Cifrari a trasposizione

Permutazione semplice

- $k = (h, \pi)$, dove h è un intero e π una permutazione dei primi h interi;
- si suddivide il messaggio in blocchi di h lettere, cifrate permutando con π;
- se la lunghezza del messaggio non è divisibile per h si aggiunge padding al testo in chiaro.

Le chiavi possibili non banali sono $h! - 1$, quindi gli attacchi di forza bruta non sono possibili.

Permutazione di colonne

- $k = (c, r, \pi)$, π permutazione dei primi c interi;
- il messaggio viene caricato in blocchi di cr caratteri su una tabella $c \times r$
- le colonne sono permutate con π
- il crittogramma si legge per colonne

Numero di chiavi esponenziale nella lunghezza del messaggio.

Cifrari a griglia

Cifrario di Richelieu: crittogarmma celato in un libro qualsiasi, la chiave è una scheda perforata più l'indicazione della pagina del libro.

Altro cifrario a griglia:

- il crittogramma è scritto in una tabella quadrata $q \times q$, con q pari;
- si costruisce una griglia con $s = q^2/4$ celle trasparenti (1/4 del totale);
- si scrivono i primi s caratteri del messaggio nelle celle trasparenti;
- si ruota la griglia 3 volte di 90° in senso orario ripetendo ogni volta la scrittura a gruppi di s caratteri.

La decifrazione è analoga, leggendo invece di scrivere.

La griglia deve essere scelta in modo che ruotandola i sulla della griglia corrispondano a celle distinte della tabella, quindi ci sono 4^s chiavi possibili.