O/E/TX

Reg. No:

Final Assessment Test – May 2024

VIT® Vellore Institute of Technology

Course: **BCSE309L - Cryptography and Network Security**

Class NBR(s): **0660/0663/0667/0671/0676/0679/ 0682/0683/0685/0688/0689/0691/0695/0698/0701/ 0703/0705/0706/0709/0713/0715/0718/0721/0748**

Slot: **E1+TE1**

Time: **Three Hours**

Max. Marks: **100**

- **KEEPING MOBILE PHONE/ELECTRONIC DEVICES EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE**
- **DON'T WRITE ANYTHING ON THE QUESTION PAPER**

Answer any TEN Questions

(10 X 10 = 100 Marks)

1. (a) Use Euler's theorem to find a number 'x' between 0 and 28 with x^{85} congruent to 6 modulo 35. **[5]**

   (b) Using Successive Squaring and reducing modulo 'n', calculate 2^{513} mod 10. **[5]**

2. (a) Find out whether the following relationship holds: 5 is a primitive root of 11. **[4]**

   (b) The child of a number theorist is sorting a large pile of pennies (worth less than a dollar) into groups of 3 pennies each. At the end, the child reports that 2 pennies are left over. The child starts over, instead sorting the pennies into groups of 4, and reports that 1 penny is left over. The child starts over again, sorting the pennies into groups of 11, and reports that 7 pennies are left over. The number theorist didn't originally know how many pennies were in the pile, but at this point, she speaks up. What does she say? Did the child make a mistake in sorting the pennies? Or does the number theorist have enough information to tell how many pennies are in the pile? **[6]**

3. (a) Differentiate between a stream and a block cipher. How can one make these differences disappear? **[4]**

   (b) Consider a Feistel cipher composed of 16 rounds with a block length of 128 bits and a key length of 128 bits. Suppose that, for a given k, the key scheduling algorithm determines values for the first 8 round keys, k_1, k_2, ..., k_8, and then sets $k_9 = k_8$, $k_{10} = k_7$, $k_{11} = k_6$, ..., $k_{16} = k_1$

   Suppose you have a ciphertext c. Explain how, with access to an encryption result, you can decrypt 'c' and determine the plain text 'm' using just a single expression. **[6]**

4. Implement the Stream Cipher RC4 algorithm for the State vector S = 8 x 3-bits where the Key K = [1 2 3 6] and the Plaintext P = [1 2 2 2]. Find out the Cipher text C.

5. (a) The difficulty of breaking the RSA cipher is because of the difficulty of factorizing large numbers. To what do we owe the difficulty of breaking the Diffie-Hellman cipher? **[3]**

(b) Let E be the Elliptic Curve E: $y^2 = x^3 + x + 1$. Let P= (4,2) and Q= (0,1) be points on E modulo 5. Solve the Elliptic Curve Discrete Logarithm Problem for P and Q, finding a positive integer *n* such that Q = *n*P. [7]

6. Suppose in the HMAC algorithm, the Message M = "Hello" and the Key K = "Hi". Find out the 'S_i' and 'S_o' based on the Hex Conversion of ASCII characters where the length of the hash code 'n' is 4 bits. Also, finally convert the 'S_i' and 'S_o' sizes in terms of the MD5 variant.

ASCII Character	Hexadecimal	ASCII Character	Hexadecimal
A	41	a	61
B	42	b	62
C	43	c	63
D	44	d	64
E	45	e	65
F	46	f	66
G	47	g	67
H	48	h	68
I	49	i	69
J	4A	j	6A
K	4B	k	6B
L	4C	l	6C
M	4D	m	6D
N	4E	n	6E
O	4F	o	6F
P	50	p	70
Q	51	q	71
R	52	r	72
S	53	s	73
T	54	t	74
U	55	u	75
V	56	v	76
W	57	w	77
X	58	x	78
Y	59	y	79
Z	5A	z	7A

7. (a) Suppose we have a set of blocks encoded with the RSA algorithm and we don't have the private key. Assume $n = pq$, e is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with n. Does this help us in any way? [5]

(b) In the Diffie-Hellman protocol, each participant selects a secret number x and sends the other participant $\alpha^x \bmod q$ for some public number α. What would happen if the participants sent each other x^α for some public number α instead? Give at least one method Alice and Bob could use to agree on a key. Can Eve break your system without finding the secret numbers? Can Eve find the secret numbers? [5]

8. (a) In SHA-512, the size of the original message is 1250 bits. What will be the number of padding bits? [3]

(b) With the possible ways, explain in detail the Birthday Paradox's impact on Digital Signatures and Hash functions. [7]

9. Consider the ElGamal signature scheme with $p = 467$, $\alpha = 2$, and $X_a = 127$. Perform detailed signing and verification procedures for the hash of the message $h(M) = 100$ and $K = 213$.

10. (a) Use Kerberos-v4 to explain how the authentication service and the ticket-granting service are provided. [5]

(b) Identify three security threats concerning node authentication in a networked environment and, for each threat you have identified, explain the counter-measure used in the Kerberos-v4 protocol. [5]

11. (a) Explain why SSL/TLS is not really a single protocol, but a stack of protocols. Also, what are the different protocols in the SSL/TLS stack? [5]

(b) How is the security achieved in the IPSec Transport and Tunnel modes? Also, explain with a neat sketch, the role of AH and ESP. [5]

12. (a) Why does PGP maintain Key Rings with every user? Explain how PGP generates the messages with a neat sketch. [5]

(b) List the functions included in MIME to enhance the security and how are they processed. [5]

⇔⇔⇔ O/E/TX⇔⇔⇔