K.S.R. COLLEGE OF ENGINEERING: TIRUCHENGODE – 637 215.
(AUTONOMOUS)
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
COURSE / LESSON PLAN SCHEDULE (2018-19)
16EC662 CRYPTOGRAPHY AND NETWORK SECURITY (ELECTIVE)
NAME: Mr.K.KARUPPANASAMY CLASS: B.E/ III-ECE-A,B

A). TEXT BOOKS:

1. William Stallings, "Cryptography and Network Security - Principles and Practices", Pearson Education, 5th edition, 2011.
2. Behrouz A. Foruzan, "Cryptography and Network Security", Tata McGraw Hill, 2nd edition, 2011.

B). REFERENCES:

1. Wade Trappe and Lawrence C. Washington, "Introduction to Cryptography with Coding theory", Pearson Education, 2nd edition, 2007.
2. Wenbo Mao, "Modern Cryptography Theory and Practice", Pearson Education, 2007.

C). LEGEND:

L - Lecture
Tx - Text
OHP - Over Head Projector
Rx - Reference
PPT - Power Point
BB - Black Board
pp - Pages

S.No.	Lecture Hour	Topics to be covered	Teaching Aid Required	Book No. / Page No.
UNIT – I SYMMETRIC CIPHERS				
1.	L 1	OSI security architecture	BB	Tx1/pp 38-39
2.	L 2	Classical encryption techniques: Symmetric cipher model, Substitution techniques	BB	Tx1/pp 55-77, Rx2/pp 243-250
3.	L 3	Transposition techniques	BB	Tx1/pp 77-79, Rx2/pp 251-252
4.	L 4	Rotor Machines, Steganography	BB+PPT	Tx1/pp 79-82
5.	L 5	Block cipher principles	BB	Tx1/pp 92-101
6.	L6	Data encryption standard , Block cipher design principles	BB+PPT	Tx1/pp 101-109.116-120 Tx2/pp 143-171, Rx1/pp 113-143, Rx2/pp 256-260,
7.	L 7	Advanced encryption standard: Structure	BB	Tx1/pp 174-179, Rx1/pp 151-164 Rx2/pp 260-281
8.	L 8	Transformation function	BB	Tx1/pp 179-190, Tx2/pp 179-188
9.	L9	Key expansion, **XTS-AES modes for block oriented storagr devices**	BB	Tx1/pp 190-193,234-238 Tx2/pp 188-193
UNIT – II ASYMMETRIC CIPHERS				
10.	L 10	Introduction to number theory	BB+PPT	Tx1/pp 267-286, Rx2/pp 213-238
11.	L 11	Fermat's and Euler's Theorem	BB	Tx1/pp 272-275
12.	L 12	Testing for premality	BB	Tx1/pp 275-278
13.	L 13	Public key cryptography: Principles of public key cryptosystems	BB	Tx1/pp 290-301
14.	L14	RSA algorithms	BB	Tx1/pp 301-315, Tx2/pp 272-283 Rx1/pp 164-169, Rx2/pp 295-298 Rx2/pp 311-313
15.	L 15	Diffie-Hellman key exchange	BB+PPT	Tx1/pp 325-329, Rx1/pp 210-212 Rx2/pp 287-295
16.	L 16	Elgamal cryptographic system	BB	Tx1/pp 329-332, Rx1/pp 212-214

