

Assignment -1
Cryptography and Network Security (MC 407)
Department of Applied Mathematics
Delhi Technological University

August 2021

1. Describe different types of attacks threatening the confidentiality of information.
2. Describe security services defined by ITU-T (X.800) related to the security goals and attacks.
3. Describe security mechanism recommended by ITU-T (X.800) to provide the security services.
4. Using the given Playfair matrix:

X	F	W	I/J	K
U	N	O	P	E
A	V	H	M	Y
Q	B	Z	R	G
D	S	T	L	C

Encrypt this message: “Must see you over Cadogan West Coming at once”.

5. How many possible keys does the Playfair cipher have? Ignore the fact that some keys might produce identical encryption results. Now take into account the fact that some Playfair keys produce the same encryption results. How many effectively unique keys does the Playfair cipher have?
6. Use the Vigenère cipher with keyword “LEG” to encipher the message “starttheambush”.
7. Use the Playfair cipher to encipher the message “The key is hidden under the door pad”. The secret key can be made by using the keyword “PLAYFAIR”.
8. Eve secretly gets access to Alice’s computer and using her cipher types “abcdefghij”. The screen shows “CABDEHFGIJ”. If Eve knows that Alice is using a keyed transposition cipher, answer the following questions:
 - a. What type of attack is eve launching?
 - b. What is the size of permutation key?
9. The following ciphertext is obtained using a substitution cipher. Give a clearly written description of steps you followed to decrypt the ciphertext.
EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCKQPKUGKMGOLICGINC
GACKSNISACYKZSCKXECJCKSHYSXCGOIDPKZCNKSHICGIWYGKKGKGOLDSILKGOIU
SIGLEDSPWZUGFZCCNDGYYSFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNSACIGOI
YCKXCJUCIUZCFZCCNDGYYSFEUEKUZCSOCFZCCNCIACZEJNCSEHFZEJZEGMXCYHCJU
MGKUCY
(Hint: F decrypts to w)
10. The plaintext “letusmeetnow” and the corresponding ciphertext “HBCDFNOPIKLB” are given. You know that the algorithm is a Hill cipher, but you don’t know the size of the key. Find the key matrix.
11. Assume a one-time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3, 19, 5..., then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on. Encrypt the plaintext “SENDMOREMONEY” with the key stream 9, 0, 1, 7, 23, 15, 21, 14, 11, 11, 2, 8, 9.

End