A trapdoor one way function is a family of invertible functions fk, such that Y= fk(X) easy, if k and X are known X=fk -1(Y) easy, if k and y are known X= fk -1(Y) infeasible, if Y is known but k is not known.

9. **Define Euler's theorem and it's application?**

Euler's theorem states that for every a and n that are relatively prime: a PRG_Q

10 . Define Euler's totient function or phi function and their applications?

The Euler's totient function states that, it should be clear for a prime number p, S_ _S-1

11. Describe in general terms an efficient procedure for picking a prime number?

The procedure for picking a prime number is as follows: 1. Pick an odd integer n at random (eg., using a pseudorandom number generator). 2.

12. Pick an integer a What are essential ingredient of the public key directory?

The essential ingredient of the public key are as follows:

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 a 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 comprised 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

PART-B

1. **State Chinese Remainder theorem and find X for the given set of congruent equations using CRT. X=2(mod 3) X=3(mod 5) X=2(mod 7)**
2. **Evaluate** using Diffie-Hellman key exchange technique. Users A and B use a common prime q=11 and a primitive root alpha=7.

(i) If user A has private key XA=3.What is A's public key YA?
(ii) If user B has private key XB=6. What is B's public key YB?
(iii) What is the shared secret key? Also write the algorithm.

3. **Describe** RSA Algorithm.
4. **Estimate** the encryption and decryption values for the RSA algorithm parameters. P=7, Q=11, E=17, M=8.
5. What are elliptic curves? **Describe** how the elliptic curves are useful for Cryptography?
6. **Describe** the key management of public key encryption in detail.
7. User A and B use Diffie-Hellman key exchange a common prime q=71 and a primitive root a=7.**Calculate** the following. If user A has private key X_A=5, what is A's public key Y_A. If user A has private key XB=12, what is B's public key YB and what is shared secret key

UNIT IV DISASTER RISK MANAGEMENT IN INDIA

PART-A

1. What is a hash in cryptography?

A **hash function** H accepts a variable-length block of data M as input and produces a fixed-size hash
value h= H(M) called as message digest as output. It is the variation on the message authentication code.

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

The hash algorithm involves repeated use of a compression function f, that takes two inputs and produce a n-bit output. At the start of hashing the chaining variable has an initial value that is specified as part of the algorithm. The final values of the chaining variable is the hash value usually b>n; hence the term compression.

3. What is cryptography hash function?

The kind of hash function needed for security applications is referred to as a **cryptographic hash function**. A cryptographic hash function is an algorithm for which it is computationally infeasible (because no attack is significantly more efficient than brute force) to find either (a) a data object that maps to a pre-specified hash result (the one-way

property) or (b) two data objects that map to the same hash result (the collision-free property). Because of these characteristics, hash functions are often used to determine whether or not data has changed.

4. What are the applications of cryptographic hash function?

- Message Authentication
- Digital Signatures
- pseudorandom function (PRF) or a pseudorandom number generator (PRNG).

5. What are the requirements for message authentication?

- Disclosure
- Traffic analysis
- Masquerade
- Content modification
- Sequence modification
- Timing modification
- Source repudiation
- Destination repudiation

6. What is collision resistant attack or birthday paradox?

For a collision resistant attack, an adversary wishes to find two messages or data blocks, *x* and , that yield the same hash function:H(x)= H(y). This turns out to require considerably less effort than a preimage or second preimage attack. The effort required is explained by a mathematical result referred to as the **birthday paradox**.

In essence, if we choose random variables from a uniform distribution in the range 0 through N-1, then the probability that a repeated element is encountered exceeds 0.5 after root(N) choices have been made. Thus, for an m -bit hash value, if we pick data blocks at random, we can expect to find two data blocks with the same hash value within root(2^m) = $2^{m/2}$ attempts

7. List the processing logic of SHA-512

- Append padding bits
- Append padding length
- Initialize hash buffer
- Process message in 1024 bits(128-words) blocks
- Output

8 Mention the various ways of producing authenticator or define the classes of message authentication function

• **Hash function:** A function that maps a message of any length into a fixed length hash value, which serves as the authenticator