17.	L 17	Elliptic curve arithmetic	BB+PPT	Tx1/pp 332-341
18.	L18	Elliptic curve cryptography, **Pseudo random number generation based on Asymmetric cipher**	BB	Tx1/pp 341-344,345-347 Tx2/pp 290-297, Rx1/pp 363-366
UNIT – III CRYPTOGRAPHIC DATA INTEGRITY ALGORITHMS				
19.	L19	Cryptographic hash functions: Applications	BB	Tx1/pp 353-357, Rx2/pp 338-342
20.	L20	Two simple hash function	BB	Tx1/pp 357-359
21.	L21	secure hash algorithm	BB+PPT	Tx1/pp 366-376
22.	L22	SHA-3	BB+PPT	Tx1/pp 376-377
23.	L23	Message authentication codes: Requirements	BB+PPT	Tx1/pp 388, Tx2/pp 316-321
24.	L24	Functions	BB	Tx1/pp 389-396
25.	L25	Security of MAC	BB	Tx1/pp 398-399
26.	L26	HMAC, CMAC	BB	Tx1/pp 399-404
27.	L27	Digital signatures, Authenticated **Encryption:CCM and GCM**	BB	Tx1/pp 420-424,407-413 Tx2/pp 357-377, Rx1/pp 244-252
UNIT – IV NETWORK AUTHENTICATION				
28.	L 28	Key management: Symmetric key distribution using symmetric	BB+PPT	Tx1/pp 437-446
29.	L 29	Asymmetric encryption	BB	Tx1/pp 446-448
30.	L 30	X.509 certificates	BB+PPT	Tx1/pp 453-461 Rx1/pp 271-277
31.	L 31	Authentication: Remote user authentication principles	BB	Tx1/pp 469-472
32.	L 32	Remote user authentication using symmetric	BB	Tx1/pp 472-476
33.	L 33	Remote user authentication using asymmetric encryption	BB	Tx1/pp 494-496
34.	L 34	Kerberos	BB	Tx1/pp 476-494, Tx2/pp 407-410 Rx1/pp 266-270, Rx2/pp 448-454
35.	L 35	Secure socket layer security	BB	Tx1/pp 513-526
36.	L 36	Secure transport layer security, **Federated Identity Management**	BB	Tx1/pp 526-530, 496-502
UNIT – V ADVANCED NETWORK CONCEPTS				
37.	L 37	Electronic mail security: Pretty good privacy	BB+PPT	Tx1/pp 591-592, Tx2/pp 429- 451 Rx1/pp 277-280
38.	L 38	S/MIME, domain keys identified mail	BB+PPT	Tx1/pp 611-627, Tx2/pp 452-459
39.	L39	IP Security: IP security overview	BB	Tx1/pp 640-646
40.	L40	IP security policy and encapsulating security payload	BB	Tx1/pp 646-658
41.	L 41	Intrusion detection	BB	Tx2/pp 556-558
42.	L 42	Firewall design principles	BB	Tx2/pp 559-564
43.	L 44	Wireless network security: Wireless application security overview	BB	Tx1/pp 567-574
44.	L 45	Wireless transport layer security, **Internet Key Exchange**	BB	Tx1/pp 574-584,662-671

Unit I - SYMMETRIC CIPHERS (CO1)

PART –A (2 MARKS)

1. Give the difference between active attack and passive attack.(U)

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis.

2. What are the 3 aspects of security?(R)

- Security Attack
- Security Mechanism
- Security Service

3. Define Security attacks. (U)

Security attack: Any action that compromises the security of information owned by an organization.

4. Define security mechanism.(U)

Security mechanism: A process that is designed to detect, prevent, or recover from a security attack

5. Define Security service. (U)

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.

6. Define the cryptanalysis and cryptography.(U)

Cryptology is the study of techniques for ensuring the secrecy and/or authenticity of information. The two main branches of cryptology are cryptography, which is the study of the design of such techniques; and cryptanalysis, which deals with the defeating such techniques, to recover information, or forging information that will be accepted as authentic.

7. Define Steganography. (U)

It is the process of hiding the message into some cover media. It hides the existence of a message. Ex: Character marking, Pin punctures, Invisible ink etc

8. What are the two basic functions used in encryption algorithms?

The two basic functions used in encryption algorithms are

- Substitution
- Transposition

9. Compare Substitution and Transposition techniques.(AN)

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

Transposition techniques means, different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. Eg: DES, AES.

10. Define Threat and attack. (NOV2009)(U)

Threat is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm. Attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

11. What are the two approaches to attacking a cipher?(R)

The two approaches to attack a cipher are: 1.Cryptanalysis 2.Brute-force attack

12. Define Brute-force attack. (U)

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

13. What is Modification of messages.(R)

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.

14. What is masquerade? (R)

A masquerade takes place when one entity pretends to be a different entity. For example, authentication sequences can be captured and replayed after a valid authentication sequence has

taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges

15. What is Reply? (R)

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

16. Define Denial of service.(U)

Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance

17. List out the components of encryption algorithm. (U)

1. Plaintext 2. Encryption algorithm 3. Secret key 4. Cipher text 5.Decryption algorithm

18. List out the components of encryption algorithm. (U)

1. Plaintext 2. Encryption algorithm 3. Secret key 4. Cipher text 5.Decryption algorithm

19. Specify the four categories of security threads?(R)

- Interruption
- Interception
- Modification
- Fabrication

20. Define integrity. (U)

It assures that the data received is sent by an authorized entity and are not modified/replayed/deleted/updated

21. Define Non repudiation. (U)

It is the process which protects against denial by one of the parties in a communication. It can be obtained through the use of digital signature, time stamps etc,.

22. Differentiate symmetric and asymmetric encryption?(AN)

Symmetric: It is a form of cryptosystem in which encryption and decryption performed using the same key. Asymmetric: It is a form of cryptosystem in which encryption and decryption performed using two keys. Eg: DES, AES Eg: RSA, ECC

23. Compare stream cipher with block cipher with example.(AN)

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.

24. Convert the Given Text "CRYPTOGRAPHY" into cipher text using Rail fence Technique.(AP)

In rail fence technique the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. CYTGAH RPORPY The cipher text is CYTGAH RPORPY.

