UNA MACCHINA CIFRANTE: IL DISCO DI LEON BATTISTA ALBERTI

Leon Battista Alberti, vissuto a metà del '400, fu una delle figure artistiche più poliedriche del Rinascimento. Scrittore, architetto e matematico, fu anche un celebrato crittografo per gli standard della sua epoca, ed inventò un metodo per generare messaggi criptati con l'aiuto di un apparecchio, il disco cifrante. Il disco cifrante è il primo sistema di cifratura polialfabetica, ancor prima del "troppo" famoso cifrario di Vigenère rispetto cui è estremamente più potente.

Egli 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 attraverso la quale comprese le inefficienze dei sistemi cifranti e allo scopo di renderli meno vulnerabili.
Il codice presupponeva la costruzione di uno strumento, la cui costruzione con cartoncino e fermacampioni è l'attività di questa lezione.

Attività:
1. costruire il disco cifrante di Leon Battista Alberti.
2. Utilizzare il disco per criptare un messaggio.

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:

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), per comodità ne potremmo costruire uno che sia identico per tutti in classe e poi lasciare il compito di costruirne un numero pari diverso a casa.

Osservazioni:
1. Il Disco Cifrante è un **cripto-sistema** polialfabetico. Tale sistema introduce un concetto fondamentale in crittografia, ovvero quello della **permutazione**: se S è un insieme di **n** oggetti, una permutazione di S non è altro che "riordinamento". Ad esempio 3,4,5,1,2 è una permutazione di 1,2,3,4,

Utilizzo del Disco cifrante:
Mittente e destinatario concordano una lettera minuscola, ad esempio k come chiave segreta. Leon Battista Alberti propone 3 metodi di cifratura, ma noi ne applichiamo solo 2.

I. Mittente e destinatario concordano una lettera **minuscola**, ad esempio k come chiave segreta. Il mittente ruota il disco mobile fino a portare **k sotto**

una maiuscola per **esempio B** che viene scritta come lettera del cifrato, dopodiché si cifrano alcune lettere con la lista risultante, quindi si ruota il disco interno di alcune posizioni ottenendo una nuova lista. Il cambio di lista viene segnalato scrivendo la **MAIUSCOLA** sotto la quale ora si trova k; e così via ad ogni cambiamento di lista.

Esempio sovrapponiamo i due dischi in modo da
A-B-C-D-E-F-G-I- L-M-N-O-P-Q-R-S-T-V-X- Z- 1- 2- 3-4
o- k-b- p- f- z-s- e-m-d-g- u- t- a- i- r- l- h- n- x- y- q- c- &
Vogliamo cifrare il messaggio **INVIARE RINFORZI DOMANI** (messaggio in chiaro)
Scriviamo senza spazi e inserendo in modo casuale delle cifre
INV1IA2RERI4NFORZID3OMANI (messaggio preparato per la codifica)
Il messaggio cifrato diventa
BeghyeoLeiqeolpcafPpmylZfhrsla (messaggio cifrato)
La decifratura procede a rovescio: il destinatario legge a inizio messaggio cifrato B, porta k sotto B e decifra con questa lista fino alla successiva maiuscola, nel nostro esempio L, allora porta k sotto L e decifra i caratteri seguenti fino alla successiva maiuscola, nel nostro caso P allora porta k sotto P e decifra e via di seguito.

II. Dato che le lettere maiuscole introdotte costituiscono un aiuto all'intercettazione L.B.Alberti propose di usare come chiave una maiuscola, per esempio B e di scrivere a inizio messaggio la minuscola corrispondente, nel nostro caso k, e di usare le 4 cifre non più come nulle ma per segnalare il cambio di alfabeto; la lettera minuscola corrispondente al numero sarà la nuova chiave e la si porterà sotto B,

esempio il messaggio **INVIARE RINFORZI DOMANI** (messaggio in chiaro)
INVIA1RERINFO4RZID2OMANI (messaggio preparato per la codifica)
Kegheoydjdbzosnetoyiocajy (messaggio cifrato)
Il cifrato coincide con il precedente solo all'inizio: non ci sono più lettere maiuscole, la decifratura procede come sopra: il destinatario porta la prima lettera k a coincidere con B e decifra con questa lista fino a quando non ottiene il numero 1, nel nostro caso in corrispondenza della y; allora ruota il disco fino a far coincidere la y con la B e così fino a trovare un'altra cifra.