

CS6701 CRYPTOGRAPHY AND NETWORK SECURITY QUESTION BANK

2 Marks

UNIT I

1. Specify the four categories of security threads? . 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 nonrepudiation? Integrity:

Service that ensures that only authorized person able to modify the message.

Nonrepudiation:

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 encryption and decryption performed using the same key.

It is a form of cryptosystem in which encryption and decryption

Performed using two keys.

Eg: DES, AES Eg: RSA, ECC

5. Define cryptanalysis?

It is a process of attempting to discover the key or plaintext or both.

6. Compare stream cipher with block cipher with example. Stream cipher:

Processes the input stream continuously and producing one element at a time. Example: caesar cipher.

Block cipher:

Processes the input one block of elements at a time producing an output block for each input block.

Example: DES.

7. Define security mechanism

It is process that is designed to detect prevent, recover from a security attack. Example: Encryption algorithm, Digital signature, Authentication protocols.

8. 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.

9. Define steganography

Hiding the message into some cover media. It conceals the existence of a message.

10. Why network need security?

When systems are connected through the network, attacks are possible during transmission time.

11. Define Encryption

The process of converting from plaintext to cipher text.

12. Specify the components of encryption algorithm.

1. Plaintext
2. Encryption algorithm
3. secret key
4. ciphertext
5. Decryption algorithm

13. 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 authorised person.

Authentication:

It helps to prove that the source entity only has involved the transaction.

14. 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.

15. Compare Substitution and Transposition techniques.

SUBSTITUTION TRANSPOSITION

*A substitution techniques is one in which the letters of plaintext are replaced by other letter or by number or symbols.

*Eg: Caesar cipher.

* It means,different kind of mapping is achieved by performing some sort of permutation on the plaintext letters.

*Eg: DES, AES.

16. 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 ciphertext and key.

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

*Block size

*Key size

*Number of Rounds

*Subkey generation algorithm

*Round function

*Fast software Encryption/Decryption

*Ease of analysis

18. Define Product cipher.

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

19. 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 many bits of the ciphertext. If the change is small, this might provide a way to reduce the size of the plaintext or key space to be searched.

20. Give the five modes of operation of Block cipher.

1. Electronic Codebook(ECB)
2. Cipher Block Chaining(CBC)
3. Cipher Feedback(CFB)

4. Output Feedback(OFB)

5. Counter(CTR)

21. State advantages of counter mode.

*Hardware Efficiency

*Software Efficiency

*Preprocessing

*Random Access

* Provable Security

*Simplicity.

22. Define Multiple Encryption.

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

23. Specify the design criteria of block cipher.

Number of rounds Design of the function F Key scheduling

24. Define Reversible mapping.

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

25. 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.

26. 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

27. 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.

28. 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

29. 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.

UNIT II

30. 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

3. The key must be secret 3. One of two keys must be kept

Secret

4. It must be impossible or at least impractical 4. It must be impossible or to decipher a message if no other information at least impractical to decipher a is available message if no other information

is available

5. Knowledge of the algorithm plus samples 5. Knowledge of the algorithm of cipher text must insufficient to determine plus one of key plus samples of the key ciphertext must be insufficient to determine the other key.

31. What are the principle elements of a public key cryptosystem?

The principle elements of a cryptosystem are:

1. plain text

2. Encryption algorithm

3. Public and private key

4. Cipher text

5. Decryption algorithm

32. 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.

33. Specify the applications of the public key cryptosystem?

The applications of the public-key cryptosystem can be 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.

34. What requirements must a public key cryptosystem fulfill to be 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 K_{Ub} , Private key K_{Rb})
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:

$$C = E_{K_{Ub}}(M)$$

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message: $M = D_{K_{Rb}}(C) = D_{K_{Rb}}[E_{K_{Ub}}(M)]$
4. It is computationally infeasible for an opponent, knowing the public key, K_{Ub} , to determine the private key, K_{Rb} .
5. It is computationally infeasible for an opponent, knowing the public key, K_{Ub} , and a ciphertext, C , to recover the original message, M .

6. The encryption and decryption functions can be applied in either order:

$$M = EK_{Ub}[DK_{Rb}(M)] = DK_{Ub}[EK_{Rb}(M)]$$

35. 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.