25. What are the different modes of operation in DES? (APR 2011 , APR 2017) (R)

Electronic Code Book (ECB) Cipher Block Chaining (CBC) Cipher Feedback (CFB) Output Feedback (OFB) Counter Mode

26. Write down the purpose of S-Boxes in DES? (NOV 2011)(R)

Each row of a S-box defines a general reversible substitution. It consists of a set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.

27. What is the difference between diffusion and confusion?(NOV 2011)(R)

In diffusion, the statistical structure of the plain text is dissipated into long-range statistics of the cipher text. This is achieved by permutation. In confusion, the relationship between the statistics of the cipher text and the value of the encryption key is made complex. It is achieved by substitution.

28. What is the difference between differential and linear cryptanalysis?(APR 2012)(R)

Differential cryptanalysis is the first published attack that is capable of breaking DES in less than encryptions. Linear Cryptanalysis method can find a DES key given known 243plaintexts, as compared to247chosen plaintexts for differential cryptanalysis

29. **What are disadvantages of double DES? (NOV 2012)(R)**

Reduction to a single stage. Meet in the middle attacks.

30. What is an avalanche effect? (NOV 2012)(R)

It is that a small change in either the plaintext or the key should produce a significant change in the cipher text.A change in one of the bit of the plaintext or one bit of the key should produce a change in many bits of the cipher text

31. What are the design parameters of Feistel cipher network?(R)

- Block size
- Key size
- Number of Rounds
- Sub key generation algorithm
- Round function
- Fast software Encryption/Decryption
- Ease of analysis

32. What is Data Encryption Standard?(R)

In Data Encryption Standard, data are encrypted in 64-bit blocks using a 56-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption.

33. What are the criteria for the design of s boxes?(R)

- No output bit of any S-box should be too close a linear function of the input bits. Specifically, if we select any output bit and any subset of the six input bits, the fraction of inputs for which this output bit equals the XOR of these input bits should not be close to 0 or 1, but rather should be near 1/2.
- Each row of an S-box (determined by a fixed value of the leftmost and rightmost input bits) should include all 16 possible output bit combinations.
- If two inputs to an S-box differ in exactly one bit, the outputs must differ in at least two bits.
- If two inputs to an S-box differ in the two middle bits exactly, the outputs must differ in at least two bits.
- If two inputs to an S-box differ in their first two bits and are identical in their last two bits, the two outputs must not be the same.
- For any nonzero 6-bit difference between inputs, no more than 8 of the 32 pairs of inputs exhibiting that difference may result in the same output difference.

34. What is an avalanche effect? (NOV 2012) (R)

It is that a small change in either the plaintext or the key should produce a significant change in the cipher text.A change in one of the bit of the plaintext or one bit of the key should produce a change in many bits of the cipher text

35. Define product cipher. (U)

Product cipher performs two or more basic ciphers in sequence in such a way that the final result or product is crypto logically stronger than any of the component ciphers

36. Brief the strength of triple DES. (DEC 2016) (U)

It is a reuse DES implementation by cascading three instances of DES. It is believed to be secure up to at least security

37. Define Cipher Feedback (CFB) (U)

In Cipher Feedback (CFB) Input is processed s-bits at a time. Preceding cipher text is used as input to the encryption algorithm to produce pseudorandom output, which is XOR ed with plaintext to produce next unit of cipher text.

38. Define Cipher Block Chaining (CBC) mode. (U)

In Cipher Block Chaining (CBC) mode the input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of cipher text

39. Define Counter (CTR). (U)

In Counter (CTR) mode each block of plaintext is XOR ed with an encrypted counter. The counter is incremented for each subsequent block

40. What is the difference between Rijndael and AES? (R)

AES was developed by NIST .AES is a symmetric block cipher that is intended to replace DES.NIST selected rijndael as the proposed AES algorithm. The two researchers who developed and submitted Rijndael for the AES are the both cryptographers from Belgium.

41. What is the difference between the AES decryption algorithm and the equivalent inverse cipher? (R)

In AES decryption, we use inverse shift rows inverse sub bytes, add round key, inverse mix columns. But in equivalent inverse cipher, we interchange inverse shift rows and inverse sub bytes.

42. What are the operations used in AES? (R)

- Substitute bytes
- ShiftRows
- MixColumns
- AddRoundKey

43. What is a Substitute byte transformation in AES? (R)

The forward substitute byte transformation, called SubBytes, is a simple table lookup. AES defines a 16x16 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

44. How the key is expanded in AES?(AN)

AES (Rijndael) uses a key schedule to expand a short key into a number of separate round keys. This is known as the Rijndael key schedule. The three AES variants have a different number of rounds. Each variant requires a separate 128-bit round key for each round plus one more.

