

KLNCIT	CLASS TEST ANSWER KEY	Format No.:ACD11A-I
		Issue No. :01
		Rev No. :00

Subject Code/Subject Name : CS6701-Cryptography and Network Security **Class Test No. : II**

Year and Branch : IV/CSE & IT **Total marks** : 25

Date : 04.09.2017 **Duration** : 50 mins.

I. Course outcomes, Question Number, Marks

COs	CO1	CO2	CO3	CO4	CO5
Q.Nos		-	1,2,3,4,5, 6(a)/6(b)	-	-
Marks (Max)		-	25	-	-

II. Knowledge skill outcomes

Level	Remember (K1)	Understand (K2)	Apply (K3)	Analysis (K4)	Evaluate (K5)	Create (K6)
Q.Nos	1,3	2, 5, 6(a)/6(b)	4	-	-	-
Marks (Max)	4	19/19	2	-	-	-

PART – A

5 × 2 = 10 Marks

Answer all the questions

1. List some authentication requirements.

(K1)

Disclosure

Traffic analysis

Masquerade

Content modification

Sequence modification

Timing modification

Source repudiation

Destination repudiation

2. Define Birthday Attack.

(K2)

A birthday attack is a cryptanalytic technique. Birthday attacks can be used to find collisions in a cryptographic hash function. For instance, suppose we have a hash function which, when supplied with a random input, returns one of k equally likely values.

3. What are the design objectives of HMAC?

(K1)

To use available hash function

To allow for easy replaceability of the embedded hash function

To preserve the original performance of the hash function without incurring a significant degradation

To use and handle keys in a simple way

To have a well understood cryptographic analysis of the strength of the authentication mechanism

4. On the basis of the digital signature properties, formulate the requirements of digital signature.

(K3)

The signature must be a bit pattern, depends on the message being signed

The signature must use some information unique to sender, to prevent forgery and denial

It must be relatively easy to produce digital signature

It must be relatively easy to recognize and verify digital signature

5. Write short notes on direct digital signature and arbitrated digital signature.

(K2)

DDS – involves communication parties

ADS – Every signed message from sender, X to a receiver, Y goes first to an arbiter

6. (a) Explain in detail process of SHA-1 algorithm with neat diagrams and outline the parameters used for comparing MD5 and SHA-1. (K2)

Logic – SHA-1

- Append padding bits
- Append length
- Initialize Message Digest buffer
- Process message in 512-bit (16-word) blocks
- Output

SHA-1 Compression function

Comparison of SHA-1 and MD5

- Security against brute force attack
- Security against cryptanalysis
- Speed
- Simplicity and compactness
- Little-endian versus big-endian architecture

(OR)

6.(b) Explain with an example the Elgamal digital signature algorithm and Schnorr digital signature algorithm. (K2)

Elgamal Digital signature:

- Generating public elements
- Signing the message / creating the signature
- Verifying the signature
- Example

Schnorr Digital Signature

- Generating public elements
- Signing the message / creating the signature
- Verifying the signature

Faculty Incharge

Course Coordinator

HOD/IT