Scheda10: DISCO CIFRANTE DI LEON BATTISTA ALBERTI

Per secoli, la semplice cifratura per sostituzione mono alfabetica aveva garantito la segretezza; ma lo sviluppo dell'analisi delle frequenze cancellò quella garanzia.

A metà del 1400 un grande matematico, latinista, letterato, musicista e architetto: Leon Battista Alberti attuò una vera analisi statistica della lingua e con un approccio totalmente scientifico analizzò l'uso delle vocali e delle consonanti e la frequenza delle lettere delle parole.

Grazie a quest'analisi comprese le inefficienze dei sistemi cifranti e allo scopo di renderli meno vulnerabili definì un codice polialfabetico.

Alberti propose di usare due o più alfabeti cifranti e di sostituirli, durante la cifratura, per confondere l'eventuale decrittatore.

Il codice presupponeva la costruzione di uno strumento (il Disco Cifrante di Leon Battista Alberti).

Attività:

Costruire il disco cifrante di Leon Battista Alberti.

Materiale necessario: due cartoncini di colore diverso, un fermacampione, compasso, goniometro, squadre

Costruzione: Il disco è formato da due cerchi concentrici (l'originale era in bronzo), quello esterno stabile con 24 caselle contenente in maiuscolo in rosso, ordinate, le 20 lettere dell'alfabeto latino , con la Z ed escluse le H,K, J, U (in latino equivalente a V) W, Y seguite dai numeri 1234.

Disco esterno: **ABCDEFGILMNOPQRSTVXZ1234**.

I numeri vengono messi nel messaggio in chiaro e sono considerate nulle.

Il disco interno è invece mobile (quindi useremo un fermacampione per consentire al disco interno di ruotare), con in nero le 24 lettere minuscole con le 20 lettere latine classiche più h,k,y,& (quest'ultimo simbolo rappresenta la congiunzione et) in ordine casuale.

Quest'ultima regola, trascurata da molti successori dell'Alberti è fondamentale altrimenti si ha una semplice successione di Cifrari di Cesare.

Almeno due dischi devono essere identici (ovvero con la stessa distribuzione casuale di lettere e cifre, altrimenti non possiamo verificare la coppia mittente e destinatario).