45. List the parameters for the three AES version? (APR/MAY 2018) (U)

Block size – 128 bits Key size – 128 , 192, 256 bits No. of rounds – 10 , 12 or 14

PART- B (16 Marks)

1. Explain about OSI Security architecture model with neat diagram.(DEC2016) **(U)**
2. Describe the various security mechanisms (DEC 2016) **(R)**
3. Classical cryptosystems and its types. (NOV2011, APR2012, NOV2012, NOV 2010, MAY2009, NOV2008, NOV2007) , (APR/MAY 2018) **(R)**
4. Using play fair cipher algorithm encrypt the message using the key "MONARCHY" and explain. [Nov/Dec 2011] (AP)
5. Explain the ceaser cipher and monoalphabetic cipher. [Nov/Dec 2011] **(U)**
6. Convert “MEET ME” using Hill cipher with the key matrix Convert the cipher text back to plaintext(AP)

   Convert the cipher text back to plaintext

   $$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$
7. Encrypt the following using play fair cipher using the keyword MONARCHY . “ SWARAJ IS MY BIRTH RIGHT”. Use X as blank space. (NOV/DEC 2017)(AP)
8. Explain in detail about DES and Triple DES. (APR2012, NOV2009, NOV2008 , APR 2017) **(U)**
9. Explain about AES in detail. (NOV2009, MAY2009, NOV2008,NOV2007,DEC2016,NOV 2017, APRIL 2018) **(U)**

UNIT II ASYMMETRIC CIPHERS (CO2)

PART –A(2 Marks)

1. State the Fermat’s Theorem. (APR2011, APR/MAY 2017, NOV/DEC 2017) (R)

Fermat theorem states the following. If p is prime and a is a positive integer not divisible by p, then $A^{p-1} \equiv 1 \bmod p$

2. State the Euler’s Theorem. (R)

Euler’s theorem states that for every a and n that are relatively prime $a^{\phi(n)} \equiv 1 \pmod n$

3. Define Primality Test. (NOV2011) (U)

A primality testing is a test to determine whether or not a given number is prime, as opposed to actually decomposing the number into its constituent prime factors (which is known as prime factorization).

4. Define Euler's theorem and it's application. (APR/MAY 2018) (U)

Euler's theorem states that for every a and n that are relatively prime: a ϕ (n)≡≡ 1 mod n

5. Find gcd (1970, 1066) using Euclid's algorithm? (DEC2016) (AP)

gcd (1970,1066) = gcd(1066,1970 mod 1066) = gcd(1066,904)= 2

6. Find gcd (1970, 1066) using Euclid's algorithm? (DEC2016) (AP)

gcd (1970,1066) = gcd(1066,1970 mod 1066) = gcd(1066,904)= 2

7. Why is asymmetric cryptography bad for huge data? Specify the reason? (APR/MAY 2018)(AN)

Asymmetric encryption takes more time. Key Management is difficult. Slower encryption speed due to long keys.

8. Perform encryption and decryption using RSA Alg. for the following.. P=17; q=11; e=7; M=88. (NOV/DEC 2017) (AP)

Soln: n=pq n=17*11=187 ö(n)=(p-1) (q-1) =16*10 = 160 e=7

C= Me mod n M = Cd mod n

9. Perform encryption and decryption using RSA Alg. for the following.. P=7; q=11; e=17; M=8. (APRIL/ MAY 2018) **(AP)**

Soln: n=pq n=7*11=77 ö(n)=(p-1) (q-1) =6*10 = 60 e=17 d =27 C= Me mod n C = 817 mod 77 = 57 M = Cd mod n = 5727 mod 77 = 8

10. What is an elliptic curve? (DEC 2016) (R)

It is a plane algebraic curve defined by an equation of the form y2 = x3 +ax +b that is non-singular also graph has no cusps or self intersections.

11. Differentiate public key and conventional encryption? Conventional Encryption Public key Encryption (AN)

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 atleast impractial
5. 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
6. Knowledge of the algorithm plus samples
7. 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.

12. What are the principle elements of a public key cryptosystem?(R)

The principle elements of a cryptosystem are:

1.plain text 2.Encryption algoritm 3.Public and private key 4.Cipher text 5.Decryption algorithm

13. What are roles of public and private key?(R)

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

www.rejinpaul.com

public key is known publicly. Usually the public key is used for encryption purpose and the private key is used in the decryption side.

