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 :1	**Unit Name :Introduction**	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

S.No	Objective Questions (MCQ /True or False / Fill up with Choices)	BTL
1.	Use Caesar's Cipher to decipher the following HQFUBSWHG WHAW a) ABANDONED LOCK b) ENCRYPTED TEXT c) ABANDONED TEXT d) ENCRYPTED LOCK **Answer: b** **Explanation: Caesar Cipher uses C =(p+3) mod 26 to encrypt.**	LT1
2.	Caesar Cipher is an example of a) Poly-alphabetic Cipher b) Mono-alphabetic Cipher c) Multi-alphabetic Cipher d) Bi-alphabetic Cipher **Answer: b** **Explanation: Caesar Cipher is an example of Mono-alphabetic cipher, as single alphabets are encrypted or decrypted at a time**.	LT2
3.	The DES Algorithm Cipher System consists of _____rounds (iterations) each with a round key a) 12 b) 18 c) 9 d) 16 Answer: d Explanation: The DES Algorithm Cipher System consists of 16 rounds (iterations) each with a round key.	LT1
4.	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
5.	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	LT1
6.	In the DES algorithm the round key is _____ bit and the Round Input is _____bits. a) 48, 32 b) 64,32 c) 56, 24	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 :1	**Unit Name :Introduction**	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	d) 32, 32 Answer: a Explanation: The round key is 48 bits. The input is 32 bits.	
7.	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.	LT1
8.	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
9.	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.	LT1
10.	The DES algorithm has a key length of a) 128 Bits b) 32 Bits c) 64 Bits d) 16 Bits Answer: c Explanation: DES encrypts blocks of 64 bits using a 64 bit key.	LT2
11.	DES follows a) Hash Algorithm b) Caesars Cipher c) Feistel Cipher Structure d) SP Networks Answer: c Explanation: DES follows Feistel Cipher Structure.	LT1
12.	Which of the following slows the cryptographic algorithm – 1) Increase in Number of rounds 2) Decrease in Block size 3) Decrease in Key Size	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 :1	**Unit Name :Introduction**	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	4) Increase in Sub key Generation a) 1 and 3 b) 2 and 3 c) 3 and 4 d) 2 and 4 Answer: b Explanation: Increase in any of the above 4 leads to slowing of the cipher algorithm i.e. more computational time will be required.	
13.	In base 26, multiplication of YES by NO gives – a) THWOE b) MPAHT c) MPJNS d) THWAE Answer: c Explanation: Convert the alphabets into their respective values in base 26 and proceed with base 26 multiplications.	LT1
14.	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
15.	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.	LT1
16.	What is the number of possible 3 x 3 affine cipher transformations ? a) 168 b) 840 c) 1024 d) 1344 Answer: d	LT2
17.	Division of (131B6C3) base 16 by (lA2F) base 16 yeilds – a) 1AD b) DAD c) BAD d) 9AD Answer: d Explanation: Base 16 division to be followed where A-F stand for 10-15.	LT1
18.	The estimated computations required to crack a password of 6 characters from the 26 letter alphabet is- a) 308915776 b) 11881376	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 :1	**Unit Name :Introduction**	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	c) 456976 d) 8031810176 Answer: a Explanation: The required answer is 26^6 = 308915776.	
