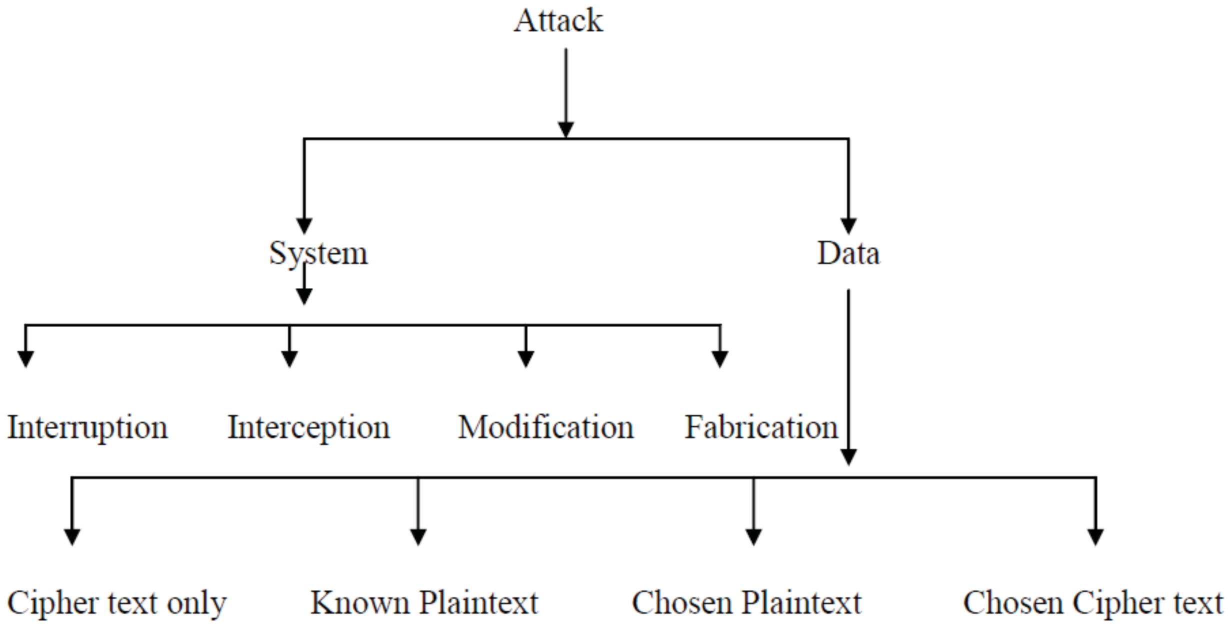
Cryptanalysis

Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. There are two general approaches to attacking a conventional encryption scheme:

- Cryptanalysis: Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
- Brute-force attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

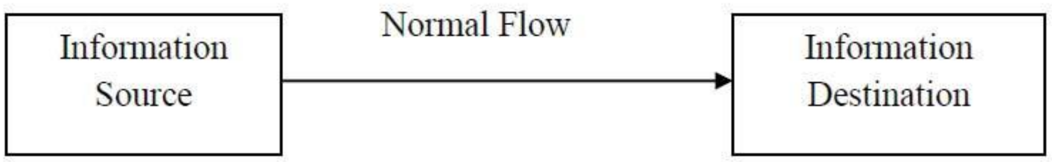
There are basically two types of attack. One is on system and other is on data shown in Figure below.



Classification of Attacks on Cryptography

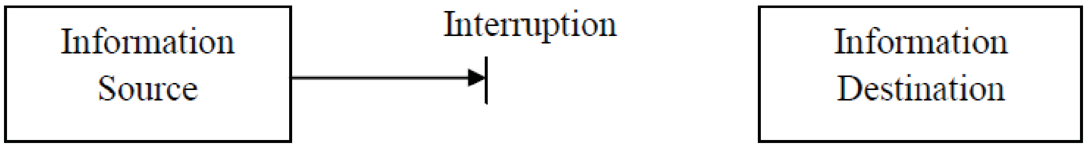
System Attacks:

In general, there is a flow of information from a source to a destination. The attacks which are on the flow of information are known as system attacks. The main security threats are listed below:



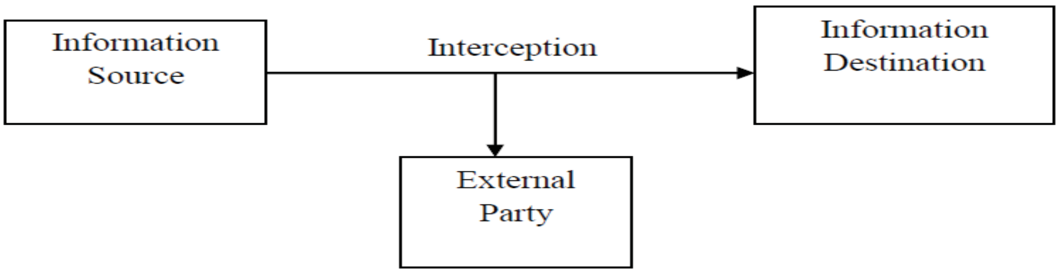
Normal Flow of Information

Interruption: It is an attack on availability of the resource. When the data flowing through source to destination becomes unavailable or unusable:



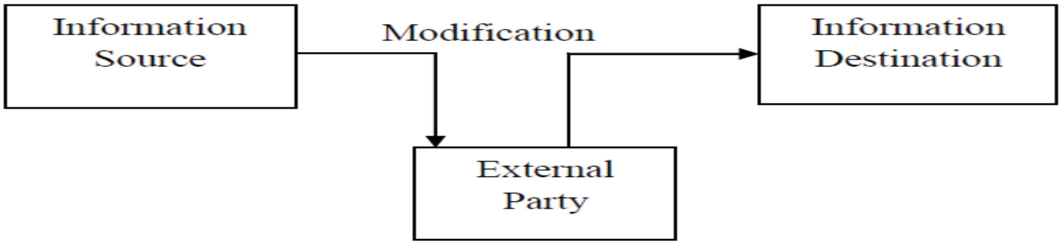
Interrupted Data Flow

Interception: It is an attack on the confidentiality of the system. In this attack an unauthorized party also has the access to a model. A person, program and a computer may be the unauthorized party:



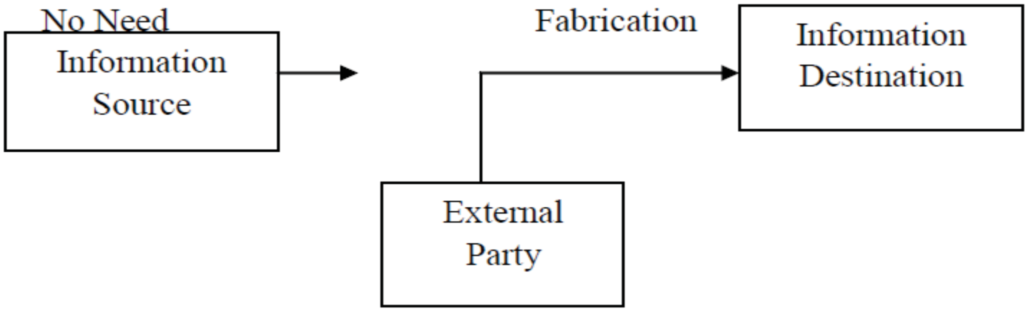
Interception Attack

Modification: It is an attack on integrity of the system. In this attack an unauthorized party not only has the access to an asset but has the power to modify it:



Modification of Data

Fabrication: It is an attack on authenticity of the system. In it an unauthorized party inserts counterfeit objects into the system:



Fabrication System Attack