M.E. COMPUTER SCIENCE & ENGINEERING- 2017
1st Year, 2nd Semester
CRYPTOGRAPHY

Time: Three hours   Full Marks: 100

Answer any ***five*** questions

1. (a) When is a permutation on a finite set called a *cycle*? Explain how such permutations can be described in *one line notation*. Represent all the permutations of the set {1,2,3} in one line notation.
   Prove that $(a\ b)(b\ c) = (a\ b\ c)$.
   (b) Prove that the set of all permutations of the set {1,2,3} forms a group with respect to function composition by calculating the group operation table.
   Show details of calculation for each entry of the table.
   Is this group *commutative*? What are the total number of elements in this group?

   7+13

2. (a) Explain how a^n is defined when a is an element of a group and n is an arbitrary integer.
   (b) Prove the following identities where a is an element of a group and m, n are arbitrary integers :
   i) $a^m a^n = a^{m+n}$
   ii) $(a^m)^n = a^{mn}$.

   3+17

3. (a) Let $f : X \to X$ be a function where X is a *finite* set. Prove that f is injective if and only if it is surjective.
   Will this result be true if X is *infinite*?
   (b) A block cipher is to be designed which will map ℓ-bit plaintexts to ℓ-bit ciphertexts. How many different encryption functions can be supported by this block cipher?
   Usually block ciphers allow only a small fraction of all these encryption functions to be used – explain why.
   (c) Describe the scheme of generation of *round* keys from the user key in **DES**. Also explain how the round keys can be generated in *reverse* order.
   Give the basic circuit diagram for a round of **DES**. Explain how the same circuit can be used for encryption as well as decryption.

   5+4+11

4. (a) Describe an algorithm for fast *exponentiation* in an arbitrary group with necessary explanation. Calculate its time complexity.
   Illustrate your algorithm by showing the details of calculation of a^{25}.
   (b) Give definition of a *monoid*.
   Prove that in a monoid if an element has a left inverse and also a right inverse, then it has a both sided inverse. Also this element cannot have any other inverse left or right.
   Prove that in a finite monoid if an element has a one sided inverse, then it also has a both sided inverse.

   12+8

5. (a) What is a *Digital Signature* system? What are its desirable properties? Give block diagrams of *signing* and *verifying* steps.
   How does it differ from manual signature scheme?
   (b) Describe the ElGamal digital signature scheme and its verification scheme.

(c) Describe the **DSA** (Digital Signature Algorithm) scheme and its verification scheme. Explain in what sense this scheme is an improvement over the ElGamal scheme.

4+8+8

6. (a) Explain what is a primitive element of Z_p^* when p is a prime.
   In Z_{17}^*, find out which of the elements 2 or 3 is a primitive element.

   (b) Describe the **Diffie-Hellman** scheme of key agreement between two parties.
   In a Diffie-Hellman scheme the parameters are $p = 23, g = 7$. The secret numbers chosen by the two users are 3 and 5. What is the value of their common secret key?

   (c) Let a be an element of order r in a group G.
   Prove that $a^i = a^j$ if and only if $i = j \mod r$.

6+6+8

7. (a) Prove that every number in the range $0 \leq x < m^2$ may be uniquely represented by an ordered pair of numbers (i, j) with $0 \leq i, j < m$.

   (b) Describe the **Baby Step Giant Step** algorithm for finding the Discrete Logarithm with necessary explanations.

   (c) Illustrate your algorithm by finding the discrete log of 11 to the base 3 in Z_{17}^*.

5+10+5