QUESTION BANK

UNIT-I

PART A (2 MARKS)

1. What is Cryptology?

The study of secure communications, which encompasses both cryptography and cryptanalysis.

2. Define Cryptography.

The branch of cryptology dealing with the design of algorithms for encryption and decryption, intended to ensure the secrecy and/or authenticity of messages.

3. Define Cryptanalysis.

The branch of cryptology dealing with the breaking of a cipher to recover information, or forging encrypted information that will be accepted as authentic.

4. What is Plain text?

An original message is known as the **plaintext (Readable format)**

5. What is Cipher Text?

Coded message is called the **Cipher Text.(Unreadable format)**

6. What is Key?

A sequence of symbols that controls the operation of a cryptographic transformation. A key is normally a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa. The key should be the only part of the algorithm that it is necessary to keep secret.

7. What is Symmetric Cryptography?

Symmetric cryptography uses a single private key to both encrypt and decrypt data.

Examples: AES/Rijndael ,Blowfish,CAST5, DES,IDEA,RC2,RC4,RC6,Serpent,Triple DES, Two fish

8. What is Asymmetric Cryptography?

Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message .The keys used are public and private key.

Examples: RSA,DSA,PGP

9. Define Stream cipher.

Processes the input stream continuously and producing one element at a time.

Example: caeser cipher.

10. Define Block cipher.

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

Example: DES.

11. What is Passive attack?

Monitoring the message during transmission.
Eg: Interception

12.What is Active attack:

Modification of data stream or creation of false data stream.
E.g.: Fabrication, Modification, and Interruption

13. List the different Types of Ciphers.

- Shift Ciphers.
- Affine Ciphers
- Vigenere Cipher
- Substitution Ciphers
- Sherlock Holmes
- Playfair and ADFGX Ciphers
- Block ciphers
- One-Time pads

14. Write short notes Congruence.

Let a,b,n be integers with $n \neq 0$. We say that $a \equiv b(\text{mod } n)$

If a-b is a multiple of n.

15. Write short notes Chinese Remainder Theorem:

Suppose gcd(m,n)=1.Given integers a and b, there exists exactly one solution x(mod mn) to the simultaneous congruence $x \equiv a(\text{mod } n)$, $x \equiv b(\text{mod } n)$.

16. Write short notes Modular Exponentiation:

Modular exponentition is of the form x^a (mod n).

17. Write short notes Fermat's Little Theorem:

If p is aprime and p does not divide a, then

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

18.Write short notes Euler's Theorem:

If gcd(a,n)=1, then

$$a^{\Phi(n)} \equiv 1(\bmod n)$$

19. 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.

20. 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.

PART B(16 MARKS)

1. Explain the followings:
(a) Playfair cipher.
(b) Vernam cipher in detail.
2. Write short notes on i) Steganography
3. Explain classical Encryption techniques in detail.
4. Write short notes on
(a) Security services
(b) Feistel cipher structure
5. Explain the OSI security architecture
6. a. Explain various transposition ciphers in detail

b.Explain in detail about various types of attacks.

7. Write short notes on
   (i)Fermat and Euler's theorem
   (ii)Chinese Remainder theorem
8. Discuss with neat sketch a network security model.
9. Explain the Miller-Rabin algorithm

UNIT-II

PART A(2 MARKS)

1. What is Avalanche effect ?

A characteristic of an encryption algorithm in which a small change in the plaintext or key gives rise to a large change in the cipher text.

2. 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

3. List the step involved in single Round of AES.

1.Substitute byte transformation 2. Shift rows transformation
3.Mixcolumns transformation 4.Add Round Key transformation

4. Define Substitute byte transformation and Shift rows transformation.

Substitute byte transformation, called SubBytes, is a simple table lookup. AES defines a 16 x 16 matrix of byte values, called an S-box that contains a permutation of all possible 256 8-bit values. Each individual byte of State is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value. These row and column values serve as indexes into the S-box to select a unique 8-bit output value.