14. Specify the applications of the public key cryptosystem?(U)

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

1. Encryption/Decryption: The sender encrypts a message with the recipient's public key.
2. Digital signature: The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to a message or to a small block of data that is a function of the message.
3. Key Exchange: Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

15. What requirements must a public key cryptosystem to fulfill to a secured algorithm?(R)

The requirements of public-key cryptosystem are as follows:

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

16. Difference between private key and public key algorithm (APR 2017)(AN)

Public key encryption encrypts data using the recipient's public key and it cannot be decrypted without using a matching private key. i.e., you need one key to lock (encrypt the piantext) and another key to unlock (decrypt the cypertext). Private key cannot be used in the place of the public key. If the locking key is made private, this system makes it possible to verify that the documents were locked by the owner. The reason is that a message encrypted by the sender can only be opened by a person with the matching public key, thus verifying that the sender did actually hold the private key (meaning that the original and non-tampered message has been received). Therefore, this is used for digital signatures.

17. What is a Shift rows? (R)

In shift row, a row shift moves an individual byte from one column to another, which is a linear distance of a multiple of 4 bytes. In Forward Shift Row, each row perform circular left shift. Second Row a 1-byte circular left shift is performed. Third Row a 2-byte circular left shift is performed. For the Fourth Row a 3-byte circular left shift is performed. In Inverse Shift Row, each row perform circular right shift.

18. What primitive operations are used in RC5? (R)

- Key expansion
- Encryption
- Decryption

19. User A & B exchange the key using Diffie Hellman alg. Assume á=5 q=11 XA=2 XB=3. Find YA, YB, K. (AP)

Soln: YA = áXA mod q =52 mod 11 = 3 YB = áXB mod q = 53 mod 11 = 4 KA = YBXA mod q = 42 mod 11 = 5 KB = YAXB mod q= 33 mod 11= 5

20. Whether the Diffie Hellman key exchange protocol is vulnerable?(AN)

Yes, the key exchange protocol is vulnerable to such an attack because it does not authenticate the participants. This vulnerability can be overcome with the use of digital signatures and public-key certificates.

21. Write about elliptic curve cryptography. (R)

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography (based on plain Galois fields) to provide equivalent security. Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization

Part – B (16 Marks)

1. Discuss Fermat's Theorem. (NOV2012, DEC2016, APR 2017) (R)
2. Discuss Euler's Theorem (APR2011, NOV2012) (R)
3. Discuss Chinese Remainder Theorem. (APR2011, APR2012, DEC2016, (APR/MAY 2018) (R)
4. Describe : Playfair cipher, Railfence cipher, Vignere cipher (APR/ MAY 2017) (R)
5. Discuss the properties that are satisfied by Groups, Rings and Fields. (NOV/DEC 2017) (R)
6. Discuss the discrete logarithm and explain Diffie-Hellman Key Exchange algorithm with its merits and demerits. (APR2011, NOV2012, NOV2010, DEC2016, APR 2017) (R)

7. State Chinese remainder theorem and find X for the given set of congruent equations using CRT (DEC 2016, APR/MAY 2017) X = 1(mod 5) (b) X = 2(mod 3) X = 2(mod 7) X = 3(mod 5) X = 3(mod 9) X = 2(mod 7) X = 4(mod 11)
8. Explain the RSA algorithm and explain the RSA with p=7,q=11,e=17,M=8. Discuss its merit. (APR2011, NOV2011, NOV2012, NOV2010, DEC2016) (U)
9. Explain in detail about elliptic curve cryptography(APRIL 2018). (U)
10. User Alice & Bob exchange the key using Diffie Hellman alg. Assume α=5 q=83 XA=6 XB=10. Find YA, YB, K. (NOV /DEC 2017). (AP)
11. Describe Diffie-Hellman Key Exchange.(R)
12. Explain RSA algorithm and security of RSA algorithm.(U)
13. Write down the steps involved in Elgamal DSS & Schnorr DSS ? (NOV/DEC 2017) (R)

UNIT – III CRYPTOGRAPHIC DATA INTEGRITY ALGORITHMS(CO3)

PART – A (2 Marks)

1. Define Hash function (APRIL/ MAY 2018) (U)

A function that maps a message of any length into a fixed length hash value, which serves as the authenticator.

2. Differentiate Message Authentication Code and Hash function. (DEC 2016) (U)

In MAC, a public function of the message and a secret key are used to produce a fixed length authenticator. A hash function accepts a variable size message as input and produces a fixed size output (hash code) which is similar to MAC. But hash code does not use a key.

3. List out the attacks during the communication across the network. (R)

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

4. Define the classes of message authentication function. (U)

- Hash function
- Message encryption
- Message authentication code (MAC

5. What you meant by MAC? (R)

MAC is Message Authentication Code. It is a function of message and secret key which produce a fixed length value called as MAC. T=MAC(K,M) where M is a variable-length message, K is a secret key shared only by sender and receiver, and MAC(K,M) is the fixed-length authenticator.

6. List out the attack on MAC. (R)

- Brute-force attacks
- Cryptanalysis.

