CS6701 - CRYPTOGRAPHY AND NETWORK SECURITY QUESTION BANK

UNIT-I PART-A

1. Specify the four categories of security threats.
   Interruption Interception Modification Fabrication
2. Explain active and passive attack with example.
   Passive attack: Monitoring the message during transmission. Eg: Interception Active attack: It involves the modification of data stream or creation of false data stream. E.g.: Fabrication, Modification, and Interruption
3. Define integrity and non repudiation.
   Integrity: Service that ensures that only authorized person able to modify the message. Non repudiation: This service helps to prove that the person who denies the transaction is true or false.
4. Differentiate symmetric and asymmetric encryption?
   Symmetric Asymmetric It is a form of cryptosystem in which It is a form of cryptosystem in which encryption and decryption performed using encryption and decryption Performed using the same key. Eg: DES, AES two keys. Eg:RSA,ECC
5. Define cryptanalysis?
   It is a process of attempting to discover the key or plaintext or both.
6. Define security mechanism
   It is process that is designed to detect prevent, recover from a security attack. Example: Encryption algorithm, Digital signature, Authentication protocols.
7. Define steganography
   Hiding the message into some cover media. It conceals the existence of a message.
8. Why network need security?
   When systems are connected through the network, attacks are possible during transmission time.
9. Define confidentiality and authentication
   Confidentiality: It means how to maintain the secrecy of message. It ensures that the information in a computer system and transmitted information are accessible only for reading by authorized person. Authentication: It helps to prove that the source entity only has involved the transaction.
10. Define cryptography.
    It is a science of writing Secret code using mathematical techniques. The many schemes used for enciphering constitute the area of study known as cryptography.
11. Compare Substitution and Transposition techniques.
    SUBSTITUTION
    TRANSPOSITION
    *A substitution techniques is one in * It means, different kind of mapping is which the letters of plaintext are replaced by other letter or by number or symbols. achieved by performing some sort of *Eg: Caeser cipher. permutation on the plaintext letters. *Eg: DES, AES.
12. Define Diffusion & Confusion.
    Diffusion: It means each plaintext digits affect the values of many ciphertext digits which is equivalent to each ciphertext digit is affected by many plaintext digits. It can be achieved by performing permutation on the data. It is the relationship between the plaintext and ciphertext.
    Confusion: It can be achieved by substitution algorithm. It is the relationship between cipher text and key.
13. Define Multiple Encryption.
    It is a technique in which the encryption is used multiple times. Eg: Double DES, Triple DES
14. Specify the design criteria of block cipher.
     Number of rounds Design of the function F Key scheduling

15. Define Reversible mapping.
    Each plain text is maps with the unique cipher text. This transformation is called reversible mapping.
16. Specify the basic task for defining a security service.
    A service that enhances the security of the data processing systems and the information transfer of an organization. The services are intended to counter security attack, and they make use of one or more security mechanism to provide the service.
17. Define network security.
    This area covers the use of cryptographic algorithms in network protocols and network applications.
18. Define computer security.
    This term refers to the security of computers against intruders and malicious software.
19. What are hill cipher merits and demerits?
    Completely hides single letter and 2 letter frequency information.
20. List-out the types of attack in ceaser cipher.
    x Brute force attack. x Just try all the 25 possible keys.

PART-B

1. Explain the followings: (a) Playfair cipher. (8) (b) Vernam cipher in detail. (8)

2. Explain simplified DES with example. (16)

3. Write short notes on i) Steganography(16)

4. Explain classical Encryption techniques in detail. (16)

5. Write short notes on (a) Security services(8) (b) Feistel cipher structure(8)

6. Explain the OSI security architecture. (16)

7. a. Explain various transposition ciphers in detail.(8)

b. Explain the basic principle of rotor machine. (8)

8. Explain in detail about Feistel cipher with diagram. (16)

9. a.Explain classical encryption techniques with symmetric cipher model. (12)

b. Explain steganography in detail. (4)

10. Convert “MEET ME” using Hill cipher with the key matrix Convert the cipher text back to plaintext.

11. Write short notes on block cipher modes of operation

12. (i) Discuss any four Substitution Technique and list their merits and demerits. (16)

