archimede.png

casagrande.jpg

LA CRITTOGRAFIA

Cifrario Di Hill

a cura di GALATANU RAZVAN e PIZZARDO ANDREA

Realizzato nell'ambito del ***progetto Archimede***
con la supervisione del Prof. Rizzo Gabriele
I.S.I.S.S. "M.Casagrande", Pieve di Soligo, a.s. 2014/15

Abstract

Per crittografia si intende quella tecnica di rappresentazione di un messaggio in una forma tale che l'informazione in esso contenuta possa essere recepita solo dal destinatario; ciò si può ottenere con due diversi metodi: celando l'esistenza stessa del messaggio o sottoponendo il testo del messaggio a trasformazioni che lo rendano incomprensibile.

Nel particolare, ***il cifrario di Hill*** è un crittosistema polialfabetico che fu inventato nel 1929 da Lester Hill. Sia m un intero positivo, definiamo $P = C = (Z_{26})^m$. L'idea è di costruire m combinazioni lineari contenenti ognuna m caratteri alfabetici del testo in chiaro e produrre, con ciascuna combinazione lineare, un singolo elemento del testo cifrato. La chiave utilizzata in questo cifrario è una matrice K invertibile di dimensione m x m .

Procediamo ora con un esempio illustrativo del funzionamento del suddetto cifrario: prendiamo in esame la parola da crittografare "*archimedeproject*". Abbiamo dunque bisogno di una matrice e di un valore da attribuire a m, che sarà 2. La nostra matrice 2 x 2, creata in modo che sia invertibile, condizione necessaria per la decodifica, sarà la seguente:

$$\begin{bmatrix} \text{a} & \text{b} \\ \text{c} & \text{d} \end{bmatrix} \rightarrow \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$$

CODIFICA

Il concetto che sta dietro alla codifica è, di per sè, abbastanza semplice: la parola da codificare va suddivisa in gruppi di m lettere, nel nostro caso 2. *archimedeproject* sarà dunque suddiviso in *ar ch im ed ep ro je ct*. Si tratterà ora di trasformare ogni coppia di lettere in un vettore colonnare, dove ogni lettera corrisponderà a un numero in base alla relativa posizione nell'alfabeto, seguendo lo schema *A = 1; B = 2; C = 3 ... Z = 26* ottenendo i vettori:

$$\begin{bmatrix} \text{x} \\ \text{y} \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 18 \end{bmatrix} \begin{bmatrix} 3 \\ 8 \end{bmatrix} \begin{bmatrix} 9 \\ 13 \end{bmatrix} \begin{bmatrix} 5 \\ 4 \end{bmatrix} \begin{bmatrix} 5 \\ 16 \end{bmatrix} \begin{bmatrix} 18 \\ 15 \end{bmatrix} \begin{bmatrix} 10 \\ 5 \end{bmatrix} \begin{bmatrix} 3 \\ 20 \end{bmatrix}$$

Ogni vettore andrà dunque moltiplicato per la matrice di codifica, nel seguente modo:

$$\begin{bmatrix} \text{a} & \text{b} \\ \text{c} & \text{d} \end{bmatrix} \cdot \begin{bmatrix} \text{x} \\ \text{y} \end{bmatrix} = \begin{bmatrix} \text{ax+by} \\ \text{cx+dy} \end{bmatrix} mod 26 = \begin{bmatrix} \text{d(x)} \\ \text{d(y)} \end{bmatrix}$$

Dove $d(x)$ e $d(y)$ rappresentano i valori x e y codificati. La dicitura $mod 26$ sta ad indicare che i valori vanno riportati in modulo 26 per essere riscritti sotto forma di lettere dell'alfabeto (Ricordiamo che per numero in modulo 26 intendiamo il resto della divisione tra il numero stesso e 26). Avremo quindi:

$$\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 18 \end{bmatrix} = \begin{bmatrix} (9)(1)+(4)(18) \\ (5)(1)+(7)(18) \end{bmatrix} mod 26 = \begin{bmatrix} 17 \\ 16 \end{bmatrix}$$

E via di seguito otterremo anche:

$$\begin{bmatrix}21\\8\end{bmatrix}\begin{bmatrix}17\\21\end{bmatrix}\begin{bmatrix}23\\16\end{bmatrix}\begin{bmatrix}19\\22\end{bmatrix}\begin{bmatrix}2\\2\end{bmatrix}\begin{bmatrix}20\\22\end{bmatrix}\begin{bmatrix}17\\14\end{bmatrix}$$

Le coppie di numeri così ottenute andranno dunque trasformate nuovamente in lettere. [17 16] diventerà *qp*, [21 8] diventerà *uh*, e via così, fino a ottenere *qpuhquwpsvbbtvqn*, che è la nostra parola codificata.

