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 :3	**Unit Name** :Public Key Cryptography	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

S.No	Objective Questions (MCQ /True or False / Fill up with Choices)	BTL
1.	SHA-1 produces a hash value of a) 256 bits b) 160 bits c) 180 bits d) 128 bits Answer: b Explanation: SHA-1 produces a hash value of 160 bits.	LT2
2.	The message in SHA-512 is padded so that it's length is a) 832 mod 1024 b) 768 mod 1024 c) 960 mod 1024 d) 896 mod 1024 Answer: d Explanation: Padding is done so that the length is 896 mod 1024.	LT1
3.	The output of the N 1024-bit blocks from the Nth stage is a) 512 bits b) 1024 bits c) N x 1024bits d) N x 512 bits Answer: a Explanation: The message digest output is 512-bits.	LT1
4.	In the SHA-512 processing of a single 1024- bit block, the round constants are obtained a) by taking the first 64 bits of the fractional parts of the cube roots of the first 80 prime numbers b) by taking the first 64 bits of the fractional parts of the cube roots of the first 64 prime numbers c) by taking the first 64 bits of the fractional parts of the square roots of the first 80 prime numbers d) by taking the first 64 bits of the non-fractional parts of the first 80 prime numbers Answer: a Explanation: The round constants (K) is obtained by taking the first 64 bits of the fractional parts of the cube roots of the first 80 prime numbers.	LT2
5.	In SHA-512, the registers 'a' to 'h' are obtained by taking the first 64 bits of the fractional parts of the cube roots of the first 8 prime numbers. a) True b) False Answer: b Explanation: The registers 'a' to 'h' are obtained by taking the first 64 bits of the fractional parts of the square roots of the first 8 prime numbers.	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 :3	**Unit Name** :Public Key Cryptography	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

6.	What is the size of W (in bits) in the SHA-512 processing of a single 1024- bit block? a) 64 b) 128 c) 512 d) 256 Answer: a Explanation: The 1024 bit message blocks are compressed to form 64 bit values(W).	LT2
7.	The big-endian format is one in which a) the least significant byte is stored in the low-address byte position b) the least significant byte is stored in the high-address byte position c) the most significant byte is stored in the high-address byte position d) the most significant byte is stored in the low-address byte position Answer: d Explanation: The big-endian format is one in which the most significant byte is stored in the low-address byte position.	LT2
8.	What is the number of round computation steps in the SHA-256 algorithm? a) 80 b) 76 c) 64 d) 70 Answer: c Explanation: The number of round computation steps in the SHA-256 algorithm is 64.	LT1
9.	What does the figure represent? a) Compression function b) Message digest generation using SHA c) Elementary SHA operation for single round d) Processing of a single 1024 bit block Answer: c Explanation: The figure represents the elementary SHA operation for single round.	LT1
10.	What is the maximum length of the message (in bits) that can be taken by SHA-512? a) 2128 b) 2256 c) 264 d) 2192 Answer: a Explanation: The maximum length of the message is 2128.	LT2
11.	In SHA-512, the message is divided into blocks of size ___ bits for the hash computation. a) 1024 b) 512 c) 256	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 :3	**Unit Name** :Public Key Cryptography	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	d) 1248 Answer: a Explanation: The message is divided into blocks of size 1024 bits, and the output produced is a 512-bit message digest.	
12.	Among the registers 'a' to 'h' how many involve permutation in each round? a) 4 b) 5 c) 6 d) 3 Answer: c Explanation: (b, c, d, f, g, and h) undergo permutations.	LT2
13.	What is a one-way password file? a) A scheme in which the password is jumbled and stored b) A scheme in which the password is XOR with a key and stored c) A scheme in which the hash of the password is stored d) A scheme in which the password is passed through a PRF, which is then stored Answer: c Explanation: A scheme in which the hash of the password is stored by an operating system rather than the password itself is the one-way password file system.	LT2
14.	Which one of the following is not an application hash functions? a) One-way password file b) Key wrapping c) Virus Detection d) Intrusion detection Answer: b Explanation: Key wrapping is a separate algorithm and not an application of hash fuctions.	LT1
15.	If the compression function is collision resistant, then so is the resultant iterated hash function. a) True b) False Answer: a Explanation: The statement is true. The problem of designing a secure hash function reduces to that of designing a collision resistant compression function.	LT1
16.	A larger hash code cannot be decomposed into independent subcodes. a) True b) False Answer: b Explanation: Hash codes can be decomposed into independent subcodes and this was the logic behind the meet in the middle attack.	LT2
17.	"Rabin Cryptosystem is a variant of the Elgamal Cryptosystem" 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 :3	**Unit Name** :Public Key Cryptography	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	b) False View Answer Answer: b Explanation: Rabin Cryptosystem is a variant of the RSA Cryptosystem.	