13. Explain in detail about various types of attacks.

14. Explain in detail about various services provided by X.800.

15. Explain in detail about various Mechanisms provided by X.800.

16. Briefly explain the design principles of block cipher. (8)

17.Write short notes on (i)Fermat and Eluer’s theorem (8) (ii)Chinese Remainder theorem (8)

18. Discuss with neat sketch a network security model. (8)

UNIT-II PART-A

1. Compare stream cipher with block cipher with example.
   Stream cipher: Processes the input stream continuously and producing one element at a time. Example: caeser cipher. Block cipher: Processes the input one block of elements at a time producing an output block for each input block. Example: DES.

2. Differentiate unconditionally secured and computationally secured .
   An Encryption algorithm is unconditionally secured means, the condition is if the cipher text generated by the encryption scheme doesn’t contain enough information to determine corresponding plaintext.

Encryption is computationally secured means, 1. The cost of breaking the cipher exceed the value of enough information. 2. Time required to break the cipher exceed the useful lifetime of information.

3. Define Diffusion & Confusion.

Diffusion: It means each plaintext digits affect the values of many ciphertext digits which is equivalent to each ciphertext digit is affected by many plaintext digits. It can be achieved by performing permutation on the data. It is the relationship between the plaintext and ciphertext. Confusion: It can be achieved by substitution algorithm. It is the relationship between cipher text and key.

4. What are the design parameters of Feistel cipher network?

*Block size

*Key size

*Number of Rounds

*Sub key generation algorithm

*Round function

*Fast software Encryption/Decryption

*Ease of analysis

5. Define Product cipher.

It means two or more basic cipher are combined and it produce the resultant cipher is called the product cipher.

6. Explain Avalanche effect.

A desirable property of any encryption algorithm is that a small change in either the plaintext or the key 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 manybits of the ciphertext. If the change is small, this might provider a way to reduce the size of the plaintext or key space to be searched. 7. Give the five modes of operation of Block cipher.

i. Electronic Codebook(ECB) ii. Cipher Block Chaining(CBC) iii. Cipher Feedback(CFB) iv. Output Feedback(OFB) v. Counter(CTR)

8. State advantages of counter mode.

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

9. Define Multiple Encryption.

It is a technique in which the encryption is used multiple times. Eg: Double DES, Triple DES

10. Specify the design criteria of block cipher.

Number of rounds Design of the function F Key scheduling

11. Define Reversible mapping.

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

12. Specify the basic task for defining a security service.

A service that enhances the security of the data processing systems and the information transfer of an organization. The services are intended to counter security attack, and they make use of one or more security mechanism to provide the service.

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

Link Encryption End to End Encryption

1.With link encryption, each vulnerable communication link is equipped on Both ends with an encryption device

2.Message exposed in sending host and in intermediate nodes

3.Transperant to user

4.Host maintains encryption facility

5.One facility for all users

6.Can be done in hardware

7.Provides host authentication

8.Requires one key per(hostintermediate) Pair and (intermediateintermediate) pair

1.With end to end ncryption, encryption process is carried out at the two end systems
2.Message encrypted in sending and intermediate nodes
3.User applies encryption
4.Users must determine algorithm
5.Users selects encryption scheme
6.Software implementations
7.Provides user authentication
8.Requires one key per user pair

14. 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.

15. List the evaluation criteria defined by NIST for AES?

The evaluation criteria for AES is as follows: 1.Security 2. Cost 3.Algorithm and implementation characteristics

16. 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.

17. List the schemes for the distribution of public keys.

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

18. Drawback of 3-DES.

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

19. List out an evaluation criteria for round 2.

x General security x Software implementation x Hardware implementation x Attacks x Encryption Vs Decryption x Key ability-Ability to change keys quickly with minimum of resources. x Versatility and Flexibility x Instruction level parallelism.

