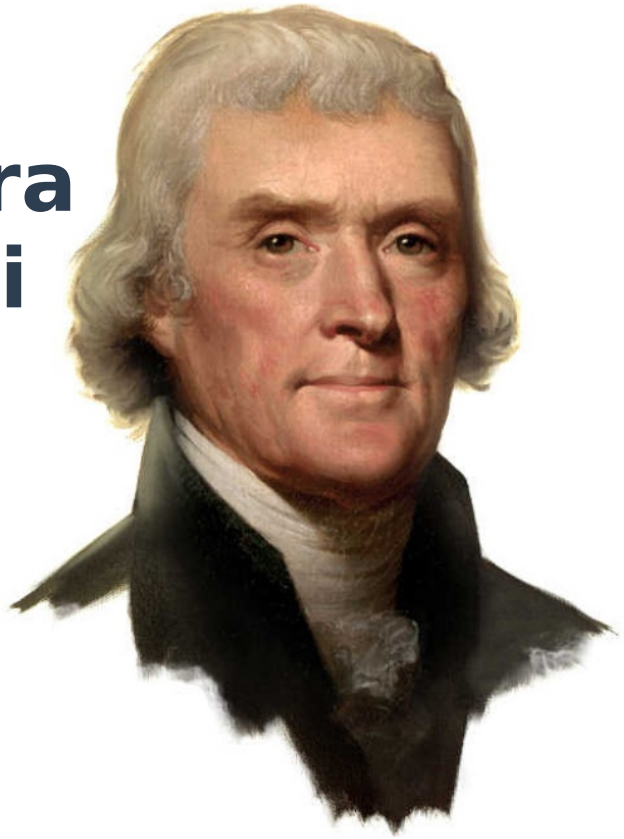
Cifrario Jefferson

Nicola Sampaolesi

5A – IIS G. Marconi E. Pieralisi – A. S. 2018-2019

Storia

Nei quattro anni passati in Francia per offrire servizi diplomatici tra il 1785 e il 1789, Thomas Jefferson si era reso conto della necessità di cifrare le comunicazioni diplomatiche, avendo rilevato che i Francesi intercettavano e leggevano tutta la corrispondenza.



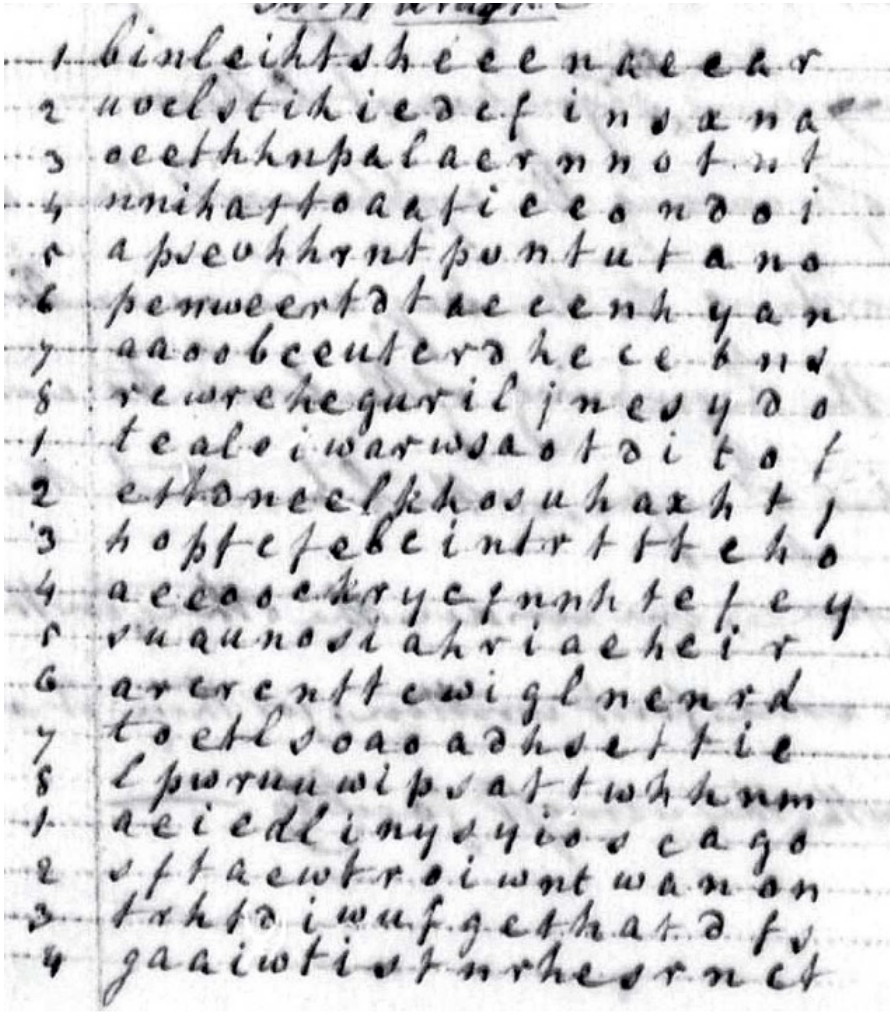
Storia

Nel 1790 divenne segretario di stato del primo presidente USA George Washington e propose quindi uno strumento con il nome di “Wheel Cipher” per la cifratura delle comunicazioni diplomatiche

- **riservate.**

Storia

Tuttavia dopo essere stato eletto Presidente, Jefferson abbandonò abbandonò il proprio cifrario nel 1802 a favore di uno propostogli dal matematico Robert Patterson.



Storia

Nel 1917 il maggiore americano Joseph O. Mauborgne riscoprì il Wheel Cipher che ribattezzandolo “M-94” lo portò in uso nell’esercito USA fino al 1943 quando fu dichiarato obsoleto.

Struttura

Il cifrario di Jefferson è un cilindro composto da più ruote identificate da un numero.

Su ogni ruota è stampato l’intero alfabeto in ordine casuale.

Le ruote possono essere estratte dal cilindro e re-inserite in qualsiasi ordine.

Il cilindro M-94 è composto da 25 ruote, l’originale di Jefferson invece da 36 ruote.

Tecnica - Cifratura

1) Vengono rimosse tutte le ruote dal cilindro e vengono re-inserite in ordine casuale appuntandosi il nuovo ordine.
2) Le ruote vengono allineate in modo da comporre il messaggio da cifrare.
3) Si sceglie un numero casuale ‘N’ tra ‘1’ e ‘25’ (Numero delle lettere dell’alfabeto meno uno).
4) Si trascrive il testo ‘N’ posizioni sotto il messaggio composto.

Il testo appena trascritto è il messaggio cifrato, l’ordine delle ruote appuntato in precedenza e il numero ‘N’ compongono la chiave per la de-cifratura.

Tecnica - De-cifratura

1) Si estraggono tutte le ruote dal cilindro e le si re-inseriscono seguendo l’ordine specificato dalla chiave.
2) Si allineano le ruote in modo da comporre il messaggio cifrato.
3) Si trascrive il testo ‘N’ posizioni sopra il messaggio appena composto.

Il testo trascritto è il testo decifrato.

Fonti:

Crittologia.eu
Corriere della Sera
Università degli Studi di Roma Tre