19.	An encryption scheme is unconditionally secure if the ciphertext generated does not contain enough information to determine uniquely the corresponding plaintext, no matter how much cipher text is available. a) True b) False Answer: a Explanation: The above statement is the definition for unconditionally secure cipher systems.	LT1
20.	On Encrypting "cryptography" using Vignere Cipher System using the keyword "LUCKY" we get cipher text a) nlazeiibljji b) nlazeiibljii c) olaaeiibljki d) mlaaeiibljki Answer: a Explanation: Cipher text:= Ci = Pi + ki mod m (mod 26).	LT2
21.	pi in terms of base 26 is a) C.DRS b) D.SQR c) D.DRS d) D.DSS Answer: c Explanation: On converting using base conversions we get 3.1415926 as D.DRS.	LT1
22.	Dividing (11001001) by (100111) gives remainder – a) 11 b) 111 c) 101 d) 110 Answer: d Explanation: Dividing (11001001) by (100111) gives us (110).	LT2
23.	Divide (HAPPY)26 by (SAD)26. We get quotient – a) KD b) LD c) JC d) MC Answer: a Explanation: Dividing (HAPPY)26 by (SAD)26 gives us KD with a remainder MLP.	LT1
24.	Consider the cipher text message: YJIHX RVHKK KSKHK IQQEV IFLRK QUZVA EVFYZ RVFBX UKGBP KYVVB QTAJK TGBQO ISGHU CWIKX QUXIH DUGIU LMWKG CHXJV WEKIH HEHGR	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 :1	**Unit Name :Introduction**	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	EXXSF DMIIL UPSLW UPSLW AJKTR WTOWP IVXBW NPTGW EKBYU SBQWS Relative Frequencies – 3 7 2 2 5 5 7 9 11 4 14 4 2 1 3 4 6 5 6 5 7 10 9 8 4 2 The Index of Coincidence is – a) 0.065 b) 0.048 c) 0.067 d) 0.044 Answer: d Explanation: Number of letters = 145.From this, IC=0.0438697 .This is very strong evidence that the message came from a polyalphabetic ciphering scheme.	
25.	If all letters have the same chance of being chosen, the IC is approximately a) 0.065 b) 0.035 c) 0.048 d) 0.038 Answer: d Explanation: If all letters have the same chance of being chosen, the IC is approximately 0.038, about half of the IC for the English language.	LT1
26.	If the sender and receiver use different keys, the system is referred to as conventional cipher system. a) True b) False Answer: b Explanation: Such a system is called asymmetric, two-key, or public-key cipher system.	LT2
27.	In brute force attack, on average half of all possible keys must be tried to achieve success. a) True b) False Check Answer: a Explanation: In brute force attack the attacker tries every possible key on a piece of cipher-text until an intelligible translation into plaintext is obtained.	LT1
28.	Consider the cipher text message with relative frequencies: 4 0 10 25 5 32 24 15 6 11 5 5 1 2 6 6 15 19 10 0 6 28 8 2 3 2 The Index of Coincidence is a) 0.065 b) 0.048 c) 0.067 d) 0.042 Answer: c Explanation: Number of letters = 250. From this, IC=0.0676627. This is very strong	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 :1	**Unit Name :Introduction**	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	evidence that the message came from a Monoalphabetic ciphering scheme.	
29.	The Index of Coincidence for English language is approximately a) 0.068 b) 0.038 c) 0.065 d) 0.048 Answer: c Explanation: The IC for the English language is approximately 0.065.	LT1
30.	3. Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former. a) True b) False Answer: b Explanation: Monoalphabetic ciphers are easier to break because they reflect the frequency of the original alphabet.	LT2
31.	[(a mod n) + (b mod n)] mod n = (a+b) mod n a) True b) False Answer: a Explanation: The equivalence is true and can be checked by substituting values.	LT1
32.	Which of the following is a valid property for concurrency? a) a = b (mod n) if n|(a-b) b) a = b (mod n) implies b = a (mod n) c) a = b (mod n) and b = c (mod n) implies a = c (mod n) d) All of the mentioned Answer: d Explanation: All are valid properties of congruences and can be checked by using substituting values.	LT2
33.	Calculate the GCD of 8376238 and 1921023 using Euclidean algorithm. a) 13 b) 12 c) 17 d) 7 Answer: a Explanation: GCD(8376238, 1921023) = 13.	LT1
34.	What is 11 mod 7 and -11 mod 7? a) 4 and 5 b) 4 and 4 c) 5 and 3 d) 4 and -4 View Answer	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 :1	**Unit Name :Introduction**	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	Answer: d Explanation:11 mod 7 = 4 ; -11 mod 7 = -4 mod 7 = 3 mod 7.	
35.	GCD(a,b) is the same as GCD(|a|,|b|). a) True b) False View Answer Answer: a Explanation:This is true. gcd(60,24) = gcd(60,-24) = 12.	LT1