Algoritmi di crittografia

a cura di PIETRO ZANIN e LEONARDO REBESCHINI
Realizzato nell'ambito del ***progetto Archimede***
con
la supervisione dei Proff. Fabio Breda, Gabriele Rizzo, Elia Secco,
Valentina Fabbro, Francesco Zampieri
I.S.I.S.S. M.Casagrande,
Pieve di Soligo, a.s. 2014/15

Il metodo Playfair

Nel 1854 lo scienziato inglese Wheatstone inventò la tecnica crittografica che diverrà poi nota come il cifrario di Playfair, dal nome del barone che lo promosse nella società politica del tempo. Il cifrario è basato non più sulla sostituzione di ogni singola lettera ma vengono presi in considerazione dei digrammi, ossia coppie di lettere, che verranno sostituiti dai corrispondenti digrammi cifrati.

Esso consiste nel riempire una tabella 5x5 con l'alfabeto (togliendo a seconda delle varie versioni la lettera Q o la lettera W o ancora considerando la I e la J come un'unica lettera). Le prime lettere appartengono ad una parola chiave, privata di eventuali lettere ripetute, alla quale succedono tutte le lettere non presenti in essa in ordine alfabetico. Se ad esempio la parola chiave è MASSIMO la matrice di Playfair sarà la seguente:

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

Si procede poi scomponendo la parola/frase da cifrare in digrammi, inserendo la lettera X in due casi: tra due lettere doppie e alla fine nel caso il numero di lettere totale (comprese le X inserite) sia dispari; dovremo ovviamente eliminare eventuali spazi. In questo modo otterremo una serie di digrammi.

La fase successiva richiede l'utilizzo della matrice secondo alcune semplici regole:

Se i caratteri del digramma si trovano sulla stessa riga , si prendono i due caratteri rispettivamente a destra di ognuno dei due che compongono il digramma, a meno del caso in cui uno dei due si trovi all'estrema destra: in quel caso si prenderà il primo carattere della riga;

Se i caratteri del digramma si trovano sulla stessa colonna , si prendono i due caratteri rispettivamente a sotto ad ognuno dei due che compongono il digramma, a meno del caso in cui uno dei due si trovi all'estremità inferiore: in quel caso si prenderà il primo carattere della colonna;

Se i caratteri non si trovano né sulla stessa riga né sulla stessa colonna si disegna un rettangolo che abbia i due caratteri come angoli e si prendono i due caratteri che corrispondono agli altri due angoli.

Questo metodo fu utilizzato dall'Inghilterra fino alla prima guerra mondiale e dall'Austria e dalla Germania fino alla seconda per informazioni con effetto immediato la cui decifratura sarebbe stata ultimata solamente dopo l'attuazione del messaggio.

Con i moderni sistemi digitali il cifrario è divenuto inutile in un contesto militare in quanto viene decifrato in pochi secondi.

Noi abbiamo ricostruito il procedimento di cifratura attraverso un'interfaccia web sviluppata in linguaggio HTML che richiama una pagina PHP che attua la vera e propria cifratura.

Il metodo Delastalle

Il metodo è dovuto a Félix-Marie Delastelle uno tra i massimi crittologi francesi del XIX secolo.

Il suo è un cifrario bifido poligrafico basato sulla matrice 5x5 usata per la prima volta nella scacchiera di Polibio e utilizzata anche dallo stesso Playfair.

Allo stesso modo del precedente metodo si compone la tabella di 25 caratteri inserendo inizialmente la parola chiave privata di lettere ripetute e poi le lettere dell'alfabeto restanti.

Un esempio di matrice è quella mostrata per il cifrario Playfair. Una volta completato questo si passa alla cifratura del messaggio che si esegue seguendo quattro regole.

Il messaggio chiaro viene spezzato in blocchi di cinque caratteri ciascuno; se l'ultimo blocco non è esattamente di cinque, gli ultimi posti sono riempiti di X.

Come esempio si prenda la matrice ottenuta con la parola chiave COMPUTER, e si voglia cifrare il messaggio RINFORZI

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

Ogni lettera del blocco viene cifrata con due cifre e cioè con l'indice di riga e l'indice di colonna, che vengono scritte in verticale sotto la lettera
chiara.

RINFO RZIXX
35322 35533
23431 25355

Le cifre vengono ora riscritte in orizzontale riga dopo riga ottenendo un messaggio con un numero di cifre doppio dell'originale.

35 32 22 34 31 35 53 32 53 55

A questo punto ogni coppia di numeri viene ritrasformata in lettera sempre secondo la matrice. Ne risulta il messaggio cifrato da trasmettere. Si ottiene:

X R E N M X I R I Z