Q1) To understand the security attacks, many aspects must be considered, Differentiate with figures between (Interruption, Modification, and Fabrication) attacks? (16-points).

ANSWER:

When an asset of the system is destroyed or becomes unavailable or unusable, it results into an ***Interruption***, see **Figure 1-2**. This is considered as an attack on the (***Availability)***. **Examples** include the destruction of a piece of hardware such as hard disc, communication line cut or disabling of file management system.

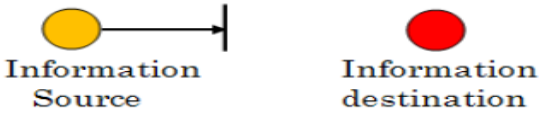

Fig. 1-2 Interruption of information flow.

When an unauthorized party not only gains an access to but tempers with an asset, it results into ***Modification***, see Figure 1-4. This is considered as an attack on the (***Integrity***). Examples include changing values in a data file or altering a program.

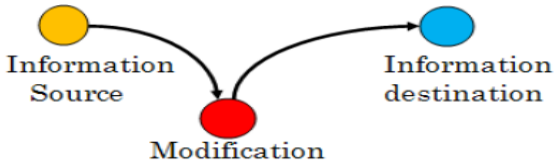

Fig. 1-4 Modification of information.

When an unauthorized party insert counterfeit object into the system, it results into ***Fabrication***, see **Figure 1-5**. This is considered as an ***(Authenticity)***. **Examples** include insertion of spurious messages in a network or the addition of records to a file.

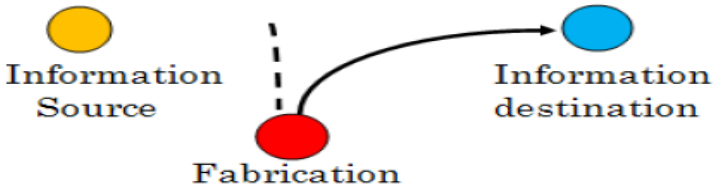

Fig. 1-5 Fabrication of information.

Q2) Decryptes using Caesar depends on the following facts:

KEY=8; ALPHABET=" abcdefghijklmnopqrstuvwxyz0123456789"; Ciphertext=" mvkwlqvoa8aa**".**

ANSWER:

This can be done M= (C-KEY) Mod 35→ Plain Text=" encoding2022".

Q3) Decryptes using Playfair the Ciphertext=" DBQOLCCABW" using Keyword=" cocomelon"?

ANSWER:

1. **We must delete redundance char from keyword: cocomelon→ comeln**
2. **Draw the 5X5 Playfair rectangle as follow:**
3. Playfair square

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

4. **DB→ BA, QO→RC, LC→EL, CA→ ON, BW→AX**
5. **THE PLAIN TEXT= BARCELONA X.**

Q4) In Hill Cipher answer the following:

a) Hill Cipher is Transposition Method? (True, False). **Answer FALSE.**
b) Encryption in hill cipher is done using (Matrix inversion, **Matrix multiplication**, 5X5 Matrix).
c) Give an example how can you extend Alphabet in Hill Cipher?

ANSWER: we can extend the alphabet by adding any char or numbers even special characters.