21. List out the attacks to RSA.

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

PART-B

1.State and explain the principles of public key cryptography?
2.Explain Diffie Hellman key Exchange in detail with an example?
3.Explain the key management of public key encryption in detail?
4.Explain RSA algorithm in detail with an example?
5.Briefly explain the idea behind Elliptic Curve Cryptosystem?
6.Explain Data Encryption Standard (DES) in detail. (16) How AES is used for encryption/decryption? Discuss with example. (16)
7.List the evaluation criteria defined by NIST for AES. (16)
8.Using play fair cipher algorithm encrypts the message using the key "MONARCHY" and Explains the poly alphabetic key. (16)
9.Explain 1.ceaser cipher 2. Mono alphabetic cipher 3.one time pad cipher (16)
10.Explain the Key Generation, Encryption and Decryption of DES algorithm in detail. (16)
11.Explain in detail the key generation in AES algorithm and its expansion format. (16)

12.a. Explain single round DES with neat sketch.(10) b .Explain Double &Triple DES with keys. (6)

13. Explain the block cipher modes of operation. (16)

14.Explain the key management of public key encryption in detail. (16)

15.Explain ECC - Diffie Hellman key Exchange with both keys in detail with an example. (16)

16.Write about elliptic curve architecture in detail and how they are useful for cryptography. (16)

17.a. Write about key distribution in detail. (10)

b. Explain the purpose of CRT. (6)

18.Explain the different methods used in random number generation. (16)

19. What are the requirements and applications of public key? Compare conventional with public key encryption. (16)

20.(i) Identify the possible threats for RSA algorithm and list their counter measures. (8)

(ii) Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and N=5. (8)

21. (i) Draw the general structure of DES and explain the encryption decryption process. (10)

(ii) Mention the strengths and weakness of DES algorithm. (6)

22. (i) Explain the generation sub key and S Box from the given 32-bit key by Blowfish. (8)

(ii) In AES, hoe the encryption key is expanded to produce keys for the 10 rounds.(8)

23.(i) Describe about RC4 algorithm. (8)

(ii) Explain the Miller-Rabin algorithm. (8)

UNIT-III PART-A

1. What is message authentication?

It is a procedure that verifies whether the received message comes from assigned source has not been altered. It uses message authentication codes, hash algorithms to authenticate the message.

2. 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.

3. What are the requirements for message authentication?

The requirements for message authentication are

i.Disclosure: Release of message contents to any person or process not processing the appropriate cryptographic key

ii. Traffic Analysis: Discovery of the pattern of traffic between parties. In a connection oriented application, the frequency and duration of connections could be determined. In either a connection oriented or connectionless environment, the number and length of messages between parties could be determined.

iii. Masquerade: Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgements of message receipt or no receipt by someone other than the message recipient.

iv. Content modification: Changes to the contents of a message , including insertion, deletion, transposition, and modification.

v. Sequence modification: Any modification to a sequence of messages between parties, including insertion, deletion, and modification.

vi. Timing modification: Delay or replay of messages. In a connection oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In connectionless application, an individual message could be delayed or replayed.

vii. Source repudiation: Denial of transmission of message by source.

viii. Destination repudiation: Denial of receipt of message by destination.

4. 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.

5. 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.

6. Any three hash algorithm.

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

7. What are the requirements of the hash function?

   • H can be applied to a block of data of any size. • H produces a fixed length output. • H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.

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. MAC = Ck(M) Where M = variable length message K = secret key shared by sender and receiver. CK(M) = fixed length authenticator.

9. 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.

10. 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.

11. What is the role of compression function in 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 value of the chaining variable is the hash value usually b>n; hence the term compression.

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

    Weak collision resistance Strong resistance collision For any given block x, it is It is computationally infeasible to computationally infeasible to fine find any pair (x,y) such that y≠x wit H(y)=H(x). H(x)=H(y). It is proportional to 2n It is proportional to 2 n/2

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

    MD5 SHA-1 RIPEMD160 Digest length 128 bits 160 bits 160 bits Basic unit of 512 bits 512 bits 512 bits processing No of steps 64(4 rounds of 16) 80(4 rounds of 20) 160(5 pairs rounds of 16) Maximummessage infinity 2 64-1 bits 2 64-1 bits size Primitive logical 4 4 5 function Additive constants 64 4 9 used Endianess Little endian Big endian Little endian

14. Distinguish between direct and arbitrated digital signature?

    Direct digital signature

    1.The direct digital signature

    2. Every signed message from a

    Arbitrated Digital Signature

1.The arbiter plays a sensitive and involves only the communicating crucial role in this digital signature. parties.