18.	In Elgamal cryptosystem, given the prime p=31. What is the respective plaintext character for C = (27, 20)? a) H b) L c) O d) M Answer: a Explanation: The Common factor for the calculation of C2 is e7 mod 31 = 257 mod 31 = 25. C = 17, 20); P = 20 X (1710)-1 mod 31 = 07; “07” = “H”.	LT2
19.	In Elgamal cryptosystem, given the prime p=31. Encrypt the message “HELLO”; use 00 to 25 for encoding. The value of C2 for character ‘O’ is a) 09 b) 07 c) 23 d) 27 View Answer Answer: a Explanation:The Common factor for the calculation of C2 is e7 mod 31 = 257 mod 31 = 25. P = “O” = 14; C1 = 37 mod 31 = 17; C2 = 14 x 25 mod 31 = 09; C = (17,09).	LT2
20.	Using Rabin cryptosystem with p=23 and q=7 Encrypt P=24 to find ciphertext. The Cipher text is a) 42 b) 93 c) 74 d) 12 Answer: b Explanation: Calculate n = p × q = 161 Plaintext P = 24 Ciphertext = C ≡ P2 (mod n) = 242 mod 161 = 93 mod 161 Ciphertext transmitted = 93.	LT1
21.	Which Cryptographic system uses C1 = (e1r) mod p and C1 = (e2r x P) mod p at the encryption side? a) Elgamal b) RSA c) Rabin d) Whirlpool	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 :3	**Unit Name** :Public Key Cryptography	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	Answer: a Explanation: The Elgamal cryptographic system uses the above formulae to compute the CT.	
22.	Sender chooses p = 107, e1 = 2, d = 67, and the random integer is r=45. Find the plaintext to be transmitted if the ciphertext is (28,9). a) 45 b) 76 c) 66 d) 13 Answer: c Explanation: P = [C2 (C1d)-1] mod p = 66.	LT2
23.	In Elgamal cryptosystem, given the prime p=31. Choose e1= first primitive root of p and d=10, calculate e2. a) 24 b) 36 c) 25 d) 62 Answer: c Explanation: We choose e1=3 (a primitive root of p = 31) and d=10. Then we have e2 = 310 mod 31 = 25.	LT2
24.	In Elgamal cryptosystem, given the prime p=31. Encrypt the message “HELLO”; use 00 to 25 for encoding. The value of C2 for character ‘L’ is a) 12 b) 07 c) 20 d) 27 Answer: d Explanation:The Common factor for the calculation of C2 is e7 mod 31 = 257 mod 31 = 25. P = “L” = 11; C1 = 37 mod 31 = 17; C2 = 11 x 25 mod 31 = 27; C = (17,27).	LT2
25.	For a 150-bit message and a 10-bit MAC, how many values are the MAC value dependent on? a) 2140 b) 2150 c) 215 d) 210 Answer: a Explanation: 2150/210 = 2140.	LT2
26.	MACs are also called a) testword b) checkword c) testbits d) none of the mentioned	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 :3	**Unit Name** :Public Key Cryptography	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	Answer: d Explanation: Another term for MACs are tags(or check sum).	
27.	MAC is a a) one-to-one mapping b) many-to-one mapping c) onto mapping d) none of the mentioned Answer: b Explanation: MACs are many to one mapping, which makes it tougher for the intruder for cryptanalysis.	LT1
28.	For an n-bit tag and a k-bit key, the level of effort required for brute force attack on a MAC algorithm is a) 2k b) 2n c) min(2k,2n) d) 2k/2n Answer: c Explanation: The level of effort required for brute force attack on a MAC algorithm is min(2k,2n).	LT2
29.	For a 100 bit key and a 32 bit tag, how many possible keys can be produced in the 3rd round? a) 24 b) 232 c) 216 d) 264 Answer: a Explanation: First round: 100 – 32 = 68 Second round: 68 – 32 = 36. Third round: 36 – 32 = 4. Therefore 24 keys can be produced by the third round.	LT2
30.	Confidentiality can only be provided if we perform message encryption before the MAC generation. a) True b) False Answer: b Explanation: Confidentiality can be provided even if we perform message encryption after the MAC generation.	LT2
31.	1. Cryptographic hash functions execute faster in software than block ciphers. a) Statement is correct b) Statement is incorrect c) Depends on the hash function	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 :3	**Unit Name** :Public Key Cryptography	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	d) Depends on the processor Answer: d Explanation: The execution time varies from processor to processor for different cryptographic systems.	
32.	What is the full-form of CMAC? a) Code-based MAC b) Cipher-based MAC c) Construct-based MAC d) Collective-based MAC Answer: b Explanation: CMAC stands for cipher-based message authentication code.	LT1
33.	Which mode of operation is used in the DAA? a) output feedback mode b) electronic code block mode c) cipher block chaining mode d) cipher feedback mode Answer: c Explanation: The DAA is an algorithm based on the DES cipher block chaining mode.	LT2
34.	What is the value of opad in the HMAC structure? a) 00111110 b) 00110010 c) 10110110 d) 01011100 Answer: d Explanation: opad is 5C in hexadecimal.	LT1
35.	Data Authentication Algorithm (DAA) is based on a) DES b) AES c) MD-5 d) SHA-1 Answer: a Explanation: The DAA is an algorithm based on the DES cipher block chaining mode.	LT2