• **Message encryption:** The ciphertext of the entire message serves as its authenticator

• **Message authentication code (MAC):** A function of the message and a secret key that produces a fixed-length value that serves as the authenticator

11. What do you meant by MAC?

It involves the use of a secret key to generate a small fixed-size block of data, known as a

cryptographic checksum or MAC, that is appended to the message. This technique assumes that two communicating parties, say A and B, share a common secret key .When A has a message to send to B, it calculates the MAC as a function of the message and the key:
MAC = MAC(*K, M*) where
M = input message
C = MAC function
K = shared secret key
MAC = message authentication code

12. Differentiate MAC and Hash function?
MAC: In MAC , 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.

13. List any three hash algorithm.
- MD5(message Digest version 5) algorithm
- SHA_1 (Secure Hash algorithm)
- RIPEMD_160 algorithm

14. What is the difference between weak and strong collisions resistance?
Weak collisions resistance: for any given block x, it is computationally infeasible to find y * x with H(y) = H(x). it is proportional to 2^n .
Strong collision resistance: it is computationally infeasible to find any pair (x,y) such that H(x)= H(y). it is proportional to $2^{n/2}$

15. 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.

16. What is the meet in the middle attack?
This is the cryptanalytic attack that attempts to find the value in each of the range and domain of the composition of two functions such that the forward mapping of one through the first function is the same as the inverse image of the other through the second function- quite literally meeting in the middle of the composed function.

17. Compare MD5, SHA1 and RIPEMD-160 algorithm.

	MD5	SHA-1	RIPEMD160
Digest length	128 bits	160 bits	160 bits
Basic unit of processing	512 bits	512 bits	512 bits
No.of steps	64(4 rounds of 16)	80(4 rounds of 20)	160(5 pairs rounds of
Maximum message size	infinity	2^{64}-1 bits	2^{64}-1 bits

Primitive logical function	4	4	5
Additive constant used	64	4	9
Endianess	Little endian	Big endian	Little endian

18. Distinguish between direct and arbitrated digital signature?

Direct digital signature	Arbitrated Digital Signature
1.The direct digital signature involves only the communicating parties. 2.This may be formed by encrypting the entire message with the sender's private key.	1.The arbiter plays a sensitive and crucial role in this digital signature. 2. 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.

19. What are the properties a digital signature should have?

It must verify the author and the data and time of signature.

- It must authenticate the contents at the time of signature.
- It must be verifiable by third parties to resolve disputes.

20. What requirements should a digital signature scheme should satisfy?

- The signature must be bit pattern that depends on the message being signed.
- The signature must use some information unique to the sender, to prevent both forgery and denial.
- It must be relatively easy to produce the digital signature.
- It must be relatively easy to recognize and verify the digital signature.
- 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.
- It must be practical to retain a copy of the digital signature in storage.

21. What is digital signature?

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

22. What is dual signature? What it is purpose?

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

23. 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.

24. What is Kerberos? What are the uses?

Kerberos is an authentication service developed as a part of project Athena at MIT.Kerberos provide a centralized authentication server whose functions is to authenticate servers.

PART-B

1. Describe Secure hash Algorithm in detail.
2. Describe the MD5 message digest algorithm with necessary block diagrams.
3. (i)Summarize CMAC algorithm and its usage.
   (ii)Describe any one method of efficient implementation of HMAC.
4. Describe digital signature algorithm and show how signing and verification is done using DSS.
5. Explain in detail ElGamal Digital Signature scheme with an example.
6. Explain in detail about different ways of distribution of public keys
7. Consider prime field q=19, it has primitive roots { 2,3,10,13,14,15}, if suppose α=10. Then write key generation by she choose X_A=16. And also sign with hash value m=14 and alice choose secret no K=5. Verify the signature using Elgamal digital Signature Scheme
8. What is Kerberos? Explain how it provides authenticated service.
9. Explain the format of the X.509 certificate.
10. Explain the technical details of firewall and describe any three types of firewall with neat diagram.

UNIT V SECURITY PRACTICE AND SYSTEM SECURITY

PART-A

1. 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.