Shift row transformation, called Shift Rows, the first row of State is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2-byte circular left shift is performed. For the fourth row, a 3-byte circular left shift is performed.

5. Define Mixcolumns transformation & Add Round Key transformation.

Mix column transformation, called MixColumns, operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column.

Add round key transformation, called AddRoundKey, the 128 bits of State are bitwise XORed with the 128 bits of the round key.The operation is viewed as a column wise operation between the 4 bytes of a State column and one word of the round key; it can also be viewed as a byte-level operation.

6. What is Primality Test?

A primality test is an algorithm for determining whether an input number is prime or not.

7. List the types of Primality Testing.

1. Fermat Primality Test.
2. Miller-Rabin Primality Test.
3. Solovay-strassen Primality Test.

8. What is Factoring ?

Factoring is the decomposition of an object into a product of other objects, or factors, which when multiplied together give the original.

9. Define RC4.

RC4 is a stream cipher designed in 1987 by Ron Rivest for RSA Security. RC4 is used in the SSL/TLS (Secure Sockets Layer/Transport Layer Security) standards that have been defined for communication between Web browsers and servers. It is also used in the WEP (Wired Equivalent Privacy) protocol and the newer WiFi Protected Access (WPA) protocol that are part of the IEEE 802.11 wireless LAN standard.

9. Define RSA.

RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography.

11. List Four possible approaches to attack the RSA Algorithm.

1. Brute Force
2. Mathematical Attacks
3. Timing attacks
4. Chosen Cipher text attacks

12. 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.

13. 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.

14. Define Differential Cryptanalysis.

A technique in which chosen plaintext with particular XOR difference patterns are encrypted. This difference pattern of the resulting ciphertext provide information that can be used to determine the encryption key.

15. List the Block cipher Modes of operation.

1. Electronic Codebook (ECB)
2. Cipher Block Chaining (CBC)
3. Cipher Feedback (CFB)
4. Output Feedback (OFB)
5. Counter (CTR)

16. List the description and application Electronic Codebook.

Each block of 64 plaintext bits is encoded independently using the same key.
Application: Secure transmission of single values (e.g., an encryption key)

17. List the description and application Cipher Block Chaining (CBC)

The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.

Application: General-purpose block-oriented transmission Authentication

18. List the description and application Cipher Feedback (CFB)

Input is processed j bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.

Application: General-purpose stream-oriented transmission Authentication

19. List the description and application Output Feedback (OFB)

Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.

Application: Stream-oriented transmission over noisy channel (e.g., satellite communication)

20. List the Advantages of counter mode:

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

PART B(16 MARKS)

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.
7. How AES is used for encryption/decryption? Discuss with example.
8. Explain Double &Triple DES with keys.
9. Explain the block cipher modes of operation.
10. Write about elliptic curve architecture in detail and how they are useful for cryptography.
11. Write about key distribution in detail.
12. (i) Identify the possible threats for RSA algorithm and list their counter measures.
    (ii) Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and N=5.
13. (i) Describe about RC4 algorithm.
    (ii) Describe about Blowfish algorithm

UNIT-III

PART A(2 MARKS)

1. Define Hash Function.

A function that maps a variable-length data block or message into a fixed-length value called a hash code. The function is designed in such a way that, when protected, it provides an authenticator to the data or message. Also referred to as a message digest (or) Hash code.

2. List the Hash Algorithms.

- SHA(Secure Hash Algorithm)
- MD5(Message Digest Version5)

3. Write Short notes on MD5.

The MD5 Message-Digest Algorithm is a widely used cryptographic hash function that produces a 128- bit (16-byte) hash value. MD5 has been employed in a wide variety of security applications, and is also commonly used to check data integrity. MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. An MD5 hash is typically expressed as a 32-digit hexadecimal number.

4. Write Short notes on SHA(Secure Hash Algorithm).

The Secure Hash Algorithm is one of a number of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS).

