Course/Branch : B.E/ CSE	**Year / Semester** :IV/VII	Format No.	NAC/TLP-07a.13
Subject Code :CS8792	**Subject Name**:Cryptography & Network Security	Rev. No.	02
Unit No :2	**Unit Name** :**Symmetric Key Cryptography**	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

S.No	**Objective Questions (MCQ /True or False / Fill up with Choices)**	BTL
1.	1. DES follows a) Hash Algorithm b) Caesars Cipher c) Feistel Cipher Structure d) SP Networks View Answer Answer: c Explanation: DES follows Feistel Cipher Structure.	LT2
2.	Using Linear Crypt-analysis, the minimum computations required to decipher the DES algorithm is a) 248 b) 243 c) 256 d) 264 Answer: b Explanation: Linear Crypt-analysis requires only 243 computations to decipher the DES algorithm	LT1
3.	Using Differential Crypt-analysis, the minimum computations required to decipher the DES algorithm is a) 256 b) 243 c) 255 d) 247 View Answer Answer: d Explanation: Differential Crypt-analysis requires only 247 computations to decipher the DES algorithm.	LT1
4.	In triple DES, the key size is ___ and meet in the middle attack takes ___ tests to break the key. a) 2192 ,2112 b) 2184,2111 c) 2168,2111 d) 2168,2112 Answer: d Explanation: The key size is 2168 and meet in the middle attack takes 2112 tests to break.	LT2
5.	How many keys does the Triple DES algorithm use? a) 2 b) 3 c) 2 or 3 d) 3 or 4	LT2

Course/Branch : B.E/ CSE	**Year / Semester** :IV/VII	Format No.	NAC/TLP-07a.13
Subject Code :CS8792	**Subject Name**:Cryptography & Network Security	Rev. No.	02
Unit No :2	**Unit Name :Symmetric Key Cryptography**	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	Answer: c Explanation: For Triple DES we can either have 2 or 3 keys. Using two keys: c = Ek1(Dk2(Ek1(m))) Using three keys: c = Ek3(Ek2(Ek1(m))).	
6.	The number of tests required to break the DES algorithm are a) 2.8×1014 b) 4.2×109 c) 1.84×1019 d) 7.2×1016 Answer: d Explanation: There are 256 keys =7.2×1016.	LT2
7.	9. In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 4th bit. a) True b) False Answer: b Explanation: Every 8th bit is ignored to shorten the key length.	LT2
8.	The number of tests required to break the Double DES algorithm are a) 2112 b) 2111 c) 2128 d) 2119 Answer: b Explanation: For Double DES key is 2112 bits, should require 2111 tests to break.	LT1
9.	A preferable cryptographic algorithm should have a good avalanche effect. a) True b) False Answer: a Explanation: Thus statement is true as 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.	LT1
10.	The number of unique substitution boxes in DES after the 48 bit XOR operation are a) 8 b) 4 c) 6 d) 12 Answer: a Explanation: The substitution consists of a set of 8 S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.	LT2
11.	During decryption, we use the Inverse Initial Permutation (IP-1) before the IP. a) True	LT2

Course/Branch : B.E/ CSE	**Year / Semester** :IV/VII	Format No.	NAC/TLP-07a.13
Subject Code :CS8792	**Subject Name**:Cryptography & Network Security	Rev. No.	02
Unit No :2	**Unit Name :Symmetric Key Cryptography**	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	b) False Answer: a Explanation: IP-1 is the first step and the last step is IP during decryption.	
12.	4. In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits. a) True b) False Answer: b Explanation: 56 bits are used, the rest 8 bits are parity bits.	LT2
13.	In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____ a) Scaling of the existing bits b) Duplication of the existing bits c) Addition of zeros d) Addition of ones Answer: a Explanation: The round key is 48 bits. The input is 32 bits. This input is first expanded to 48 bits (permutation plus an expansion), that involves duplication of 16 of the bits.	LT2
14.	In the DES algorithm the round key is _____ bit and the Round Input is _____bits. a) 48, 32 b) 64,32 c) 56, 24 d) 32, 32 Answer: a Explanation: The round key is 48 bits. The input is 32 bits.	LT1
15.	The DES algorithm has a key length of a) 128 Bits b) 32 Bits c) 64 Bits d) 16 Bits View Answer Answer: c Explanation: DES encrypts blocks of 64 bits using a 64 bit key.	LT1
16.	What is the size of the key in the SDES algorithm? a) 24 bits b) 16 bits c) 20 bits d) 10 bits Answer: d	LT2