36. 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 f_k , such that

$Y = f_k(X)$ easy, if k and X are known

$X = f_k$

$-1(Y)$ easy, if k and y are known

$X = f_k$

$-1(Y)$ infeasible, if Y is known but k is not known

37. Define Euler's theorem and its application?

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

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

38. 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 ,

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

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

40. Define Fermat Theorem?

Fermat Theorem states the following: If p is prime and a is a positive integer not divisible by p , then

$$a^{p-1} \equiv 1 \pmod{p}$$

41. List four general characteristics of schema for the distribution of the public key?

The four general characteristics for the distribution of the public key are

1. Public announcement
2. Publicly available directory
3. Public-key authority
4. Public-key certificate

42. What is a public key certificate?

The public key certificate is that used by participants to exchange keys without contacting a public key authority, in a way that is as reliable as if the keys were obtained directly from the public-key authority. Each certificate contains a public key and other information, is created by a certificate authority, and is given to a participant with the matching private key.

43. 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.

44. Find gcd (1970, 1066) using Euclid's algorithm?

$$\text{gcd}(1970, 1066) = \text{gcd}(1066, 1970 \bmod 1066)$$

$$= \text{gcd}(1066, 904)$$

$$= 2$$

45. User A and B exchange the key using Diffie-Hellman algorithm. AVVXPH_

q=11 XA=2 XB=3. Find the value of YA, YB and k?

Soln: YA=_ X

$$A \bmod q$$

$$= 25 \bmod 11$$

$$= 3$$

$$YB_X$$

$$B \bmod q$$

$$= 125 \bmod 11$$

$$= 4$$

$$K = (YA) \times B \bmod q$$

$$= 27 \bmod 11$$

$$= 5$$

$$K = (YB) \times A \bmod q$$

$$= 16 \bmod 11$$

$$= 5$$

46. What is the primitive root of a number?

We can define a primitive root of a number p as one whose powers generate all

the integers from 1 to $p-1$. That is p , if a is a primitive root of the prime number p then the numbers.

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

Soln:

We know, $\gcd(a, b) = \gcd(b, a \bmod b)$ $\gcd(24140, 16762) = \gcd(16762, 7378)$ $\gcd(7378, 2006)$
 $= \gcd(2006, 1360)$ $\gcd(1360, 646) = \gcd(646, 68)$ $\gcd(68, 34) = 34$

$\gcd(24140, 16762) = 34$.

48. Perform encryption and decryption using RSA Alg. for the following, $P=7$; $q=11$; $e=17$; $M=8$.

Soln:

$$n = pq$$

$$n = 7 \times 11 = 77$$

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

$$= 6 \times 10 = 60 \quad e = 17$$

$$d = 27$$

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

$$C = 8^{17} \bmod 77$$

$$= 57$$

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

$$= 5727 \bmod 77$$

$$= 8$$

49. What is an elliptic curve?

The principle attraction of ECC compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead.

Unit III

50. 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.

51. 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.

52. What are the requirements for message authentication?

The requirements for message authentication are

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

2. 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.

3. 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.

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

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

6. 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.

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

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

53. 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.

54. 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.

55. Any three hash algorithm.

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

56. 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.

57. 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.

58. 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.

59. 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.

60. 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.

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

Weak collision resistance Strong resistance collision

For any given block x , it is computationally infeasible to find $y \neq x$ such that $H(x) = H(y)$

It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$

It is proportional to 2^n

It is proportional to $2^{n/2}$

62. 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 paired rounds of 16) Maximum

message size

.

264-1 bits

264-1 bits Primitive logical function

4

4

5

Additive constants used

64 4 9

Endianess Little Endian Big Endian Little Endian

63. Distinguish between direct and arbitrated digital signature?

Direct digital signature Arbitrated Digital Signature

The direct digital signature involves only the communicating parties.

The arbiter plays a sensitive and crucial role in this digital signature.

This may be formed by encrypting the entire message with the sender's private key.

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.

64. What are the properties a digital signature should have? $\frac{3}{4}$ It must verify the author and the data and time of signature. $\frac{3}{4}$ It must authenticate the contents at the time of signature. $\frac{3}{4}$ It must be verifiable by third parties to resolve disputes.

65. 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.

66. 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.

67. 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.

