CRYPTOGRAPY AND NETWORK SECURITY – CS 8792

UNIT 1 - INTRODUCTION

2MARKS

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

~ Secret key

~ Cipher text

~ Decryption algorithm

7. Describe security mechanism.

• 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 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 riginal plaintext.

10. Specify four categories of security threats

- Interruption

- Interception
- Modification
- Fabrication

16 MARKS

1. State and Describe

(1) Fermat's theorem. (8)

(2) Euler's teorem. (8)

2. (i) Tabulate the substitution Techniques in detail. (12)

(ii) Describe the Transposition Techniques in detail. (4)

3. (i) List the different types of attacks and explain in detail.(8)

(ii) Describe in detail about the types of cryptanalytic attack. (8)

4. (i) Evalute3^21 mod 11 using Fermat's theorem. (6)

(ii) State Chinese Remainder theorem and find X for the given set of congruent

equations using CRT. (10)

X=2(mod 3)

X=3(mod 5)

X=2(mod 7)

UNIT 2 -SYMMETRIC KEY CRYPTOGRAPHY

2MARKS

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 th 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.

16MARKS

1. Explain in detail about working of DES encryption and decryption

- Definition

- Encryption- Diagram
- Initial Permutation
- Details of Single Round- diagram , S-box
- decryption

2. Explain in detail about working of AES

Definition

Structure – diagram and its explanation (10 pt)

Transformation function

3. Explain in detail about AES key expansion

4. Explain briefly about the block cipher modes of operations

Diagram , adv and disadv for each

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

UNIT 3 - PUBLIC KEY CRYPTOGRAPHY

2MARKS

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(2m) = 2m/2 attempts

7. List the processing logic of SHA-512

1. Append padding bits

2. Append padding length

3. Initialize hash buffer

4. Process message in 1024 bits(128-words) blocks

5. 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

9. 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

10. List any three hash algorithm.

- MD5(message Digest version 5) algorithm
- SHA_1 (Secure Hash algorithm)
- RIPEMD_160 algorithm

16 MARKS

1. Describe Secure hash Algorithm in detail. (16)

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

3. (i)Summarize CMAC algorithm and its usage.(8)

(ii)Describe any one method of efficient implementation of HMAC. (8)

4. Describe digital signature algorithm and show how signing and verification is done using DSS. (16)

5. Explain in detail ElGamal Digital Signature scheme with an example. (16)

UNIT IV - MESSAGE AUTHENTICATION AND INTEGRITY

2MARKS

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?

- Secure
- Reliable
- Transparent
- 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:

- 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”.

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

- Masquerader
- Misfeasor
- Clandestine user

7. 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:

- Parasitic virus
- Memory-resident virus
- Boot sector virus
- Stealth virus
- Polymorphic virus
- Metamorphic 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?

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

10. What are the steps involved in SET Transaction?

- The customer opens an account
- The customer receives a certificate
- Merchants have their own certificate

- The customer places an order.
- The merchant is verified.
- The order and payment are sent.
- The merchant requests payment authorization.
- The merchant confirm the order.
- The merchant provides the goods or services.
- The merchant requests payment

16 MARKS

1. What is Kerberos? Explain how it provides authenticated service.

2. Explain the format of the X.509 certificate.

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

4. Write short notes on Intrusion Detection.

5. Define virus. Explain in detail.

6. Explain Secure Electronic Transaction with neat diagram.

7. What is a trusted system? Explain the basic concept of data access control in trusted systems. (8)

UNIT V - SECURITY PRACTICE AND SYSTEM SECURITY

2MARKS

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

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.

16 MARKS

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)