7. What do you mean by one way property in hash function? (APR2011, NOV2012) (R)

An algorithm that turns messages or text into a fixed string of digits, usually for security or data management purposes. The "one way" means that it's nearly impossible to derive the original text from the string. A one-way hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message.

8. Define Replay Attack. (NOV2011) (U)

Replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IPpacket substitution

9. **Define Digital signature. (U)**

A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. Typically the signature is formed by taking the hash of the

message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message

10. What are the properties of Digital Signature? (R)

The digital signature must have the following properties: It must verify the author and the date and time of the signature. It must authenticate the contents at the time of the signature. It must be verifiable by third parties, to resolve disputes.

11. List out the attacks related to Digital Signature. (R)

Key-only attack: (R) (R)

- Known message attack
- Generic chosen message attack
- Directed chosen message attack
- Adaptive chosen message attack

12. Mention the signature function in DSS ? (NOV/DEC2017) (R)

The hash function used in the DSS standard is specified in the Secure Hash Standard (SHS), which are the specificati**(R)**ons for the Secure Hash Algorithm (SHA).

13. Define Generic chosen message attack. (R)

If A is the sender and C is the attacker. Then C chooses a list of messages before attempting to breaks A's signature scheme, independent of A's public key. C then obtains from A valid signatures for the chosen messages. The attack is generic, because it does not depend on A's public key; the same attack is used against everyone.

14. What are the two approaches of Digital Signature? (NOV2012) (R)

- RSA Approach
- DSS Approach

15. How is the security of MAC expressed? (NOV /DEC 2017)(AN)

MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages. In contrast, a digital signature is generated using the private key of a key pair, which is public-key cryptography. Since this private key is only accessible to its holder, a digital signature proves that a document was signed by none other than that holder. Thus, digital signatures do offer non-repudiation

16. How Digital signature differs from authentication protocols? (APR/ MAY 2018)(AN)

A digital signature is a mathematical scheme for presenting the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message, and that the message was not altered in transit. An authentication protocol is a type of computer communications protocol or cryptographic protocol specifically designed for transfer of authentication data between two entities. It allows the receiving entity to authenticate the connecting entity (e.g. Client connecting to a Server) as well as authenticate itself to the connecting entity (Server to a client) by declaring the type of information needed for authentication as well as syntax.

17. List out some hash algorithm. (R)

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

18. What is the role of compression function in hash function? (APR 2017) (R)

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.

19. What is MAC based on DES? (R)

One of the most widely used MACs, referred to as Data Authentication Algorithm (DAA) is based on DES. The algorithm can be defined as using cipher block chaining (CBC) mode of operation of DES with an initialization vector of zero. The data to be authenticated are grouped into contiguous 64-bit blocks: D1, D2 □ Dn. if necessary, the final block is padded on the right

with zeros to form a full 64-bit block. Using the DES encryption algorithm and a secret key, a data authentication code

PART – B (16Marks)

1. Illustrate about the SHA algorithm and explain. (NOV 2017 ,NOV2011, NOV2010, NOV2009, MAY2009, MAY2007) **(U)**
2. Compare the performance of RIPEMD-160 algorithm and SHA-1 algorithm? (APR 2017)**(AN)**
3. Describe about Hash Function. How its algorithm is designed? Explain its features & properties? (NOV 2012, NOV2008, APRIL 2018) **(U)**
4. Describe HMAC algorithm.(U)
5. Explain message authentication functions.(U)
6. Write a detailed note on Digital signatures. (NOV2011, DEC 2016, APR 2017) **(R)**
7. Explain Digital Signature Standards algorithm.(U)

UNIT – IV NETWORK AUTHENTICATION(CO4)

PART – A (2 Marks)

1. What is mean by key distribution?(R)

Key Distribution is the function that delivers a key to two parties who wish to exchange secure encrypted data.

2. List out the Requirements of Kerberos. (APR2011) (R)

- Secure
- Reliable
- Transparent
- Scalable

3. Define Kerberos. (R)

Kerberos is an authentication service developed as part of project Athena atMIT.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.

4. In the content of Kerberos, what is realm? (R)

A full service Kerberos environment consisting of a Kerberos server, a no. Ofclients, 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 anenvironment is referred to as "Realm".

5. Mention the scenario where kerberos scheme is preferred. (April/May 2010)

Kerberos is a authentication service designed for use in a distributed environment. The kerberos that is preferred to address is, assume an open distributed environment in which users at work stations wish to access services on servers distributed throughout the network.

6. What is the problem that kerberos addresses? (April /May2012)(R)

The problem that Kerberos addresses is this: Assume an open distributed environment in which users at workstations wish to access services on servers distributed throughout the network. We would like for servers to be able to restrict access to authorized users and to be able to authenticate requests for service. In this environment a workstation cannot be trusted to identify its users correctly to network services.