68. What 4 requirements were defined by Kerberos?

. _Secure . _Reliable . _Transparent . _Scalable

69. 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”.

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

Dialogue between client 'C' , server 'S' and authentication server(AS) are given below

a) C AS: [IDc|| Pc || IDs]

b) AS C: Ticket

c) C S: [IDc || ADc || IDs] Ticket = EKs [IDc ||ADc || IDs]

Step 1: The user logon to workstation and request access to the server S. The

client module C in the workstation request user password and sends message to AS that includes user ID(IDc), server ID(IDc) and its password.

Step 2: Now the AS verify users password against its password database, if it is valid. AS sends the ticket to C that includes user ID(IDc), server ID(IDs) and the address of the client workstation (ADc) are encrypted with key which is shared by both AS and server(S).

Step 3: Now the client use the ticket to server S, to send the message to S with IDc to access service.

71. 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.

Unit IV & 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-1 for 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. Draw the diagram for PGP message transmission reception?

8. What is the general format for PGP message?

9. 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.

10. What are the elements of MIME? 9_Five new message header fields are defined which may be included in an

RFC 822 header. 9_A number of content formats are defined. 9_Transfer encodings are defined that enable the conversion of any content

format into a form that is protected from alteration by the mail system.

11. What are the headers fields define in MIME?

MIME version. Content type.

Content transfer encoding. Content id.

Content description.

12. What is MIME content type and 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.

13. What are the key algorithms used in S/MIME?

Digital signature standards. Diffi Hellman.

RSA algorithm.

14. 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 .

15. What you mean by Verisign certificate?

Mostly used issue X.509 certificate with the product name "Verisign

digital id". Each digital id contains owner's public key, owner's name and serial number of the digital id.

16. What are the function areas of IP security?

Authentication Confidentiality Key management.

17. Give the application of IP security?

Provide secure communication across private & public LAN. Secure remote access over the Internet.

Secure communication to other organization.

18. 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.

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

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

20. Specify the IP security services?

Access control. Connectionless integrity. Data origin authentication

Rejection of replayed packet. Confidentiality.

Limited traffic for Confidentiality.

21. 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.

22. 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 sent the sequence number is incremented in the counter by the sender.

23. General format of IPsec ESP Format?

Security Parameter Index(SPI) Sequence Number(SN) Payload Data (Variable) Padding(0-255 bytes) Authentication Data (variable)

24. Differentiate Transport and Tunnel mode in IPsec?

25. What is Authentication Header? Give the format of the IPsec Authentication

Header?

It provides the authentication of IP Packet, so authentication is based on the use of MAC.

Format of IPsec Authentication Header: First Header Payload Length Reserved Security Parameter Index(SPI)

Sequence number(SN) Authentication Data(Variable)

26. Explain the format of ESP Transport Mode?

Authenticated

Encrypted

Orig IPhdr ESP

hdr

TCP DATA ESP Trlr

ESP

auth

Fig: IPV4

Authenticated Encrypted Orig IP

hdr

Hop by hop,dest,routing,fragment ESP

hdr

dest Tcp Data ESP

trir ESP auth

Fig:IPV6

Transport mode Tunnel Mode

1. Provide the protection for

upper layer protocol between two hosts.

2. ESP in this mode encrypts and optionally authenticates IP Payload but not IP Header.

3. AH in this mode authenticate the IP Payload and selected portion of IP Header.

1. Provide the protection for entire IP Packet.

2. ESP in this mode encrypt authenticate the entire IP packet.

3. AH in this mode authenticate the entire IP Packet plus selected portion of outer IP Header.

27. Define Transport Adjacency and Iterated Tunnel?

Transport Adjacency:

Apply authentication after encryption, two bundle transport mode Security

Association

o Inner SA (ESP_SA) o Outer SA(AH_SA) Iterated Tunnel:

Apply authentication before encryption, 2 SA are combined,

o Inner Sa-AH transport mode.

o Outer Sa-ESP Tunnel mode.

28. Give features and weakness of Diffie Hellman?

FEATURES:

Secret keys created only when needed. Exchange requires no preexisting infrastructure.

WEAKNESS: . _Provide no information about identities. . _It is subjected to man in middle attack.

29. 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 user ID based on the private key and Y. B compute the secret key and A compute k2 based on private key of A and Y.

