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 :4	**Unit Name** :Message Authentication & Integrity	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

S.No	Objective Questions (MCQ /True or False / Fill up with Choices)	BTL
1.	What is the effectiveness of an n-bit hash value? a) 2n b) 2-n c) 22n d) 2-2n View Answer Answer: b Explanation: When an n-bit hash value is used its effectiveness is 2^-n, that is, the probability that a data error will result in an unchanged hash value is 2-n.	LT2
2.	A function that is second pre-image resistant is also collision resistant. a) True b) False View Answer Answer: b Explanation:The statement is false. A function that is collision resistant is also second image resistant.	LT1
3.	For an m bit hash value, if we pick data blocks at random we can expect to find two data blocks with the same hash value within ____ attempts. a) 2m b) 2(m-1) c) 2(m/2) d) (2m) – 1 View Answer Answer: c Explanation: This is known as the birthday paradox. If we choose random variables from a uniform distribution in the range 0 through N-1, then the probability that a repeated element is encountered exceeds 0.5 after root (N) choices have been made.	LT1
4.	Which attack requires the least effort/computations? a) Pre-image b) Second Pre-image c) Collision d) All required the same effort View Answer Answer: c Explanation: Due to the birthday paradox it requires 2(m/2) computations only.	LT2
5.	For an m-bit value, the adversary would have to try _____ values to generates a given hash value h. a) 2m b) 2(m-1) c) 2(m/2) d) (2m) – 1 View Answer Answer: b	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 :4	**Unit Name** :Message Authentication & Integrity	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	Explanation: The adversary would have to try 2(m-1) values to generates a given hash value h.	
6.	What is the effectiveness of a 128 bit hash value? a) 2-64 b) 264 c) 2-112 d) 2-128 View Answer Answer: c Explanation: In most normal text files, the high order bit of each octet is always zero. So if a 128 bit hash value is used, instead of an effectiveness of 2-128, the hash function will have an effectiveness of 2-112.	LT2
7.	We define collision as: A collision occurs if we have x=y and H(x) = H(y). a) True b) False View Answer Answer: b Explanation: A collision occurs if we have x not equal to y and H(x) = H(y).	LT1
8.	Public key encryption/decryption is not preferred because a) it is slow b) it is hardware/software intensive c) it has a high computational load d) all of the mentioned Answer: d Explanation: Due to high computational load (thus being slow) public key systems are not preferred for large cryptosystems and large networks.	LT1
9.	Which one of the following is not a public key distribution means? a) Public-Key Certificates b) Hashing Certificates c) Publicly available directories d) Public-Key authority Answer: b Explanation: Hashing certificates is some I just made up. It doesn't exist noob.	LT2
10.	What is the PGP stand for? a) Permuted Gap Permission b) Permuted Great Privacy c) Pretty Good Permission d) None of the mentioned Answer: d Explanation: PGP stands for Pretty Good Privacy.	LT2
11.	Which systems use a timestamp? i) Public-Key Certificates ii) Public announcements	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 :4	**Unit Name** :Message Authentication & Integrity	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	iii) Publicly available directories iv) Public-Key authority a) i) and ii) b) iii) and iv) c) i) and iv) d) iv) only Answer: c Explanation: Public announcements and Public Certificates involve the use of timestamps.	
12.	Which of these systems use timestamps as an expiration date? a) Public-Key Certificates b) Public announcements c) Publicly available directories d) Public-Key authority Answer: a Explanation: Public key certificates use timestamps as expiration dates.	LT1
13.	Which system uses a trusted third party interface? a) Public-Key Certificates b) Public announcements c) Publicly available directories d) Public-Key authority Answer: a Explanation: Public-Key certificates use a trusted third party interface.	LT1
14.	Which of the following public key distribution systems is most secure? a) Public-Key Certificates b) Public announcements c) Publicly available directories d) Public-Key authority Answer: a Explanation: Public certificates are the most secure key distribution/management systems right now.	LT2
15.	PGP makes use of which cryptographic algorithm? a) DES b) AES c) RSA d) Rabin Answer: c Explanation: PGP recommends the use of RSA.	LT2
16.	USENET is related to which of the following Public Key distribution schemes? a) Public-Key Certificates b) Public announcements	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 :4	**Unit Name** :Message Authentication & Integrity	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	c) Publicly available directories d) Public-Key authority Answer: b Explanation: Many PGP users append their public key to messages that they send to public forums, such as USENET and Internet mailing lists.	
17.	Publicly Available directory is more secure than which other system? a) Public-Key Certificates b) Public announcements c) Public-Key authority d) None of the mentioned Answer: b Explanation: Publicly Available directory is more secure than Public announcements.	LT1
18.	Extensions were added in which version? a) 1 b) 2 c) 3 d) 4 Answer: c Explanation: Extensions to the X.509 certificates were added in version 3.	LT1
19.	"Conveys any desired X.500 directory attribute values for the subject of this certificate." Which Extension among the following does this refer to? a) Subject alternative name b) Issuer Alternative name c) Subject directory attributes d) None of the mentioned Answer: c Explanation: The Subject directory attributes has the function of conveying any desired X.500 directory attribute values for the subject of this certificate."	LT2
20.	Certificates generated by X that are the certificates of other CAs are Reverse Certificates. a) True b) False Answer: a Explanation: The statement is true. Certificates of X generated by other CAs are forward certificates.	LT2
21.	6. It is desirable to revoke a certificate before it expires because a) the user is no longer certified by this CA b) the CA's certificate is assumed to be compromised c) the user's private key is assumed to be compromised d) all of the mentioned	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 :4	**Unit Name** :Message Authentication & Integrity	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	Answer: d Explanation: All of the options are true with regard to revocation of a certificate.	
22.	7. CRL stands for a) Cipher Reusable List b) Certificate Revocation Language c) Certificate Revocation List d) Certificate Resolution Language Answer: c Explanation: CRL stands for Certificate Revocation List.	LT1
23.	Which of the following is not a part of an Extension? a) Extension Identifier b) Extension value c) Criticality Indicator d) All of the mentioned constitute the Extension Answer: d Explanation: Extension Identifier, Extension value and the Criticality Indicator all constitue the Extension header.	LT1
24.	The criticality indicator indicates whether an extension can be safely ignored. a) True b) False Answer: a Explanation: The statement is true.	LT2
25.	The subject unique identifier of the X.509 certificates was added in which version? a) 1 b) 2 c) 3 d) 4 Answer: b Explanation: The subject unique identifier was added in the 2nd version.	LT2
26.	Which of the following is not an element/field of the X.509 certificates? a) Issuer Name b) Serial Modifier c) Issuer unique Identifier d) Signature Answer: b Explanation: Serial Modifier is not an element/field of the X.509 certificates.	LT2
27.	Suppose that A has obtained a certificate from certification authority X1 and B has obtained certificate authority from CA X2. A can use a chain of certificates to obtain B's public key. In notation of X.509, this chain is represented in the correct order as –	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 :4	**Unit Name** :Message Authentication & Integrity	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	a) X2 X1 X1 B b) X1 X1 X2 A c) X1 X2 X2 B d) X1 X2 X2 A Answer: c Explanation: The correct representation would be X1 X2 X2 B.	
28.	Larger networks would prefer a full decentralization. a) True b) False Answer: b Explanation: Full decentralization is not practical for larger networks as there would be too many connections.	LT1
29.	Which of these is not a type of session key? a) PIN-encrypting key b) File-encrypting key c) Session encrypting key d) Data encrypting key Answer: c Explanation: Data, PIN and File are the different session keys.	LT2
30.	Which session key is used for electronic funds transfer and point of sale applications? a) Data-encrypting key b) File-encrypting key c) PIN-encrypting key d) None of the mentioned Answer: c Explanation: PIN-encrypting key is the session key which is used for electronic funds transfer and point of sale applications.	LT2
31.	Sometimes a simple tag is introduced along with the session key. This tag has 8 bits. Which of the following options is wrong? a) One bit indicates whether the key is a session key or a master key b) One bit indicates whether the key can be used for encryption c) Three bit indicates whether the key can be used for decryption d) Remaining bits are for future use Answer: c Explanation: One bit indicates whether the key can be used for decryption.	

