UNIVERSITÀ DEGLI STUDI "ROMA TRE"
CORSO DI STUDI IN SCIENZE COMPUTAZIONALI
IN450 - ALGORITMI PER LA CRITTOGRAFIA – A.A. 2018-2019

M. PEDICINI

ESONERO DEL 09/11/2018 – TEMPO 3H00

COGNOME _____ NOME _____ MATRICOLA _____

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

```
001 FIOPPQNTPN BUUGGMOCYY JFMDVUUDEY ICLDYVITVL IJMMAAPYGF
051 MOEHFKFMTV ZEIFMETVBV KDDNPFVKOI YHJZIVNRUI DCZMBKYAZX
101 AMPEIZYEVW QOKDAPJUOK VTRKQGCZDH LFVIOIAVDM ZXHVLTJEJP
151 EVSZUDMRUJ JUDRRCYNZJ NRJENKDTHG YJEVLRHHOK PTGLBZTJNS
201 LINZJNVYUG ZBIBZUNFIO RNKVCHEAAU GZWEELTVMV NGPQGCVLRN
251 WZCZCBUVZJ NIBUYMVGIT PENVYIILHN VYAYSQXROT BSYXRCAAUE
301 YZMIGAEYZJ RTHDDQUAEZ YNVXOAKEDG MOCYYNKVTH AYDELUNUJJ
```

(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. *Siano date le seguenti S-box (espansive) di codifica di triple di bit in quadruple di bit:*

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

per $i = 1$, S_1 è rappresentata dalla sequenza esadecimale `58F4C162`*, mentre per $i = 2$, S_2 è rappresentata dalla sequenza esadecimale* `A243F168`*,*

(1) Verificare che S_1 ed S_2 siano iniettive e che quindi ha senso considerarne l'inversa (parziale).
(2) Considerare la seguente tabella di approssimazione lineare di S_1:

$$N_L(S_1) = \begin{bmatrix} 8 & 5 & 5 & 4 & 3 & 4 & 4 & 3 & 5 & 4 & 4 & 1 & 4 & 3 & 3 & 4 \\ 4 & 3 & 3 & 4 & 1 & 4 & 4 & 5 & 3 & 4 & 4 & 3 & 4 & 5 & 5 & 8 \\ 4 & 3 & 7 & 4 & 5 & 4 & 4 & 5 & 3 & 0 & 4 & 3 & 4 & 5 & 5 & 4 \\ 4 & 5 & 5 & 4 & 3 & 4 & 0 & 3 & 5 & 4 & 4 & 5 & 4 & 7 & 3 & 4 \\ 4 & 3 & 5 & 6 & 3 & 6 & 4 & 5 & 3 & 4 & 6 & 5 & 2 & 3 & 1 & 4 \\ 4 & 1 & 3 & 2 & 5 & 6 & 4 & 3 & 5 & 4 & 6 & 3 & 6 & 5 & 3 & 4 \\ 4 & 5 & 3 & 2 & 5 & 6 & 4 & 7 & 5 & 4 & 2 & 3 & 2 & 5 & 3 & 4 \\ 4 & 3 & 5 & 2 & 3 & 2 & 4 & 5 & 7 & 4 & 6 & 5 & 2 & 3 & 5 & 4 \end{bmatrix}$$

e completare la seguente tabella di approssimazione lineare di S_2:

