COMITATO ORGANIZZATORE OBJ
CO.R.P.
COMITATO REGIONALE PIEMONTE

Code Obj: **CHARLIE**
Nome Obj: **LA FABBRICA DI CARTA**
Tipologia: **A + E**
Durata Obj: **25 minuti**
Area temporale: **Dalle 09:00 del 8/10/2022 alle 09:00 del 9/10/2022**
Coordinate: **Vedi Allegato Coordinate**

ALLEGATO 1_CIFRARIO DI CESARE_CHARLIE

IL CIFRARIO DI CESARE

In crittografia, il cifrario di Cesare è uno dei più antichi algoritmi crittografici di cui si abbia traccia storica.

È un cifrario a sostituzione monoalfabetica, in cui ogni lettera del testo in chiaro è sostituita, nel testo cifrato, dalla lettera che si trova un certo numero di posizioni dopo nell'alfabeto.

Questi tipi di cifrari sono detti anche cifrari a sostituzione o cifrari a scorrimento a causa del loro modo di operare: la sostituzione avviene lettera per lettera, scorrendo il testo dall'inizio alla fine.

LA STORIA DEL CIFRARIO DI CESARE

Il cifrario di Cesare prende il nome da Giulio Cesare, che lo utilizzava con l'intento di proteggere i suoi messaggi criptati.
Sono molto scarse le notizie sulla crittografia romana: le uniche nozioni riguardano il fatto che Giulio Cesare ed Augusto usavano questo particolare sistema di cifratura nelle loro corrispondenze con i famigliari.
A fornircene informazioni è solo Svetonio, nella Vita dei dodici Cesari, un'opera del II secolo d.C.

Grazie a questo importante storico, sappiamo che Cesare utilizzava in genere una chiave di 3 per il cifrario, come nel caso della corrispondenza militare inviata alle truppe comandate da Quinto Tullio Cicerone.
Svetonio racconta che Giulio Cesare usava per le sue corrispondenze riservate una cifra monoalfabetica molto semplice, nella quale la lettera chiara viene sostituita dalla lettera che la segue di tre posti nell'alfabeto: la lettera A è sostituita dalla D, la B dalla E e così via fino alle ultime lettere che sono cifrate con le prime come nella tabella che segue (che fa riferimento all'odierno alfabeto internazionale).
Al tempo era sicuro perché gli avversari spesso non erano neanche in grado di leggere un testo in chiaro, men che mai uno cifrato; inoltre non esistevano metodi di crittoanalisi in grado di rompere tale codice, per quanto banale.

Conosciamo anche altri che usarono questo cifrario al tempo di Cesare: Augusto, suo nipote, lo utilizzava con chiave 1, ma senza ripartire da sinistra in caso di fine dell'alfabeto. Quindi, scriveva B per A, C per B ma usava AA per Z.

GLI SVILUPPI DELL'USO

Dalla scoperta dell'analisi delle frequenze da parte del matematico arabo Al-Kindi nell'XI secolo circa, tutti i cifrari di questo tipo sono divenuti molto semplici da rompere.

Infatti, nessuno di questi è adatto per comunicazioni sicure allo stato tecnologico attuale, né lo è stato negli ultimi 1000 anni.

Tuttavia, una forma di questo cifrario, chiamata ROT13, è ancora usata oggi per offuscare parti di un messaggio in modo da non renderle immediatamente comprensibili.

Nel tempo, questa tecnica di cifratura è stata utilizzata da numerose personalità, tra cui Mary Stuart, regina di Scozia del VI secolo e Bernardo Provenzano, celebre boss mafioso.

DESCRIZIONE DEL CIFRARIO

Cesare utilizzava uno spostamento di 3 posizioni
(la chiave, cioè ciò che indica di quanto spostarsi era dunque 3),mma si può arrivare anche con una chiave a 5 posizioni, secondo il seguente schema nell'alfabeto latino classico, che aveva 23 caratteri:

Testo in chiaro: a b c d e f g h i k l m n o p q r s t v x y z
Testo cifrato: D E F G H I K L M N O P Q R S T V X Y Z A B C

Lo stesso si può fare con l'alfabeto latino esteso, che ha 26 caratteri:

Testo in chiaro: a b c d e f g h i j k l m n o p q r s t u v w x y z
Testo cifrato: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Per cifrare un messaggio, basta prendere ogni lettera del testo in chiaro e sostituirla con la corrispondente lettera della riga testo cifrato.
Per decifrare, viceversa.
Basta sapere quale alfabeto viene utilizzato e il numero di chiave.