Subject: CRYPTOGRAPHY & NETWORK SECURITY

Time: 3 Hours **Max. Marks: 100**

DECEMBER 2010

NOTE: There are 9 Questions in all.

- **Question 1 is compulsory and carries 20 marks. Answer to Q.1 must be written in the space provided for it in the answer book supplied and nowhere else.**
- **The answer sheet for the Q.1 will be collected by the invigilator after half an hour of the commencement of the examination.**
- **Out of the remaining EIGHT Questions answer any FIVE Questions. Each question carries 16 marks.**
- **Any required data not explicitly given, may be suitably assumed and stated.**

Q.1 Choose the correct or the best alternative in the following: (2×10)

a. If we want to ensure the principle of _____, the contents of a message must not be modified while in transit.

(A) Confidentiality **(B)** Authentication
(C) Integrity **(D)** Non-repudiation

b. The technique of decoding message from non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format is called as _____

(A) Cryptography **(B)** Cryptanalysis
(C) Cryptology **(D)** Cryptogram

c. Initial key supplied to DES is of size ____ bits

(A) 32 **(B)** 56
(C) 64 **(D)** 128

d. 7^5 mode 119 is

(A) 21 **(B)** 7
(C) 105 **(D)** 28

e. If X and Y want to communicate securely with each other, Y must not know _____.

(A) X's Private Key **(B)** X's Public Key
(C) Y's Private Key **(D)** Y's Public Key

f. When two different message digests have the same value, it is called as _____ .

(A) Attack
(B) Collision
(C) Hash
(D) Digital signature

g. _____ works on block mode

(A) CFB
(B) OFB
(C) CCB
(D) CBC

h. _____ are very crucial for the success of asymmetric key cryptography

(A) Integers
(B) Positive numbers
(C) Prime numbers
(D) Fractions

i. _____ is a stream cipher

(A) DES
(B) AES
(C) RSA
(D) RC4

j. SSL Layer is located between _____ and _____ .

(A) Transport layer, Network layer
(B) Application layer, Transport layer
(C) Data Link layer, Physical layer
(D) Network layer, Data Link layer

Answer any FIVE Questions out of EIGHT Questions.
Each question carries 16 marks.

Q.2 a. With a proper diagram, bring out the taxonomy of security goals and the categorization of various security attacks while realizing these goals. **(9)**

b. Provide the Extended Euclidean Algorithm to find the multiplicative inverse of an integer. Using the algorithm, find the multiplicative inverse of 550 in Z_{1769}. **(7)**

Q.3 a. Explain with a neat diagram how an attacker can perform chosen-cipher text attack. **(5)**

b. Using Playfair cipher encrypt the message "My name is Jui" with the key given by the matrix given below: **(5)**

H	A	R	S	B
C	D	E	F	G
I/J	K	L	M	N
O	P	Q	T	U
V	W	X	Y	Z

c. With the appropriate diagram, explain the one round Fiestel cipher. Also p... that encryption and decryption of the cipher are inverses of each other. **(6)**

Q.4 a. Briefly explain how Meet-in- the-Middle attack can be performed on Double DES. Also explain how Triple DES can overcome this attack. **(10)**

b. DES uses unique sub-key for every 16 rounds in the encryption and decryption operations, even though the cipher inputs only one key. Explain the sub-key generation process. **(6)**

Q.5 a. When modern ciphers are used for encryption in real life applications, different modes of cipher operations are used. Justify the need of different modes of operation. Describe the encryption operation using any one of the modes of operation. **(8)**

b. Assume that p = 7, q = 17, e = 5 and 0 to 25 for English alphabets. What are the keys used by RSA for enciphering? Along with the required steps show how to encrypt the alphabet 'T' and decrypt it back. **(8)**

Q.6 a. Use appropriate diagrams and explain the difference between Modification Detection Code and Message Authentication Code. **(6)**

b. What is the function of SHA-512? Provide its important features. Briefly explain the outline of its compression function. **(10)**

Q.7 a. Differentiate between conventional signature and digital signature. **(4)**

b. Explain how a Certification Authority distributes the public key certificates. What is the deficiency of this method? How does X.509 overcome this deficiency? Explain the format of X.509 certificate. **(12)**

Q.8 a. Justify the need for using two types of key rings in PGP. Explain the structure of the two key rings. **(8)**

b. Explain the content type used in S/MIME for obtaining the following security service
(i) Data Authentication
(ii) Message integrity **(8)**

Q.9 a. In the internet protocol stack, show the location of Secure Socket Layer protocol and briefly explain the various services offered by it. **(6)**

b. Explain briefly the various phases of handshake protocol in Secure Socket Layer protocol. **(10)**