Criptografia Clàssica

Aprén a xifrar missatges amb els mètodes clàssics que es van fer servir fins la Iª Guerra Mundial.
I descobreix les tècniques de criptoanàlisi per trencar el codi.

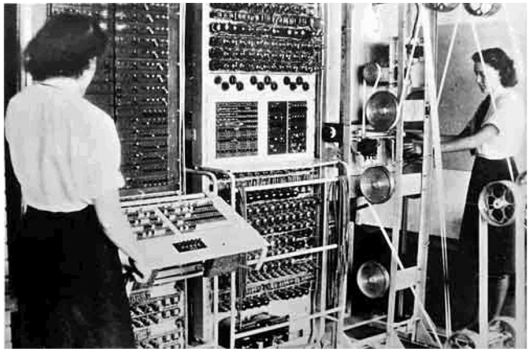
$$\begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} \begin{bmatrix} 13 \\ 14 \end{bmatrix} = \begin{bmatrix} 16 \\ 21 \end{bmatrix}$$

- L'escitala
- El xifrat Cèsar
- Substitució afí
- Xifrat monoalfabètic

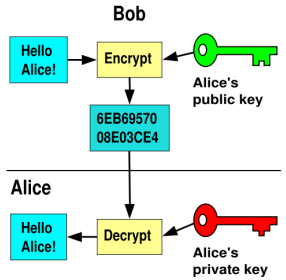
...

Segona Guerra Mundial : les matemàtiques entren en joc

La necessitat de llegir els missatges secrets dels enemics en temps de guerra va impulsar decididament l'evolució del criptoanàlisi i la creació de les primeres màquines de còmput.



Criptografia Moderna: la xarxa està codificada



Al 1978 els matemàtics Rivest, Shamir i Adleman van desenvolupar un nou mètode de xifrat que permetia fer anar claus diferents per codificar i descodificar missatges.

Aquest mètode va resultar crucial pel desenvolupament de les signatures electròniques i el comerç a la Xarxa.