Course/Branch : B.E/ CSE	**Year / Semester** :IV/VII	Format No.	NAC/TLP-07a.13
Subject Code :CS8792	**Subject Name**:Cryptography & Network Security	Rev. No.	02
Unit No :2	**Unit Name** :**Symmetric Key Cryptography**	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	Explanation: The size of the key in the SDES algorithm is 10 bits.	
17.	The Ciphertext for the Plaintext 01110010, given that the keys K1 is 10100100 and K2 is 01000011 is a) 01110111 b) 10010110 c) 01010110 d) 01000101 Answer: a Explanation: Perform the SDES algorithm and compute the cipher text.	LT2
18.	Assume input 10-bit key, K: 0010010111 for the SDES algorithm. What is K2? a) 11101010 b) 11011011 c) 01101000 d) 10101111 Answer: a Explanation: The permuted key P10 = 0000101111. Input to P8: 0010011101 and K2 is 11101010.	LT2
19.	The Plaintext for the Ciphertext 10100101, given that the key is 0010010111 is a) 01100111 b) 00110110 c) 01001000 d) 01001100 Answer: b Explanation: Perform the SDES Decryption algorithm and compute the cipher text.	LT2
20.	The Plaintext for the Ciphertext 00001111, given that the key is 1111111111 is a) 01100111 b) 00001010 c) 11111111 d) 01101101 Answer: c Explanation: Perform the SDES Decryption algorithm and compute the cipher text.	LT1
21.	Assume input 10-bit key, K: 0010010111 for the SDES algorithm. What is K1? a) 00101111 b) 01011011 c) 01101000 d) 10100111 Answer: a Explanation: The permuted key P10 = 1000010111. Input to P8: 0000101111 and K1 is 00101111.	LT1
22.	The Plaintext for the Ciphertext 11110000, given that the key is 0000000000 is a) 01100111	LT2

Course/Branch : B.E/ CSE	**Year / Semester** :IV/VII	Format No.	NAC/TLP-07a.13
Subject Code :CS8792	**Subject Name**:Cryptography & Network Security	Rev. No.	02
Unit No :2	**Unit Name** :**Symmetric Key Cryptography**	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	b) 00000000 c) 01001000 d) 01101100 Answer: b Explanation: Perform the SDES Decryption algorithm and compute the cipher text.	
23.	The Plaintext for the Ciphertext 00100010, given that the key is 1111111111 is a) 01100111 b) 00001010 c) 01001000 d) 01001100 Answer: d Explanation: Perform the SDES Decryption algorithm and compute the cipher text.	LT2
24.	The Ciphertext for the Plaintext 11010101, given that the key is 0111010001 is a) 00010001 b) 10110010 c) 11010010 d) 01110011 Answer: d Explanation: Perform the SDES Encryption algorithm and compute the cipher text.	LT2
25.	In SDES, Encryption algorithm can be written as a composition of functions: IP-1 o fK2 o fK1 o SW o IP a) True b) False Answer: b Explanation: The SDES algorithm follows the order – IP-1 o fK2 o SW o fK1 o IP.	LT2
26.	Assume input 10-bit key, K: 1010000010 for the SDES algorithm. What is K1? a) 10100100 b) 01011011 c) 01101000 d) 10100111 Answer: a Explanation: The permuted key P10 = 1000001100. Input to P8: 0000111000 and K1 is 10100100.	LT1
27.	Assume input 10-bit key, K: 1010000010 for the SDES algorithm. What is K2? a) 10100111 b) 01000011 c) 00100100 d) 01011010	LT1

Course/Branch : B.E/ CSE	**Year / Semester** :IV/VII	Format No.	NAC/TLP-07a.13
Subject Code :CS8792	**Subject Name**:Cryptography & Network Security	Rev. No.	02
Unit No :2	**Unit Name** :**Symmetric Key Cryptography**	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	Answer: b Explanation: Input to P8: 0010000011 and K2 is 01000011.	
28.	Confusion hides the relationship between the ciphertext and the plaintext. a) True b) False Answer: b Explanation: Confusion hides the relationship between the ciphertext and the key.	LT2
29.	The S-Box is used to provide confusion, as it is dependent on the unknown key. a) True b) False Answer: a Explanation: The S-Box is used to provide confusion, as it is dependent on the unknown key. The P-Box is fixed, and there is no confusion due to it, but it provides diffusion.	LT2
30.	The Initial Permutation table/matrix is of size a) 16×8 b) 12×8 c) 8×8 d) 4×8 Answer: c Explanation: There are 64 bits to permute and this requires a 8×8 matrix.	LT2
31.	The multiplicative Inverse of 24140 mod 40902 is a) 2355 b) 5343 c) 3534 d) Does not exist Answer: d Explanation: The multiplicative Inverse does not exist as GCD (24140, 40902) = 34	LT2
32.	The multiplicative Inverse of 1234 mod 4321 is a) 3239 b) 3213 c) 3242 d) Does not exist Answer: a Explanation: The multiplicative Inverse of 1234 mod 4321 is 3239.	LT1
33.	117 mod 13 = a) 3	LT1

Course/Branch : B.E/ CSE	**Year / Semester** :IV/VII	Format No.	NAC/TLP-07a.13
Subject Code :CS8792	**Subject Name**:Cryptography & Network Security	Rev. No.	02
Unit No :2	**Unit Name** :**Symmetric Key Cryptography**	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	b) 7 c) 5 d) 15 Answer: d Explanation: The correct answer is 2. Or in this case 15 mod 13 = 2.	
34.	[(a mod n) – (b mod n)] mod n = (b – a) mod n a) True b) False Answer:b Explanation:The equivalence is false and can be checked by substituting values. The correct equivalence would be [(a mod n) – (b mod n)] mod n = (a – b) mod n.	LT2
35.	The multiplicative Inverse of 1234 mod 4321 is a) 3239 b) 3213 c) 3242 d) Does not exist Answer: a Explanation: The multiplicative Inverse of 1234 mod 4321 is 3239.	LT2