30. List the steps involved in SSL record 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.

31. Give SSL record format?

Content type Major Version Minor Version

Compressed length

Plain Text(Optionaly Compressed) MAC

0, 16 or 20 bytes.

32. 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 the major version is 3 minor version is 1.

* SSL use HMAC alg., except that * TLS makes use of the same alg. the padding bytes concatenation.

* SSL supports 12 various alert * TLS supports all of the alert codes codes. defined in SSL3 with the exception of

no _ certificate.

33. 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

34. 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.

35. 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.

36. List the 3 classes of intruder?

Classes of Intruders

- 1) Masquerader
- 2) Miffeasor
- 3) Clandestine user

37. 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

38. 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.

39. List the design goals of firewalls?

1. All traffic from inside to outside, and vice 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.

Part B Unit I

1. i) Explain Playfair cipher & Vernam cipher in detail. Playfair cipher

i) Multiple letter encryption cipher ii) Example

iii) Four Rules

Vernam Cipher

i) Encryption $C_i = P_i \oplus K_i$ ii) Decryption $P_i = C_i \oplus K_i$ iii) Example

ii) Convert “MEET ME” using Hill cipher with the key matrix

Convert the ciphertext back to plaintext.

2. Explain simplified DES with example.

Structure of S-DES Functions

Key Generation

Encryption –Block Diagram

3. Write short notes on i) Steganography

Definition

Historical Techniques Advanced Techniques Drawbacks

ii) Block cipher modes of operation

Electronic Code book mode Cipher block chaining mode Cipher feedback mode Output feedback mode

4. Explain classical Encryption techniques in detail. Substitution techniques

o Caesar cipher

o Playfair Cipher

o Hill Cipher

o Monoalphabetic Cipher

o Polyalphabetic cipher

Transposition Techniques

5. Write short notes on

a. **Security services** Definition Confidentiality Authentication Integrity

Non Repudiation Access Control Availability

b. Feistel cipher structure

Block diagram

Explanation of Encryption and Decryption Process

Design Parameters

6. Explain Data Encryption Standard (DES) in detail.

Block diagram

Details of Single Round Calculations of F(R, K) Key Generation

DES Decryption

7. How AES is used for encryption/decryption? Discuss with example.

AES Parameters Structure of AES AES Key Expansion

8. List the evaluation criteria defined by NIST for AES.

Security

Cost

Algo. And Implementation characteristics

Final-9 points

Unit II

1. State and explain the principles of public key cryptography.

Problems in CE Characteristics Elements

2. Explain Diffie Hellman key Exchange in detail with an example

Algorithm

Example

3. Explain the key management of public key encryption in detail

Public Key announcement Publicly available directory Public key Certification Public Key Authority

Simple Secret Key Distribution

Secret Key Distribution with confidentiality and authentication

Hybrid Scheme

4. Explain RSA algorithm in detail with an example

Requirements

Algorithm

Example

Computational Aspects

Security of RSA

5. Briefly explain the idea behind Elliptic Curve Cryptosystem.

EC over Real No and \mathbb{Z}_p ECC DH Key Exchange EC E/D

Security of ECC

Unit III

1. Explain the classification of authentication function in detail

Introduction Message Encryption MAC

Hash function

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

512 bit block size produces 128 bit MD Processing steps

Compression function

Comparison

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

512 bit block size produces 160 bit MD Processing steps

Compression function

Comparison and advantages

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

512 bit block size produces 160 bit MD Processing steps

Compression function

Comparison

5. Describe HMAC algorithm in detail.

Algorithm Structure Security

6. Write and explain the Digital Signature Algorithm.

Signature = (r,s)