5. What is Digital Signature?

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

6. List the Digital Signature Algorithms.

- RSA
- ElGamal
- DSA

7. List the Processes involved in Digital Signature.

- Signing Process
- Verification Process

8. 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.

9. What is Birthday attack ?

This cryptanalytic attack attempts to find two values in the domain of a function that map to the same value in its range.

10. What is Discrete Logarithms?

Discrete logarithms are fundamental to a number of public-key algorithms, including Diffie-Hellman key exchange and the digital signature algorithm.

11. List the approaches of Computing Discrete Logarithms.

- Pohlig Hellman Algorithm
- Baby-step Giant-step
- Index calculus algorithm

12. What is 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.

13. What is the purpose of using Diffie-Hellman Key Exchange?

The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages.

14.User A and B exchange the key using Diffie-Hellman algorithm. Assume α=5 q=11 XA=2 XB=3. Find the value of YA,YB and k?

Soln:

YA= αXA mod q= 25 mod 11 = 3

YB = αXB mod q= 125 mod 11 = 4

K = (YB) XA mod q= 16 mod 11 = 5

15.Define ElGamal Public Key Cryptosystem.

ElGamal Public Key Cryptosystem is an asymmetric key encryption for public key cryptography based on Diffie-Hellman Key Exchange.

16. Difference between MD5 and SHA-1.

Point of Discussion	**MD5**	**SHA-1**
1.Message digest length in bits	**128**	**160**
2.Speed	**Faster(64 iterations)**	**Slower(80 iterations)**
3.Attack to try and find two messages producing the same message digest	**Requires 2^{64} operations to break in.**	**Requires 2^{80} operations to break in.**

17. 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.

18. Using ElGamal Scheme, let α = 5, p =11, XA= 2. Find the value of YA?

α = 5, p =11, XA= 2

$$YA = \alpha^{XA}\text{mod } p$$

$$= 52 \text{ mod } 11$$

19. **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.

20. **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.

PART B(16 MARKS)

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 discuss its advantages.
4. Describe HMAC algorithm in detail.
5. Write and explain the Digital Signature Algorithm.
6. (i)Explain in detail Hash Functions. (8)
   (ii)Compare the Features of SHA-1 and MD5 algorithm. (8)
7. (i)Explain in detail EIGamal Public key cryptosystem. (8)
   (ii)Discuss clearly Secure Hash Algorithm(SHA) (8)
8. Describe the MD5 message digest algorithm with necessary block diagrams.

UNIT-IV

PART A(2 MARKS)

1. What is Kerberos?

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.

2. What 4 requirements were defined by Kerberos?

- Secure
- Reliable
- Transparent
- Scalable

3. Define X.509 Authentication Service.

X.509 is part of the X.500 series. X.509 define a directory service. X.509 is based on the use of public-key cryptography and digital signatures. X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. For example, the X.509 certificate format is used in S/MIME, IP Security , and SSL/TLS and SET .

4. Define Public-Key Infrastructure.

Public-key infrastructure (PKI) as the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.

5. Define PGP.

Pretty Good Privacy is an open-source freely available software package for e-mail security. It provides authentication through the use of digital signature; confidentiality through the use of symmetric block encryption; compression using the ZIP algorithm; e-mail compatibility using the radix-64 encoding scheme; and segmentation and reassembly to accommodate long e-mails.

6. Define S/MIME

Secure/Multipurpose Internet Mail Extension is an Internet standard approach to e-mail security that incorporates the same functionality as PGP.

7. Write short notes on IP Security.

IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.

8. Write short notes on Web Security:

Secure socket layer (SSL) provides security services between TCP and applications that use TCP. The Internet standard version is called transport layer service (TLS).

9. Write short notes on Secure Electronic Transaction .What are the features of SET?

Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transactions on the Internet.

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication

10. Write short notes on Transport Layer Security(TLS) ?

Transport Layer Security is defined as a Proposed Internet Standard in RFC 2246. RFC 2246 is very similar to SSLv3. The TLS Record Format is the same as that of the SSL Record Format, and the fields in the header have the same meanings. The one difference is in version number.