2. List the limitations of SMTP/RFC 822?

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

3. **Define S/MIME?**

Secure/Multipurpose Internet Mail Extension(S/MIME) is a security enhancement to the MIME

4. **What are the different between SSL version 3 and TLS?**

SSL	TLS
In SSL , the minor version is zero and major version is 3	In TLS, the major version is 3 and the minor version is 1

SSL use HMAC algorithm, except that the padding bytes concatenation	Make use of the same algorithm
SSL supports 12 various alert codes	It supports all of the alert codes defined in SSL3 with the exception of no-certificate.

5. **What are the services provided by PGP services.**
• Digital signature
• Message encryption
• Compression
• E-mail compatibility
• Segmentation

6. **Explain the reasons for using PGP?**
 It is available free worldwide versions that run on a variety of platforms, including DOS/Windows, UNIX, Macintosh and many more
 It is based on algorithms that have survived extensive public review and are considered extremely secure (eg). RSA,DSS
 It has a wide range of applicability from corporations that wish to select and enforce a standardized scheme for encrypting files and communication
 It was not developed by nor and is it controlled by any government or standard organization.

7. **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.

8. **Name any cryptographic keys used in PGP?**
 One time session conventional keys
 Public keys
• Private keys
 Pass phrase based conventional keys.

9. **List out the features of SET.**
 Confidentiality
 Integrity of data
 Cardholder account authentication
 Merchant authentication

10. **What is security association?**
A security association (SA) is the establishment of shared security attributes between two network entities to support secure communication.

11. **What does Internet key management in IPSec?**
Internet key exchange (IKE) is a key management protocol standard used in conjunction with the Internet Protocol Security (IPSec) standard protocol. It provides security for Virtual Private Networks (VPNs) negotiations and network access to random hosts.

12. **List out the IKE hybrid protocol dependence.**
- ISAKMP - Internet Security Association and Key Management Protocols.
- Oakley

13. **What does IKE hybrid protocol mean?**
Internet Key Exchange (IKE) is a key management protocol standard used in conjunction with the internet protocol security (IPSec) standard protocol. It provides security for Virtual Private Networks (VPNs) negotiations and network access to random hosts.

14. **What are the two security services provided by IPSec?**
- Authentication Header (AH)
- Encapsulating Security Payload (ESP).

15. **What are the fields available in AH header?**
- Next header
- Payload length
- Reserved
- Security parameter
- Sequence number Integrity check value

16. **What is virtual private network?**
VPN means virtual private network, a secure tunnel between two devices.

17. **What is ESP?**
ESP- encapsulating security payload provides authentication, integrity and confidentiality, which protect against data tempering and provide message content protection. IPSec provides standard algorithms, such as SHA and MD5.

18. **What is Behavior-Blocking Software (BBS)?**
BBS integrates with the OS of a host computer and monitors program behavior in real time for malicious actions.

19. **List password selection strategies.**
- User education
- Reactive password checking
- Computer-generated password.
- Proactive password checking.

20. **List out the applications of IPsec**
- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establishing extranet and intranet connectivity with partners
- Enhancing electronic commerce security

21. **Write down the benefits of IPsec**

• When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.
• IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.
• IPsec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.

22. **Differentiate Transport mode and Tunnel mode**

Transport mode	**Tunnel mode**
Provide the protection from upper layer between 2 hosts	Provide the protection for entire IP Packet
ESP in this mode encrypts and optionally authenticates IP Payload but not IP headers	ESP in this mode encrypt authenticate the entire IP packet
AH in this mode authenticate the IP payload and select the portion of IP header	AH in this mode authenticate the entire IP packet plus selected portion of outer IP header

23. **List services 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

PART-B

1. How IPSec ESP does provide transport and Tunnel Mode operation? Explain with a neat sketch. (16)
2. What is the need for security in IP networks? Describe the IPv6 authentication header.(16)
3. What is PGP? Show the message format of PGP(8)
4. Explain the operational description of PGP(10)
5. Describe about the PKI. (8)
6. Identify the fields in ISAKMP and explain it.(8)
7. Evaluate the different protocols of SSL. Explain Handshake protocol in detail.(16)
8. Describe the phases of Internet key exchange in detail. (16)
9. Explain in detail about S/MIME. (8)