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 :4	**Unit Name** :Message Authentication & Integrity	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

32.	"Meet in the middle attack" and "man in the middle attack" are the same. a) True b) False Answer: b Explanation: Man is the middle attack is different from meet in the middle attack.	
33.	Which of the following is required to find the session key? i) Control Vector ii) Master Key iii) Encrypted session Key a) i) b) i) and ii) c) i) and iii) d) i) ii) and iii) Answer: d Explanation: We require all three to find the session key.	
34.	Which is the correct representation for session key recovery for the plain text? a) D ([Km XOR H], E([Km XOR H], Ks) b) D([Km XOR H],Ks) c) D ([Km XOR H], E([Km XOR H]) d) None of the mentioned Answer: a Explanation: The correct representation is D([Km XOR H], E([Km XOR H], Ks), to recover the session key.	
35.	"Meet in the middle attack" is an attack a) where the timing required for the attack via brute force is drastically reduced b) where the adversary uses 2 or more machines to decrypt thus trying to reduce the time c) where messages are intercepted and then either relayed or substituted with another message d) where cryptanalysis takes lesser time than the brute force decryption Answer: c Explanation: "Meet in the middle attack" is an attack where messages are intercepted and then either relayed or substituted with another message.	
36.	Hash Value = H = h(CV) Key Input = Km XOR H Ciphertext = E([Km XOR H],Ks) What is CV here? a) Cipher vector	

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 :4	**Unit Name** :Message Authentication & Integrity	Date	30.09.2020

OBJECTIVE TYPE QUESTION BANK

	b) Current vector c) Control vector d) None of the mentioned Answer: c Explanation: CV is known as Control Vector.	