2.This may be formed by sender x to a receiver y goes first to encrypting the an arbiter A, who subjects the message and its signature to a entire message with the sender's number of tests to check its origin private key. and content.

15. 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.

16. 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.

PART-B

1. Explain the classification of authentication function in detail.

2. Describe MD5 algorithm in detail. Compare its performance with SHA-1.

3. Describe SHA-1 algorithm in detail. Compare its performance with MD5 and RIPEMD-160 and discuss its advantages.

4. Describe RIPEMD-160 algorithm in detail. Compare its performance with

5. Describe HMAC algorithm in detail.

6. Write and explain the Digital Signature Algorithm.

7. Briefly explain Deffie Hellman key exchange with an example. (16)

8. Write and explain the digital signature algorithm. (8)

(ii) Explain in detail Hash Functions. (8)

9. Compare the Features of SHA-1 and MD5 algorithm. (8)

10. Discuss about the objectives of HMAC and it security features. (8)

11. How man in middle attack can be performed in Diffie Hellman algorithm.(4)

12. Explain in detail EIGamal Public key cryptosystem. (8)

13. Discuss clearly Secure Hash Algorithm(SHA) (8)

14. Describe the MD5 message digest algorithm with necessary block diagrams. (16)

UNIT-IV PART-A

1. 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.

2. 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.

3. What 4 requirements were defined by Kerberos?

x Secure x Reliable x Transparent x Scalable

4. 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:

x The Kerberos server must have user ID and hashed password of all participating users in its database.

x The Kerberos server must share a secret key with each server. Such an environment is referred to as "Realm".

5. What is the purpose of X.509 standard?

X.509 defines framework for authentication services by the X.500 directory to its users.X.509 defines authentication protocols based on public key certificates.

6. List the 3 classes of intruder?

Classes of Intruders x Masquerader x Misfeasor x Clandestine user

7. Define virus. Specify the types of viruses?

x 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: x Parasitic virus x Memory-resident virus x Boot sector virus x Stealth virus x Polymorphic virus

8. 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.

9. List the design goals of firewalls?

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

10. What are the steps involved in SET Transaction?

x The customer opens an account x The customer receives a certificate x Merchants have their own certificate x The customer places an order. x The merchant is verified. x The order and payment are sent. x The merchant requests payment authorization. x The merchant confirm the order. x The merchant provides the goods or services. x The merchant requests payment.

11. 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.

12. Give SSL record format?

Content type Major version Minor version Compressed length Plain text(Optimality compressed) MAC 0,16,or 20bytes.

13. What is the need for authentication applications?

x Security for E-mail x Internet protocol security x IP address security.

14. Differentiate public key encryption and conventional encryption.

Conventional encryption Public key encryption Same algorithm with same key used for encryption and decryption. Same algorithm Is used for encryption and decryption with a pair of keys. Sender and receiver must share the algorithm and keys. Sender and reciver have one of the matched pair keys. Key must be kept secret. Any one of the key must be kept secretly.

15. What is message authentication?

Message authentication is a process that verifies whether the recived message comes from assigned source has not been altered.

16. Specify the requirements for message authentication?

x Disclosure x Traffic analysis x Masquerade x Content modification x Sequence modification x Timing modification x Repudiation.

17. Specify the four categories of security threats?

x Interruption x Interception x Modification x Fabrication

20. What do you mean by SET? What are the features of SET?

SET is an open encryption and security specification designed to protect credit card transaction on the Internet.

21. Write any 3 hash algorithm?

x MD5 algorithm x SHA-I x RIPEMD-160 algorithm.

22. Define the classes of message authentication function.

x Message encryption x Meassage authentication code x Hash function.

23. List out the four phases of virus.

x Dormant phase x Propogation phase x Triggering phase x Execution phase

24. 24. What is worm?

