M.TECH COMPUTER TECHNOLOGY - 2018
2nd Year, 2nd Semester
CRYPTOGRAPHY

Time: Three hours | Full Marks: 100

Answer any ***five*** questions

1. Let a, b, c be three positive integers. Prove that
   (a) $\gcd(ab, ac) = a \gcd(b, c)$.
   (b) If $\gcd(a, b) = 1$ then $\gcd(a, bc) = \gcd(a, c)$.
   (c) Hence describe an algorithm whch calculates gcd of two numbers without any division operation. Prove its correctness using the above results.
   Show the steps of this algorithm for the inputs 19 and 46.

6+6+8

2. (a) Let a, b, c be three positive integers. Prove that $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$ implies $\gcd(a, bc) = 1$.
   (b) Define the set Z_m^* when m is a positive integer.
   Prove that it forms a group under multiplication mod m.
   (c) What is a divisor of zero in Z_m?
   Prove that for each element of Z_m *exactly one* of the following is true :
   - it has a unique multiplicative inverse mod m.
   - it is a divisor of zero.

5+8+7

3. (a) Explain the differences between *block* and *stream* ciphers. Compare their advantages.
   (b) Explain the basic principles of a stream cipher.
   What is the period of a stream cipher? Explain its significance.
   (c) Describe the operation of the stream cipher **RC4**.
   If the key for a **RC4** cipher is chosen to be 256 bytes all 0, show the initial permutation states upto 10 iterations.

4+4+12

4. Let X, Y be finite sets.
   (a) Prove that if there exists a 1-1 function from X to Y, then $|X| \leq |Y|$.
   (b) Prove that if there exists an onto function from X to Y, then $|X| \geq |Y|$.
   (c) Let $|X| = |Y|$. Prove that a function $f : X \to Y$ is $1 - 1$ if and only if it is onto.
   Hence explain if the block length of a block cipher is n, what should be the length of the corresponding cipher text block.
   Find out how many different encryption functions exist when the block length of the block cipher is n.
   Are all such functions useful?

4+4+12

5. (a) Describe the **Feistel Cipher** scheme.
   Prove that it defines a 1-1 mapping and can be inverted using the same circuit that was used for encryption.
   Explain carefully, why iteration is necessary in using such schemes.
   (b) Describe the **DES** scheme, with details of the *expansion* function used by it.

(c) What are **S-boxes**? What are their desirable properties?

5+10+5

6. (a) Describe the differences between *Private Key* and *Public Key* cryptosystems. Compare their advantages.

   (b) Describe the RSA cryptosystem. Prove the correctness of its decryption process, outlining the group theoretic properties used.

   (c) In a certain RSA system, the two primes chosen were 3 and 11.
   Find out all possible pairs of valid encryption, decryption coefficients (e, d) in this system.

7+10+3

7. (a) Describe the **Discrete Logarithm** Problem.
   Find the Discrete Logarithm of 11 in Z_{13}^* to the base 2.

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

5+15