Crittoanalisi statistica

Forzare il cifrario non dal punto di vista algoritmico ma statistico (analisi delle frequenze). I cifrari storici sono stati violati con attacchi statistici di tipo cipher text.
Primo esempio violazione del cifrario di Vigenère nel XIX secolo.
Informazioni note:

- metodo di cifratura;
- linguaggio naturale del messaggio, e relative frequenze di lettere e q-grammi;
- crittogrammi sufficientemente lunghi;

Sostituzione monoalfabetica

se y nel crittogramma corrisponde a x nel messaggio, frequenza(x)=frequenza(y) si costruisce l'istogramma delle frequenze del crittogramma e si associano in cifrari tipo cesare scoprire una corrispondenza determina tutte le altre nel cifrario completo non basta, bisogna scoprire tutte le asocciazioni cifrari affini ne servono 2 per trovare a e b

Sostituzione polialfabetica

istogramma delle frequenze non funziona
Vigenère se la chiave è lunga h, tutte le lettere distanti un multiplo di h sono cifrate con la stessa traslazione decompongo il messaggio e provo a decifrare come con Cesare
scoprire h: cerchiamo sottosequenze identiche ripetute più volte, che probabilmente corrispondono ai q-grammi più frequenti della lingua si cercano coppie di posizioni (p_1, p_2) in cui iniziano sottosequenze identiche $p_2 - p_1$ è probabilmente uguale o multiplo di h
Alberti immune se la chiave è cambiata spesso.

Trasposizione

permutazione semplice si cercano all'interno del crittogramma le lettere corrispondenti ai q-grammi più frequenti: nel crittogramma non saranno adiacenti ma nel testo in chiaro sì (scopriamo un pezzo di permutazione).

Individuare il metodo di cifratura

Calcolando l'istogramma delle frequenze:

- se coincide con quello della lingua del messaggio, trasposizione;
- se è una suo permutazione, sostituzione monoalfabetica;
- se è più appiattito, sostituzione polialfabetica.