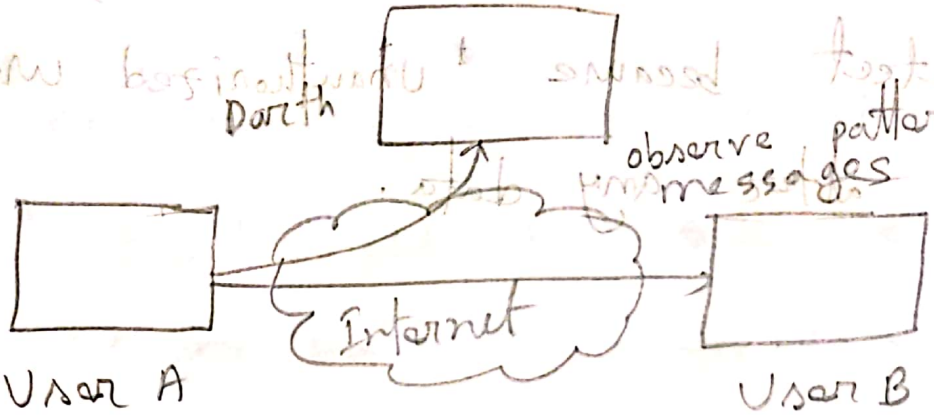
Ans to the Q:No-1

Traffic analysis:



Here User A send a message to User B and unauthorized user Parth, observe the message pattern.

It is categorize as a type of passive attack because message is not altered or modified, message is just read by a unauthorized person.

That's why it is called passive attack. passive attack are very difficult to detect because unauthorized user don't alter any data.

Ans: to the Q: No-2

* Different types of data confidentiality defined in X.800 security services:

confidentiality is the protect of data from passive attack. Different types of confidentiality in given below:

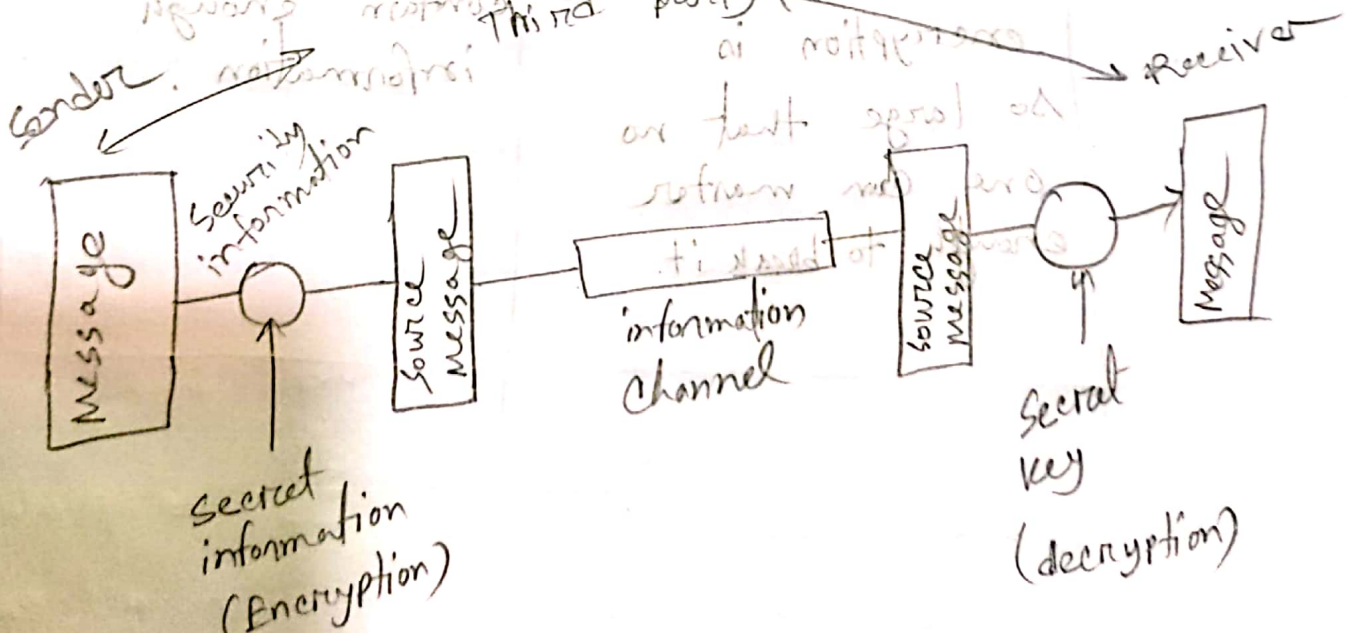
i) connection confidentiality: The protection of all user data in a connection

ii) connectionless confidentiality: protection of user data in a single data block.

iii) Selective field confidentiality: protection of selective-field within the user data in a connection.

iv) Traffic-flow: protection of information that might be derived from observation of traffic flows.

Ans: to Q: No-3



Ans: to the Q: No-4

Unconditionally secure	computationally secure
i) No matter how much chipper text is available.	i) costs of breaking cipher exceeds value of encrypted information
ii) Example: one time pad	ii) Example: DES, AES
iii) If the amount of computing power required to break the encryption is so large that no one can master enough to break it	iii) Unconditionally the scheme does not contain enough information.

Ans: to the Q: No - 06

Steganography: The methods of this process conceal the existance of the message, the methods of cryptography render the message unintelligible to outsiders.

It is not an easy process.

Some example of this technique:

1) character marking
2) Invisible ink
3) pin function
4) Typewritten correction ribbon.

Ans. to the Q: No-5

In caesar cipher is far from secure, ~~A dramatic~~ because momo alaphabetic use permutation and $26!$ Where keys is greater than 4×10^{26} possible keys its not easy to ~~break~~ check all keys in brute force method.

Afterall, there is a limitation in this method, first of all the relative frequency of letters can be determined and compared to a standard frequency distribution ~~of~~ for English.

For example, Azad ϕ in text, and a is appearing twice a in greater freqency. and hacker will easily understand the letter.