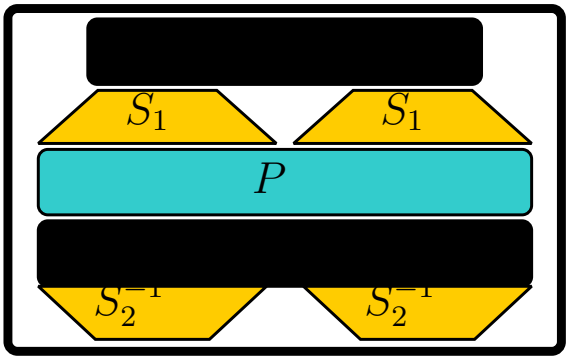
$$N_L(S_2) = \begin{pmatrix} 8 & 5 & 3 & 4 & 5 & 4 & 4 & 3 & 5 & 4 & 4 & 3 & 4 & 1 & 3 & 4 \\ 4 & 5 & 3 & 4 & 1 & 4 & 4 & 3 & 3 & 6 & 6 & 5 & 2 & 3 & 5 & 6 \\ 4 & 3 & 3 & 2 & 5 & 6 & 4 & 1 & 3 & 4 & 6 & 3 & 6 & 5 & 5 & 4 \\ 4 & 3 & 3 & 6 & 5 & 6 & 4 & 5 & \square & 2 & 4 & 5 & 4 & 3 & 3 & 6 \\ 4 & 5 & 3 & 4 & 5 & 4 & \square & 3 & 5 & 4 & 4 & \square & 4 & 5 & 3 & 4 \\ 4 & 5 & 7 & 4 & \square & 4 & 4 & 3 & 3 & 2 & 6 & 5 & 2 & 3 & 5 & 2 \\ 4 & 7 & 3 & 2 & 5 & 6 & 4 & 5 & 3 & 4 & 2 & 3 & 2 & 5 & 5 & 4 \\ 4 & 3 & 3 & 2 & 5 & 2 & 4 & 5 & 5 & 2 & 4 & 5 & 4 & 3 & \square & 6 \end{pmatrix}$$

(3) Per una generica funzione di sostituzione, che relazione c'è tra $N_L(S)$ ed $N_L(S^{-1})$?

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

$$P = (85674321)$$

e il rettangolo in nero la combinazione con la chiave.



Calcolarne un cammino con sbilanciamento non nullo.

Esercizio 3. *Dato il seguente polinomio di 16 variabili suddivise in variabili pubbliche v_i e segrete x_i*

$$\begin{aligned} p(v_1, \dots v_8, x_1, \dots, x_8) = {} & v_1v_2x_1 + v_2v_7x_1 + v_8x_1 + v_1v_3x_2 + v_8x_2 + v_2x_3 + v_1v_2x_3 + v_1v_5v_6x_3 + v_2v_7x_3 + \\ & + v_2v_4v_8x_3 + v_1v_8x_1x_3 + v_1v_2v_3x_2x_3 + v_1v_5v_6x_4 + v_2v_4v_8x_4 + v_2x_5 + v_1v_5x_5 + v_8x_5 + \\ & + v_2v_4v_8x_5 + v_7v_8x_2x_3x_4x_5 + v_2x_6 + v_1v_3x_6 + v_1v_3v_8x_2x_6 + v_2v_4v_6x_1x_5x_6 + v_1v_5x_7 + \\ & + v_1v_5v_6x_7 + v_2v_7x_7 + v_6v_7x_7 + v_1v_3v_5x_2x_7 + v_1v_2x_8 + v_2v_4v_5x_1x_8 + v_6v_7x_4x_8 \end{aligned}$$

(1) trovare alcuni maxterm e commentare se con tali maxterm è possibile stabilire un sistema lineare invertibile di equazioni soddisfatte dalle variabili segrete.

(2) se il numero di maxterm e i superpolinomi corrispondenti non permettono di determinare una soluzione, valutare la complessità residua di un attacco di forza bruta.

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

0	0.0992915					
1	0.0106683					
2	0.0372666					
3	0.040898					
4	0.124034					
5	0.00774706					
6	0.0238545					
7	0.00450298					
8	0.130893					
9	0.0000					
10	0.0000					
11	0.0739683					
12	0.0230959					
13	0.0710147					
14	0.0892042					
15	0.0266789					
16	0.00216272					
17	0.0622024					
18	0.0476283					
19	0.0697719					
20	0.0270179					
21	0.0126858					
22	0.0000					
23	0.000242096					
24	0.0000					
25	0.0151713					

Indice di coincidenza: 0.0780504