AKGEC/IAP/FM/02

Ajay Kumar Garg Engineering College, Ghaziabad

Department of CSE

Sessional Test-2

Course: B.Tech	Semester: VII
Session:2017-18	Section: CS-1, 2, 3, IT-I, J
Subject: Cryptography & Network Security	Sub. Code: NIT-701
Max Marks: 50	Time: 2 hours

Note : Answer **all** the Sections.

Section-A

A. Attempt **all** the parts. **(5 X 2 = 10)**

(1) What are the requirements for hash functions?

(2) What requirements should a digital signature scheme satisfy?

(3) Compare and contrast AES with DES for message encryption.

(4) Find the value of 3^{201} mod 11.

(5) Explain the compression function of MD5 algorithm for hash calculation.

Section-B

B. Attempt **all** the parts. (5 X 5 = 25)

(6) State and prove Euler's theorem. Compute Ø(300).

(7) Explain Euclid's algorithm. Find gcd(1970,1066) using Euclid's algorithm.

(8) What are the securities of RSA? Perform encryption and decryption using RSA for p=17, q=11, if the message M=88.

(9) Explain Elgamal scheme of digital signature generation and verification.

(10) Discuss the logical structure, components and algorithmic steps of SHA-512.

Section-C

C. Attempt **all** the parts. (2 X 7.5 = 15)

(11) Explain Chinese Remainder Theorem, use it to solve: X≡2 mod 3, X≡3 mod 5, X≡2 mod 7.

(12) Write the signature generation and verification process of digital signature algorithm of Digital Signature Standard (DSS).