Registration No : | | | | | | | | | | |

Total Number of Pages : 01 **M.Sc.I**

FMCE1002

10th Semester Regular Examination 2018-19

CRYPTOGRAPHY

BRANCH : M.Sc.I(MC)

Time : 3 Hours

Max Marks : 70

Q.CODE : F059

Answer Question No.1 which is compulsory and any FIVE from the rest.

The bold figures in the right hand margin indicate marks.

Q1 **Answer the following questions :** **(2 x 10)**

a) Define cryptosystems.

b) What is encryption and decryption functions?

c) What do you mean by randomized encryption?

d) Define alphabets and words.

e) What is the length of alphabet used in computing?

f) What is block ciphers and substitution ciphers?

g) Sketch block diagram of ECB mode.

h) Draw the logical table of exclusive or.

i) Define affine linear.

j) Let $A=\begin{pmatrix}1 & 2\\ 2 & 3\end{pmatrix}$ and $v=\begin{pmatrix}1 & 2\end{pmatrix}$ then find the value of Av.

Q2 **a)** Distinguish between symmetric and asymmetric cryptosystems. **(5)**

b) Encrypt and decrypt “Today is holiday” with key 5. **(5)**

Q3 **a)** Prove that S_n, the group of permutations of $\{0,1,...,n\}$, has order $n!$. **(5)**

b) Write all the elements of S_3. **(5)**

Q4 **a)** The number of integers 'a' prime to 'n' in the set $\{0,1,...,n-1\}$ for which a^k has a different order $\bmod p$ and $\bmod q$ is at least $(p-1)(q-1)/2$. **(5)**

b) Let a,u,v be positive real numbers. Then for $n\to\infty$ we have **(5)**

$$\psi(n^a, L_n[u,v]) = n^a L_n[1-u, -(a/v)(1-u)+o(1)].$$

Q5 **a)** For a prime divisor 'p' of 'n', let $\chi(p)$ be the discrete logarithm of α_p to the base γ_p. If $\chi=\chi(p)\bmod p^{e(p)}$. Then prove that χ is a discrete logarithm of α to the base γ. **(5)**

b) Solve $5^x \equiv 3 \bmod 2017$. **(5)**

Q6 For Encrypt the plaintext m=101100010100101 for the block cipher that applies bit permutations to bit vectors of length 4 using CBC mode with a permutation key. **(10)**

Q7 Discuss different types of attacks on cryptosystems. **(10)**

Q8 Discuss the ECB mode for encrypting long documents. **(10)**