SRM University, Kattankulathur

Faculty of Engineering and Technology, Department of Information Technology

IT1117 - CRYPTOGRAPHY

Cycle Test – 2

Degree : B.Tech | Specialisation: IT

Year/Sem: III/V | **Date:.7/9/16**

Duration : 90 Minutes | Max. Marks: 50

Instructional Objectives covered in this test:

2.Acquire fundamental knowledge on the concepts of finite fields and number theory

3.Understand various block cipher and stream cipher models

Student outcomes covered in this test:

Outcome a: An ability to apply knowledge of computing and mathematics appropriate to the Information Technology.

Outcome j: An ability to use and apply current technical concepts and practices in the core information technologies.

Part-A [Answer any five questions] **(5x4=20 Marks)**

1. Define Galois field
2. Using Euclidean algorithm find the gcd(465,527)
3. Solve ø(24),ø(19),ø(125)
4. Explain DES key expansion.
5. Explain the generation of round keys for multiples of four in AES algorithm.
6. Write Miller Rabin algorithm

Part-B [Answer the question] **(2x15=30 Marks)**

7.a.i. Using extended Euclidean algorithm solve 550^{-1} mod 1769. (8 mark)

7.a.ii. Explain in detail about AES round layers (8 mark)

OR

7.b.i. PT=00110010,Key =10010000,P10=3 5 2 7 4 10 1 9 8 6,P8=6 3 7 4 8 5 10 9
IP=2 6 3 1 4 8 5 7,E/P =4 1 2 3 2 3 4 1,P4= 2 4 3 1

S0= $\begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix}$ S0= $\begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$

Encrypt the given plain text using S-DES algorithm

8. a. i. $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, $x \equiv 3 \pmod 7$ Solve x using Chinese Reminder Theorem (12 mark)

8. a. ii. Explain Output feedback mode (3 mark)

OR

8. b. Multiply using binary arithmetic in $GF(2^8)$ (8 mark)

i) $f(x)=x^6+x^4+x^2+x+1, g_1(x)=x^7+x+1$

ii) $f(x)=x^6+x^4+x^2+x+1, g_2(x)= x^6+ x^5+x+1$

iii) $f(x)=x^6+x^4+x^2+x+1, g_3(x)=x^7+ x^2+x+1$

Evaluation:

Question No.	Instructional Objective	Outcome	Max.Mark	Mark Obtained
1	IO2	a	4	
2	IO2	a	4	
3	IO2	a	4	
4	IO3	j	4	
5	IO3	j	4	
6	IO2	a	4	
7.a.i	IO2	a	8	
7.a.ii	IO3	j	8	
7.b	IO3	j	15	
8.a.i	IO2	a	12	
8.a.ii	IO2	a	3	
8.b.	IO2	a	15	
Total			50	

Outcome a: :Met/Not Met Outcome j: :Met/Not Met

Signature of Examiner:

****