Verify $v = r'$ Algorithm Block diagram

7. Assume a client C wants to communicate with a server S using kerberos protocol. How can it be achieved?

Introduction

Simple Authentication Dialogue

Secure Authentication Dialogue

Unit IV

1. Explain the operational description of PGP

Authentication Confidentiality Compression

Email Compatibility

Segmentation

2. Write Short notes on S/MIME

MIME Elements Functionality Algorithms MIME Messages

Certificate Processing

3. Explain the architecture of IP Security

Introduction

IP Sec. Documents IP Sec. Services Security Association

4. Write short notes on authentication header and ESP

Authentication header format

Anti replay service Transport and tunnel mode ESP format

ESP Encryption and Authentication

Combined Security Association

5. Explain in detail the operation of Secure Socket Layer in detail.

SSL concepts

SSL Record protocol operation

Logical connection between client and server

6. Explain Secure Electronic transaction with neat diagram.

Introduction

Services

Requirements and features

Participants Sequence of even Dual signature Payment processing

Unit V

1. Explain the technical details of firewall and describe any three types of firewall with neat diagram

Pack filtering router Application level gateway Circuit level gateway

2. Write short notes on Intrusion Detection.

Intrusion Techniques Statistical anomaly detection Rule based detection Distributed Intrusion Detection

3. Define virus. Explain in detail.

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.

Nature of viruses – 4 phases

Virus Structure Types of viruses Antivirus Approaches

4. Describe Trusted system in detail.

Access control structure

Reference Monitor concept

5. Explain in detail about password management.

Password protection Loading a new password Verifying a password

Password selection strategies

CS6701 CRYPTOGRAPHY AND NETWORK SECURITY 16 MARKS

UNIT 1

Question Bank

Part-B (16 Marks)

1. (i) Discuss any four Substitution Technique and list their merits and demerits. (10)

(ii) Explain in detail Transposition Technique? (6)

2. Write short notes on

(i). Security attacks (8)

(ii). Security services. (8)

3. (i) Convert "MEET ME" using Hill cipher with the key matrix

Convert the cipher text back to plaintext (8)

17	17	5
21	18	21
2	2	19

(ii) Explain in detail the Legendre and Jacobi symbols.

4. (i) Briefly explain the design principles of block cipher. (8) (ii) Discuss in detail block cipher modes of operation. (8)

5. Write short notes on

(i) Fermat and Euler's theorem (8)

(ii) Chinese Remainder theorem (8)

Unit-II

Part-B (16 Marks)

1. (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)

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

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

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

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

4. (i) Describe about RC4 algorithm. (8) (ii) Explain the Miller-Rabin Algorithm. (8)

Unit-III

Part-B (16 Marks)

1. (i) Briefly explain Diffie Hellman key exchange with an example. (16)
 2. (i) Write and explain the digital signature algorithm. (8) (ii) Explain in detail Hash Functions. (8)
 3. (i) Compare the Features of SHA-1 and MD5 algorithm. (8)
(ii) Discuss about the objectives of HMAC and its security features. (8)
 4. Users A and B use the Diffie Hellman key exchange technique, a common prime $q=11$ and a primitive root $\alpha=7$.
(i) If user A has private key $X_A=3$. What is A's public key Y_A ? (4)
(ii) If user B has private key $X_B=6$ What is B's public key Y_B ? (4) (iii) What is the shared secret key? Also write the algorithm. (4)
(iv) How many in the middle attack can be performed in Diffie Hellman algorithm. (4)
 5. (i) Explain in detail ElGamal Public key cryptosystem. (8)
(ii) Discuss clearly Secure Hash Algorithm (SHA) (8)
 6. Describe the MD5 message digest algorithm with necessary block diagrams. (16)
-

Unit-IV

Part-B (16 Marks)

1. How does PGP provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components. (16)
 2. Write Short notes on S/MIME .
 3. Explain the architecture of IP Security (16)
 4. (i) Describe the SSL Specific protocol – Handshake action in detail. (8)
(ii) Explain Secure Electronic transaction with neat diagram. (8)
 5. (i) What is Kerberos? Explain how it provides authenticated service. (8)
(ii) Explain the format of the X.509 certificate. (8)
-

Unit-V

Part-B (16 Marks)

1. (i) Explain any two approaches for intrusion detection. (8) (i) Identify a few malicious programs that need a host program for their existence.(8)
2. (i) Explain firewalls and how they prevent intrusions. (8) (ii)List and Brief, the different generation of antivirus software (8)
3. (i) Define intrusion detection and the different types of detection mechanisms, in detail. (8)
4. (i)Explain the types of Host based intrusion detection. List any two IDS software available. (8)
(ii) What are the positive and negative effects of firewall? (8)
5. (i) Describe packet filtering router in detail. (16)
6. Describe the familiar types of firewall configurations. (16)