7. Assume the client C wants to communicate server S using Kerberos procedure. How can it be achieved?(AN)

Write the authentication dialogue? (NOV /DEC 2017) a) C ->AS: [IDC|| PC || IDV] b) AS ->C: Ticket c) C ->V: [IDC || ADC || IDV] Ticket = EKV [IDC ||ADC || IDV]

8. What you mean by versioned certificate? (R)

Mostly used issue X.509 certificate with the product name" versioned digital id". Each digital id contains owner's public key, owner's name and serial number of the digital id.

9. List any two applications of X.509 Certificate? (NOV/DEC 2017) (R)

Various code-signing schemes, such as signed Java ARchives, and Microsoft Authenticode. Various secure E-Mail standards, such as PEM and S/MIME. E-Commerce protocols, such as SET.

10. List Steps involved in SSL required protocol?(R)

1. SSL record protocol takes application data as input and fragments it. 2. Apply lossless Compression algorithm. 3. Compute MAC for compressed data.

11. What are the technical deficiencies in the kerberos version 4 protocol?(Nov/Dec 2009) (R)

i. Double encryption:

ii. PCBC encryption:It uses non standard modes of DES

iii.Session key:Each ticket includes a session key that is used by the client to encrypt the authenticator

iv. Password attacks: Vulnerable to Password attacks

12. Mention four SSL protocols. (APR 2011) (R)

- SSL Record Protocol
- Handshake Protocol.
- Change Cipher Spec Protocol.
- Alert Protocol.

13. Define TLS. (APR 2012) (R)

TLS is an IETF standardization initiative whose goal is to produce an Internet standard version of SSL. TLS is defined as a Proposed Internet Standard in RFC 5246. RFC 5246 is very similar to SSLv3.

14. What protocol compromise SSL? (NOV 2012) (R)

Secure Sockets Layer (SSL) protocol, originally developed by Netscape Communications, provides application-independent security and privacy over the Internet. SSL protocol is designed as a "stack" comprised of two separate protocols: the Record protocol and the Handshake protocol. These two protocols work together to ensure the secure encryption, transmission and reception of sensitive data between an authenticated website (server) and user (client), preventing unwanted interception by untrustworthy companies or persons.

15. What is the difference between an SSL connection and SSL session? (M/J-09)

Connection is a transport that provides a suitable type of service. For SSL, such connections are peer-topeer relationships. The connections are transient. Every connection is associated with one session. Session: An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

16. List out the attacks fixed by SSL v3. (U)

- Downgrade Attack
- Truncation Attack

17. What is the difference between TLS and SSL security? (APRIL /MAY 2018) (R)

Secure Sockets Layer (SSL) is a cryptographic protocol that enables secure communications over the Internet. SSL works mainly through using public/private key encryption on data. It is commonly used on web browsers, but SSL can also be used with email servers or any kind of client-server transaction.

Transport Layer Security (TLS) is the successor to SSL. TLS uses stronger encryption algorithms and has the ability to work on different ports.

PART – B(16 Marks)

1. Explain about the various Key management techniques.
2. Describe the symmetric key distribution using symmetric encryption.(U)
3. Describe the symmetric key distribution using Asymmetric encryption.(U)
4. Briefly explain the key distribution scenario.(U)
5. Explain kerberos authentication mechanism with suitable diagram?(DEC2016, APRIL 2018) **(U)**
6. Discuss in detail Kerberos 4 message Exchanges for providing authentication.(R)
7. Explain X.509 Authentication Services.(U)
8. Describe the SSL Architecture in detail. [Nov/Dec 2011](U)
9. Explain the steps, methodology involved in SSL/TLS protocol? (NOV/DEC 2017) **(U)**

UNIT – V ADVANCED NETWORK CONCEPTS(CO5)

Part – A (2 Marks)

1. What do you mean by S/MIME? (APR 2012) (R)

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public keyencryption and signing of MIME data. S/MIME is on an IETFstandards track and defined in a number of documents, most importantly RFCs (3369,3370,3850,3851). S/MIME was originally developed by RSA Data Security Inc.S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity, non-repudiation of origin (using digital signatures), privacy and data security (using encryption)

2. What is the purpose of S/MIME? (R)

Abbreviated as : Secure/Multipurpose Internet Mail ExtensionSpecified as a standard way of encoding arbitrary data in email such as pictures, rich text,video clips ,binary files etc., along with adding signed and encrypted data.

3. What are the types of MIME? (NOV 2012) (R)

- Text
  - Plain
  - Enriched
- Multipart
  - Mixed
  - Parallel
  - Alternative
  - Digest
- Message
  - rfc822
  - Partial
  - External-body
- Image
  - jpeg
  - gif
- Video
  - mpeg
  - Audio
  - Basic
- Application
  - PostScript
  - octet-stream

4. Write about PGP? (R)

- Secure Mail Protocol
- Abbreviated as Pretty Good Privacy
- Proposed by Phil Zimmermann
- PGP performs encryption and integrity protection on files
- PGP uses public key cryptography for personal use
- Certificates are optional in PGP

5. What are the services provided by PGP ? (APRIL /MAY 2018) (R)

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

6. Explain the reasons for using PGP? (U)

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-

1for 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.

