Mid term Examination M.Sc. (Second Semester) Cryptography & Network Security Full Marks: 30

Answer all Questions

a. Encrypt the message "meet me at hill" using the Hill cipher with the key .

9	5
4	7

Show your calculations and the result. Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext.

b. "Hill cipher succumbs to a known plaintext attack if sufficient plaintext–ciphertext pairs are provided." --- Comment with necessary Justification.

c. Comment on the performance of Public Key Cryptography and Secret Key Cryptography for protecting spoofing attack.

d. Find the Multiplicative inverse of 23 in Z_{100}.

e. The encryption Key in a transposition cipher is [3,2,6,1,5,4]. Find the decryption key.

f. Consider a cipher. The cipher is affine, but the keys depend on the position of the character in the PT. If the PT character to be encrypted is in position i, the keys are defined as

The multiplicative key is the (i mod 12) th element in Z_{26}^*

The additive key is the (i mod 26)th element in Z_{26}

Encrypt the message "Exam is fun" using this cipher.

g. Illustrate the meet in the middle attack through an example.

h. Consider a desktop publishing system used to produce documents for various organizations.

- Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.
- Give an example of a type of publication in which data integrity is the most important requirement.
- Give an example in which system availability is the most important requirement.

[6+2+2+5+1+5+6+3 = 30]