Tipi di attacco ad un cifrario

Si dividono in:

passivi il crittoanalista si limita ad osservare la conversazione;

attivi (man-in-the-middle) agisce sul canale disturbando la comunicazione e/o modificando il contenuto dei messaggi.

Sulla base delle informazioni a disposizione:

cipher text attack (solo testo cifrato) il crittoanalista conosce solo i crittogrammi;

known plain-text attack (testo in chiaro noto) conosce una serie di coppie (messaggio, crittogramma);

chosen plain-text attack (testo in chiaro scelto) coppie relative a messaggi scelti dall'attaccante;

chosen cipher-text attack (testo cifrato scelto) coppie relative a crittogrammi scelti;

bruteforce

Un cifrario è sicuro se non ci sono attacchi più efficienti del forza bruta.