UNIVERSITÀ DEGLI STUDI "ROMA TRE"
CORSO DI STUDI IN MATEMATICA
IN450 - INFORMATICA 6
ALGORITMI PER LA CRITTOGRAFIA – A.A. 2016-2017

M. PEDICINI

ESONERO DEL 14/11/2016 – TEMPO 2H00

COGNOME _____ NOME _____ MATRICOLA _____

Esercizio 1. *Dato il seguente testo cifrato (in italiano, alfabeto a 26 lettere) :*

```
001 GVCDPMUUZE KVEMBNVCDZ CUIJPFLRJA MNCDEGNDMR CZTIMYZEZE
051 YUOVQGYTHV QZXJACZXVA MVCIVLHBZA RLTNREBXOR AVCQVCURMR
101 BLGZCCYDXU CUDIPGZXHR RATNFCJDIG SAIVDSLAGN ZBDINTVVGV
151 YJWZFYWTQN GTEDREHGZA CSAJEBPGXN ZHAZRLLANH QJXONPUTHV
201 APPGFSVVMN LUTHVAVTIE GJDDIEPPXP FLEZEOBTNG YWPMGCSPNG
251 MYXVNRATNG YJDHRPPJNP GZHZNBHGHN PLRJARYDLH CSGZVJKJXN
261 BPHVIMPPVP SPUZPCWTMQ CYEDHBBCVP GAIVPMTTMV SZRDFQLPAN
```

(1) Verificare se si tratta di cifrario monoalfabetico;
(2) Effettuare il Kasiski test per determinare la lunghezza della chiave m;
(3) Calcolare l'indice di coincidenza per il secondo sottoblocco estratto dal cifrato;
(4) Ipotizzare una chiave g per il secondo sottoblocco (in base alle frequenze alfabetiche del blocco);
(5) Verificare l'ipotesi utilizzando l'indice di mutua coincidenza M_g.

Esercizio 2. *Effettuare un attacco con plaintext noto, sapendo che è stato utilizzato un cifrario di Hill con chiave lunga 3 in $\mathbb{Z}_{26}$:*

Plaintext:	$(1,2,3)$	$(3,4,1)$	$(17,5,21)$	$(2,11,11)$
Cifrato:	$(23,9,14)$	$(17,9,0)$	$(23,24,14)$	$(12,20,9)$

Esercizio 3. *Sia data la seguente S-box (espansiva) che codifica triple di bit in quadruple di bit:*

$$S : \{0,1\}^3 \to \{0,1\}^4$$

rappresentata dalla sequenza esadecimale `58F4C162`.

(1) Verificare che S sia invertibile e calcolarne l'inversa.

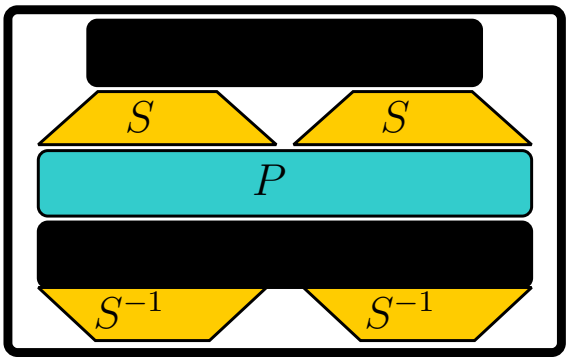
(2) Completare la seguente tabella di approssimazione lineare di S:

$$N_L(S) = \begin{bmatrix} 8 & 5 & 5 & 4 & 3 & 4 & 4 & 3 & 5 & 4 & 4 & 1 & 4 & 3 & 3 & 4 \\ 4 & 3 & 3 & \square & \square & \square & 4 & 5 & 3 & 4 & 4 & 3 & 4 & 5 & \square & \square \\ 4 & 3 & 7 & 4 & 5 & 4 & 4 & 5 & \square & \square & \square & 3 & 4 & 5 & 5 & 4 \\ 4 & 5 & 5 & 4 & 3 & \square & \square & \square & 5 & 4 & 4 & 5 & 4 & 7 & 3 & 4 \\ 4 & 3 & 5 & 6 & 3 & 6 & 4 & 5 & 3 & 4 & 6 & 5 & 2 & 3 & \square & \square \\ 4 & \square & \square & \square & 5 & 6 & 4 & 3 & 5 & 4 & 6 & 3 & 6 & 5 & 3 & 4 \\ 4 & 5 & 3 & 2 & 5 & 6 & 4 & 7 & 5 & 4 & 2 & 3 & 2 & 5 & 3 & 4 \\ 4 & 3 & 5 & 2 & 3 & 2 & 4 & 5 & 7 & 4 & 6 & 5 & 2 & 3 & 5 & 4 \end{bmatrix}$$

(3) Sia la S-box utilizzata nella seguente SPN, dove P rappresenta la permutazione

$$P = (15674328)$$

e il rettangolo in nero la combinazione con la chiave.



Calcolarne un cammino con massimo sbilanciamento (che relazione c'è tra la tabella $N_L(S)$ e quella per l'inversa $N_L(S^{-1})$?).

Frequenze di riferimento per l'italiano utilizzato nell'esercizio 1:

0	0.11387					
1	0.00976787					
2	0.046949					
3	0.0372904					
4	0.120561					
5	0.0105369					
6	0.0171614					
7	0.0134988					
8	0.0955512					
9	0.0000224459					
11	0.0557664					
12	0.0236882					
13	0.0729882					
14	0.0965691					
15	0.0297174					
16	0.00781215					
17	0.0661081					
18	0.0547055					
19	0.0610431					
20	0.0357065					
21	0.0230168					
22	0					
23	0.0000731932					
24	0					
25	0.00758574					

Indice di coincidenza: 0.0731