PLAYFAIR CIPHER

CARLETTI MATTIA 5 A INFORMATICA

IIS MARCONI PIERALISI JESI

Crittografia classica

- La crittografia classica si sviluppa in parallelo alla evoluzione della stenografia e il primo esempio lo si fa risalire a 4500 anni fa ai geroglifici egizi.
- La crittografia non mira a nascondere il messaggio in sé, ma il suo significato.
- Per rendere incomprensibile un testo, lo si altera per mezzo di un procedimento concordato dal mittente e dal destinatario.
- Il vantaggio della crittografia è che anche se il nemico intercetta il messaggio, esso risulta incomprensibile e quindi inutilizzabile.

Che cosa è

- Il Playfair cipher fu inventato dal noto fisico Sir Charles Wheatstone(1802-1875) ma divulgato dal barone Lyon Playfair.
- La speranza di Playfair era quella di far utilizzare il *Cipher* durante la guerra di Crimea, fu in realtà usato dall‟esercito britannico solo nella guerra di Boeria.
- Il Playfair Cipher è una forma di cifrario poligrafico nella quale il testo è scomposto da bigrammi.
  - POLIGRAFICO, sono cifrari nei quali la cifratura avviene per gruppi di segni (lettere); il testo chiaro viene raggruppato in gruppi di M elementi, ogni gruppo viene cifrato con un gruppo di N elementi dell'alfabeto cifrante.
  - BIGRAMMI, coppia di lettere

Come funziona

- Bisogna creare una griglia 5 * 5 comprendente tutte le lettere dell'alfabeto. Sono 26: e infatti la i e la j vengono accorpate in un'unica casella.
- Per creare questa griglia occorre l'utilizzo della chiave, ossia una parola prestabilita che verrà inserita all'inizio della griglia scrivendo una sola volta le doppie lettere. La tabella verrà poi completata con le lettere dell'alfabeto restanti in ordine.
- ESEMPIO

CHIAVE = locomotiva

L	O	C	M	T
I	V	A	B	D
E	F	G	H	K
N	P	Q	R	S
U	W	X	Y	Z

Come funziona

- Il testo va scomposto in bigrammi e individuo le due lettere sulla griglia.
- Siccome vengono cifrati i bigrammi, ossia le coppie di lettera, se uno di questi bigrammi è composto da due lettere uguali occorre spezzarlo aggiungendo un'altra lettere «rara», di solito la X.
  - ESEMPIO CC → CXC
- Inoltre, sempre per i bigrammi, occorre che il numero delle lettere del testo sia pari, perciò so non lo è, si aggiunge una lettera alla fine, ad esempio la X, o qualche latra lettera «rara».

  - ESEMPIO

    «attaccare immediatamente» → at ta cc ar ei mm ed ia ta me nt e →

    at ta cx ca re im me di at am en te

Come funziona

Le coppie di lettere individueranno un rettangolo nella griglia considerandole come i due angoli opposti di esso:

1. Se le due lettere stanno sulla stessa riga vengono sostituite dalle lettere che stanno immediatamente a destra rispetto ad ognuna di essa. Se si esce dal lato destro della tabella si rientra dal sinistro sulla stessa riga.
2. Se le due lettere stanno sulla stessa colonna verranno sostituite dalle lettere che stanno immediatamente sotto, e anche qui se si esce da sotto si rientra da sopra nella stessa colonna.
3. In tutti gli altri casi ogni lettera va sostituita con quella appartenente alla propria riga ma sulla colonna dell'altra lettera del bigramma.

Come funziona

CHIAVE = locomotiva

TESTO = at ta cx **CA** **RE** im me **DI** at am en te

L	O	C	M	T
I	V	A	B	D
E	F	G	H	K
N	P	Q	R	S
U	W	X	Y	Z

DI → IV

CA → AG

RE → NH

TESTO CIFRATO

dc cd ac ag nh bl lh iv dc bc nu lk

Decifratura

La **decifratura** avviene al contrario:

- le lettere sulla stessa riga vengono sostituite dalle lettere che stanno a sinistra
- le lettere sulla stessa colonna vengono sostituite dalle lettere che stanno sopra
- le lettere che formano un quadrato vengono sostituite dalle lettere all'altro estremo del lato orizzontale del quadrato su cui si trova la lettera.

Fonti

- http://www.crittologia.eu/critto/playfair.phtml
- http://www.swappa.it/wiki/Uni/CifrarioPlayfair
- https://avires.dimi.uniud.it/claudio/teach/sicurezza2013/lezione-02.pdf