Nel caso in cui la parola da codificare abbia un numero dispari di lettere, l'unica soluzione sta nell'aggiungere una lettera stabilita a priori alla parola prima della codifica, con l'inconveniente che poi questa comparirà dopo la decodifica, nel messaggio tradotto. Una sola lettera aggiunta al termine di una parola (se non di una frase, nel caso di messaggi più lunghi) non dovrebbe comunque, nella maggior parte dei casi, destare particolari problemi. Nel caso, ad esempio, della codifica della parola *messaggio*, se dopo la decodifica dovessimo ottenere *messaggioz* il messaggio sarebbe ugualmente comprensibile, specie se il lettore è a conoscenza del fatto che in caso di lettere dispari si è assunta come regola l'aggiungere alla fine la lettera *z*.

DECODIFICA

La decodifica nel cifrario di Hill aggiunge la complicazione di dover trovare la matrice inversa della matrice di codifica, che diventerà la nostra matrice di decodifica. Una volta calcolata, il funzionamento di traduzione del messaggio è analogo al precedente. Partiamo dalla nostra matrice di codifica:

$$\begin{bmatrix}a & b\\c & d\end{bmatrix} \rightarrow \begin{bmatrix}9 & 4\\5 & 7\end{bmatrix}$$

E procediamo innanzitutto col calcolarne il determinante *d*, che porremo in modulo 26:

d = ad - bc $\rightarrow$ d $= 9 \cdot 7 - 4 \cdot 5 = 63 - 20 = 43 \rightarrow$ 43 mod26 = 17

Dobbiamo dunque procedere con l'inversione dei valori a e d e con la sostituzione di b e c con $-b$ e $-c$, ottenendo dunque la matrice:

$$\begin{bmatrix}a & b\\c & d\end{bmatrix} \rightarrow \begin{bmatrix}d & -b\\-c & a\end{bmatrix}$$

E dunque:

$$\begin{bmatrix}9 & 4\\5 & 7\end{bmatrix} \rightarrow \begin{bmatrix}7 & -4\\-5 & 9\end{bmatrix}$$

La matrice così ottenutta andrà dunque moltiplicata per quel numero x tale che il suo prodotto con il determinante d, in modulo 26, sia uguale a 1, un problema che nel codice PHP abbiamo risolto in questo modo:

```
$c = false;
$x = 0;
while (!$c)
{
    $x++;
    if ((($det * $x) % 26) == 1)
    {
        $c = true;
    }
}
```

Fatto questo, sarà sufficiente moltiplicare la matrice prima ottenuta per il nostro numero x:

$$x \cdot \begin{bmatrix} \text{d} & \text{-b} \\ \text{-c} & \text{a} \end{bmatrix} \rightarrow 23 \cdot \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} = \begin{bmatrix} 161 & -92 \\ -115 & 207 \end{bmatrix}$$

E poi porla in modulo 26:

$$mod 26 \begin{bmatrix} 161 & -92 \\ -115 & 207 \end{bmatrix} = \begin{bmatrix} 5 & 14 \\ 11 & 25 \end{bmatrix}$$

Abbiamo così ottenuto la nostra matrice inversa e, a questo punto, il procedimento è analogo a quello di codifica: il messaggio andrà suddiviso in coppie di lettere che andranno a costituire i relativi vettori colonnari. Il messaggio codificato di prima, *qpuhquwpsvbbtvqn*, diventerà dunque:

$$\begin{bmatrix} 17 \\ 16 \end{bmatrix} \begin{bmatrix} 21 \\ 8 \end{bmatrix} \begin{bmatrix} 17 \\ 21 \end{bmatrix} \begin{bmatrix} 23 \\ 16 \end{bmatrix} \begin{bmatrix} 19 \\ 22 \end{bmatrix} \begin{bmatrix} 2 \\ 2 \end{bmatrix} \begin{bmatrix} 20 \\ 22 \end{bmatrix} \begin{bmatrix} 17 \\ 14 \end{bmatrix}$$

E, una volta che i vettori saranno moltiplicati per la matrice di decodifica e posti in modulo 26, sempre seguendo lo stesso procedimento della codifica, otterremo:

$$\begin{bmatrix} 1 \\ 18 \end{bmatrix} \begin{bmatrix} 3 \\ 8 \end{bmatrix} \begin{bmatrix} 9 \\ 13 \end{bmatrix} \begin{bmatrix} 5 \\ 4 \end{bmatrix} \begin{bmatrix} 5 \\ 16 \end{bmatrix} \begin{bmatrix} 18 \\ 15 \end{bmatrix} \begin{bmatrix} 10 \\ 5 \end{bmatrix} \begin{bmatrix} 3 \\ 20 \end{bmatrix}$$

I quali, trasformati nuovamente in lettere, altro non rappresentano che il messaggio iniziale, la scritta *archimedeproject*.