7. Why E-mail compatibility function in PGP needed? (U)

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 forthis purpose is Radix-64 conversion

8. Name any cryptographic keys used in PGP? (R)

a) One-time session conventional keys. b) Public keys. c) Private keys. d) Pass phrase based conventional keys.

9. Give the steps for preparing envelope data MIME? Generate Ks. (R)

- Encrypt Ks using recipient's public key. RSA algorithm used for encryption.
- Prepare the 'recipient info block'. Encrypt the message using Ks.

10. What are the function areas of IP security? (R)

- Authentication Confidentiality Key management

11. Give the application of IP security. (R)

- Provide secure communication across private & public LAN.
- Secure remote access over the Internet.
- Secure communication to other organization

12. Give the benefits of IP security. (APR 2017) (R)

- 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

13. What are the protocols used to provide IP security? (R)

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

14. Specify the IP security services. (R)

- Access control. Connectionless interpretty.
- Data origin authentication Rejection of replayed packet.
- Confidentiality Limited traffic for Confidentiality

15. What do you mean by Security Association? Specify the parameters that identifies the Security Association? (R)

An association is a one-way relationship between a sender and receiver thataffords 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

16. List the design goals of firewalls? (U)

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.

23. What are the different phases a virus go through his lifetime? (R)

1. Dormant phase 2. Propagation phase 3. Triggering Phase 4. Execution phase

24. Define the roles / functions of firewall? (APR 2017, APRIL 2018) (U)

A firewall acts as a barrier between a trusted network and and an untrusted network. A firewall controls access to the resources of a network through a positive control model.

25. State the difference between threats and attack? (APR 2017) (U)

Threat: object, person, or other entity representing a constant danger to an asset. This can take any form and can be malevolent, accidental, or simply an act of nature. Attack: a deliberate act that exploits vulnerability. It can be either active or passive attack.

26. Define password selection strategy? (R)

- The technique used to give password is: User education
- Computer generated password
- Reactive password checking

- Proactive password checking

27. What are the types of firewalls? (R)

The three types of firewalls are

- Packet Filtering Router
- Application Level gateway
- Circuit level gateway

28. Define trusted system? (R)

One way to increase the security of a system against intruders and malicious program is toimplement trusted system.

29. Define Intrusion. (APR2012,NOV2012) (R)

The process of accessing a network or system without proper permission or rights.

30. List the 3 classes of intruder? Define intruder (April/May 2010,2011) (Nov/Dec 2009,2012)(U)

Classes of Intruders 1) Masquerader 2) Misfeasor 3) Clandestine user

Intruder: someone who intrudes on the privacy or property of another without permission.

31. Give few examples for worms. (NOV2012) (R)

A worm is a program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function. An e-mail virus has some of the characteristics of a worm because it propagates itself from system to system.

32. Define virus. Specify the types of viruses? (R)

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

33. What is Trojan horse?(R)

A Trojan horse1 is a useful, or apparently useful, program or command procedure containing
hidden code that, when invoked, performs some unwanted or harmful function. Trojan horse
programs can be used to accomplish functions indirectly that an unauthorized user could not
accomplish directly. For example, to gain access to the files of another user on a shared system, a
user could create a Trojan horse program that, when executed, changes the invoking user's file
permissions so that the files are readable by any user.

PART-B (16 Marks)

1. Explain with suitable diagrams how authentication and confidentiality is provided in Electronic Mail. (U)
2. Explain in detail about the security services (PGP, S/MIME) for E-mail. (U)
3. Explain the operation description of PGP.(APR2011, NOV2012, NOV2010, NOV2009, MAY2009,DEC2016, APRIL 2018) (U)
4. Explain in detail about architecture of IP Security. (APR2011, APR 2012, NOV2010, DEC 2017) (U)
5. Explain in detail about firewalls. (APR2011, NOV2011, APR 2012, NOV2012, NOV2010, DEC2016, NOV 2017). (U)
6. Explain the Firewall Design Principles.(U)
7. How does screened host architecture for firewalls differ from screened subnet firewall architecture? Which offers more security for information assets on trusted network? Explain with neat sketch? (APRIL 2018) (U)
8. Explain about viruses in detail. (APR2011, NOV2012, APR 2017) (U)
9. Explain the types of Intrusion Detection Systems. (NOV2011, NOV2010, APR 2017) (U)
10. Explain about Malicious Software. (APR2012) (U)