11. What are the function areas of IP security?

Authentication
Confidentiality
Key management.

12. Differentiate Transport and Tunnel mode in IPsec?

Transport mode	Tunnel Mode
1. Provide the protection for upper layer protocol between two hosts.	1. Provide the protection for entire IP Packet.
2. ESP in this mode encrypts and optionally authenticates IP Payload but not IP Header.	2. ESP in this mode encrypt authenticate the entire IP packet.
3. AH in this mode authenticate the IP Payload and selected portion of IP Header.	3. AH in this mode authenticate the entire IP Packet plus selected portion of outer IP Header.

13. 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.

14. **What does you mean by Reply Attack?**

- A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination.
- Each time a packet is send the sequence number is incremented in the counter by the sender.

15. Name any cryptographic keys used in PGP?

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

16. **Define Certification authority.**

The issuer of certificates and certificate revocation lists (CRLs). It may also support a variety of administrative functions, although these are often delegated to one or more Registration Authorities.

17. List the Applications of IPSec.

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establishing extranet and intranet connectivity with partners
- Enhancing electronic commerce security

18. What do you mean by 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).

19. Specify the parameter that identifies the Security Association?

A security Association is uniquely identified by 3 parameters:

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

20. What are the headers fields define in MIME?

- MIME version.
- Content type.
- Content transfer encoding.
- Content id.
- Content description.

PART B(16 MARKS)

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. Define virus. Explain in detail.
7. Describe trusted system in detail.
8. Explain any two approaches for intrusion detection.
9. Explain firewalls and how they prevent intrusions.
10. Define intrusion detection and the different types of detection mechanisms, in detail.
11. Explain the types of Host based intrusion detection. List any two IDS software available.
12. Describe the familiar types of firewall configurations.

UNIT-V

PART A(2 MARKS)

1. Define Intruder

An individual who gains, or attempts to gain, unauthorized access to a computer system or to gain unauthorized privileges on that system.

2. List Classes of Intruders.

- Masquerader
- Misfeasor
- Clandestine user

3. Write short notes on Intrusion detection system

A set of automated tools designed to detect unauthorized access to a host system.

4. Write short notes on Malicious software.

Malicious software is software that is intentionally included or inserted in a system for a harmful purpose.

5. Write short notes on Virus.

A virus is a piece of software that can "infect" other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs.

6. Write short notes on Worm.

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

7. Define Statistical anomaly detection.

Involves the collection of data relating to the behavior of legitimate users over a period of time.

Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.

8. Define Threshold detection.

This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.

9. Define Profile based.

A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

10. Define Rule-based detection.

Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

11. Define Anomaly detection.

Rules are developed to detect deviation from previous usage patterns.

12. Define Penetration identification.

An expert system approach that searches for suspicious behavior.

13. Define Honeypot .

A decoy system designed to lure a potential attacker away from critical systems. A form of intrusion detection.

14. What is Zombie?

A program that secretly takes over another Internet-attached computer and then uses that computer to launch attacks that are difficult to trace to the zombie's creator.

15. What is Denial of Service?

A denial of service (DoS) attack is an attempt to prevent legitimate users of a service from using that service.

16. Define Firewall.

A firewall is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access.

17. List the types of Firewall:

1.Packet Filtering Router
2.Application-Level Gateway
3.Circuit-Level Gateway

18. List the Firewall Configuration.

1. Screened host Firewall System(single homed bastion system)
2. Screened host Firewall System(Dual homed bastion system)
3. Screened Subnet Firewall System

19. What is Trusted System?

A trusted system is a computer and operating system that can be verified to implement a given security policy. Typically, the focus of a trusted system is access control.

20. List the types of Viruses:

- parasitic virus
- memory-resident virus
- boot sector virus
- stealth virus
- polymorphic virus
- metamorphic virus.

PART B(16 MARKS)

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