A worm is a program that can relicate itself and send copies from computer to computer across network connections.

25. What is Bastion host?

Bastion host is a system identified by firewall administrator as critical strong point in network security.

26. What is a trusted software?

Trusted software a system that enhance the ability of a system to defend against intruders and malicious programs by implementing trusted system technology.

27. Four general techniques of firewall.

x Security control x Direction control x User control x Behaviour control

28. Three types of firewall.

x Packet filter x Application level gateway x Circuit level gateway.

29. List approaches for intrusion detection.

x Statistical anamoly detection x Rule based detection

30. What is intruder?

An intruder is an attacker who tries tog an unauthorized access to a system.

31. 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: a). Confidentiality of information b). Integrity of data c). Cardholder account authentication d). Merchant authentication

32. What is Zombie?

A Zombie is a program that securely takes over another internet-attached computer and then uses that computer to launch attacks are difficult to trace the Zombie's creator.

PART-B

1. Explain in detail about KDC.
2. Explain the different ways of public key distribution in detail.
3. What is Kerberos? Explain how it provides authenticated service.
4. Explain the format of the X.509 certificate.
5. Explain the technical details of firewall and describe any three types of firewall with neat diagram.
6. Write short notes on Intrusion Detection.
7. Define virus. Explain in detail.
8. Describe trusted system in detail.
9. Explain the technical details of firewall and describe any three types of firewall with neat diagram.
10. Write short notes on Intrusion Detection.
11. Explain any two approaches for intrusion detection.
12. Explain firewalls and how they prevent intrusions.
13. Define intrusion detection and the different types of detection mechanisms, in detail.
14. Explain the types of Host based intrusion detection. List any two IDS software available.

15. What are the positive and negative effects of firewall? 16. Describe the familiar types of firewall configurations.

17. Explain Intrusion detection.

18. Explain the firewall design principles.

19. Name some viruses & explain it.

20. Describe about trusted systems.

UNIT-V 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?

1. SMTP cannot transmit executable files or binary objects. 2. It cannot transmit text data containing national language characters. 3. SMTP servers may reject mail message over certain size. 4. SMTP gateways cause problems while transmitting ASCII and EBCDIC. 5. 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 Internet E-mail format standard, based on technology from RSA Data Security.

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

SSL TLS * In SSL the minor version is 0 and * In TLS, the major version is 3 and the minor major version is 3. version is 1. * SSL use HMAC alg., except that the padding bytes concatenation. * TLS makes use of the same alg. * SSL supports 12 various alert codes. * TLS 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. 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.

7. Name any cryptographic keys used in PGP?

x One-time session conventional keys. x Public keys. x Private keys. x Pass phrase based conventional keys.

8. 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.

9. What are the services provided by PGP services?

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

10. Name any cryptographic keys used in PGP?

x One time session conventional keys x Public keys x Private keys x Pass phrase based conventional keys.

11. What are the steps involved in SET transaction?

x The customer opens an account. x The customer receives a certificate x Merchants have their own certificate x The customer places an order. x The merchant requests payment authorization. x The merchant confirm the order. x The merchant provides the goods or services. x The merchant requests payments.

12. List out the features of SET.

x Confidentiality x Integrity of data x Cardholder account authentication x 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.

x ISAKMP - Internet Security Association and Key Management Protocols. x 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?

x Authentication Header (AH) x Encapsulating Security Payload (ESP).

15. What are the fields available in AH header?

x Next header x Payload length x Reserved x Security parameter x 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.

x User education x Reactive password checking x Computer-generated password. x Proactive password checking.

PART-B

1. Explain the operational description of PGP.
2. Write Short notes on S/MIME.
3. Explain the architecture of IP Security.
4. Write short notes on authentication header and ESP.
5. Explain in detail the operation of Secure Socket Layer in detail.
6. Explain Secure Electronic transaction with neat diagram.
7. Write brief note on E-mail Security.
8. Write brief note on IP Security.
9. Write brief note on Web Security.
10. Explain about PKI in detail.
11. Describe about SSL/TLS Protocol.
12. Explain in detail the operation of Internet Key Exchange with an example.