UNIVERSITÀ DEGLI STUDI "ROMA TRE"
CORSO DI STUDI IN SCIENZE COMPUTAZIONALI
IN450 - ALGORITMI PER LA CRITTOGRAFIA – A.A. 2020-2021

M. PEDICINI

ESONERO DEL 21/04/2021 – TEMPO 3H00

COGNOME _____ NOME _____ MATRICOLA _____

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

```
0001 WIQVVGPVUI UWNPJEIOKQ PRVIYQWIIG LTFHVWOQSM KHTCNEEWNW
0051 NIZRPIMITC XCOIUOCIHK ZIYOFVJWOI UYKHTQQSGC WQFHRHFBUI
0101 CSYIAMFBTI MJZBPKIIFU YQJRUWGQEY FSOWHRZCCO BRFRPTMEJC
0151 NQFXROGMOH FQZAUEEHPU FRKSAZFWVB EMRYVGEIEM TVTISEQWZV
0201 FWZGQWSDZR TXSSDIZDFV VQZVMMEGPO OEDSYBPICS OCDEQWZVFM
0251 CFTAQIKHZL JULSDBJHZF TBUMVRTYVI JHPTJFVFEI FHZULZBRKW
0301 CVFQVRTIOX VATAVVVDCW HVVGDQWIUW NISEKHPZFR RNTWOECSPQ
0351 OXVFYIAMFB LTFPLBTDFV JOWMFHVTQM UXZJZZJGFB ZADMDSYBPI
0401 IWDXFXKCEI OXFTCIJTFD ZTJHVUWQTX VGDQTXRHTU FQSFTYVEEH
0451 ZNSEHIPTMM USTBFVIWEW SMJCEBPTFG EQBPCOWWSS XWFZJWUWKQ
0501 PRVOCBJGFZ ZBVXKWRTJI JGPZJYDOYQ OEJQZVPPZP PZJIUSRCBP
0551 ZWYLJKEWEI FHZFTBUMVG DQTSECOWUE KWOQSEXWZV FIUWNWTGZS
0601 YHBIUSGWOS RUTZFKCWFV JZVFDWHPZO WBSMZBDXJV ZHZLJJIOEM
0651 MPRBKIBVKW NWMSRRZOOM ZBOQWMUIZA QIKHLVPXLH EQJHZFTBUM
0701 VHFBUICSWQ CIIHLMOYEQ TIUIESWTBT ISDMOXVRTK IMRFLHJSES
0751 DMODRRTAUM ENTWOIRZNC OEGSCZBKZC YQEMIOKHBH ZQZTPVVRTA
0801 FWJCOQMMEU FIEMISWQHM FBPLJSGWYQ PRVDZTJXZQ LWEMRZEZPK
0851 VBPZFHZCCQ HMESYIAMFB LTFSJCNQBP VRTZJGTVPH AEUWYITGZH
0901 LWEMRZEZBG FBOQAMFBPV FWJIYIEMJH TVAMFBPABV RWYWMXISDB
0951 BFZZTBBWLZ WICEJSOMMP FGEIUYKCAW MMKWNWHMLF TLJGFCTVUI
1001 IBLHJSEOWM EICDLMTIFR PTUIIFTBPV ZCNCJYEOAM SWFBLIQTRF
1051 EQFRVGTIJR UWAMOHVBEM PWFHEWQSJH ZIEEDATVJW KFLHJSESQQ
1101 EYTWLZJEFB ZVBYKCYWNS FGZOHIKHZI RYRZDQBWZZ TUJXRNTWOI
1151 UWDWWVRBTB BEIHTKPPFC RVJMERTDJH LCSIEMIWEB PECZLDJXRO
```

(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 terzo sottoblocco estratto dal cifrato;
(4) Ipotizzare una chiave g per il terzo sottoblocco (in base alle frequenze alfabetiche del blocco);
(5) Verificare l'ipotesi utilizzando l'indice di mutua coincidenza M_g.

Esercizio 2. *Dato il seguente polinomio di 20 variabili suddivise in variabili pubbliche y_i e segrete x_i*

$$p(x_1,\dots x_{10},y_1,\dots,y_{10}) = x_{10}x_2x_3 + x_1x_2x_6 + x_1x_2x_5x_9 + x_2x_7x_9 + x_1x_2x_7x_9 + x_1x_3x_7x_9 + x_1x_5x_7x_9 + x_{10}x_2x_3y_1 + x_4x_5x_6y_1 + x_6x_7y_1 + x_3x_4x_5y_{10} + x_3x_6x_8y_{10} + x_9y_1y_{10} + x_3x_4y_1y_2 + x_3x_8y_1y_2 + x_1x_5y_3 + x_3x_9y_3 + x_2x_3y_1y_3 + x_1x_9y_{10}y_3 + x_1x_{10}x_6y_4 + x_{10}x_4x_7y_4 + x_2x_7x_8y_4 + x_8x_9y_4 + x_4x_8y_2y_4 + x_8y_1y_2y_4 + x_1y_{10}y_2y_4 + x_2x_5y_3y_4 + y_1y_3y_4 + x_3y_1y_3y_4 + x_3x_8y_5 + x_7x_8y_{10}y_5 + x_1x_{10}y_2y_5 + x_5x_7y_2y_5 + x_8y_2y_5 + y_{10}y_2y_5 + x_8y_{10}y_2y_5 + x_3y_1y_3y_5 + x_6y_{10}y_3y_5 + x_4y_4y_5 + x_2y_2y_4y_5 + x_9y_6 + y_1y_{10}y_6 + x_2x_3y_2y_6 + x_5y_3y_6 + x_4x_5y_4y_6 + x_3y_3y_4y_6 + x_{10}x_5y_7 + x_{10}x_2x_7y_7 + x_{10}x_5y_1y_7 + x_1x_{10}y_2y_7 + x_7y_2y_7 + x_3y_{10}y_2y_7 + x_5y_{10}y_3y_7 + x_9y_1y_4y_7 + y_3y_4y_7 + x_6x_8y_6y_7 + x_8x_9y_6y_7 + x_1x_7y_8 + x_5x_8y_8 + x_{10}x_9y_8 + x_3x_7y_{10}y_8 + x_1x_4y_2y_8 + x_5y_3y_8 + x_3x_5y_3y_8 + x_7y_3y_8 + x_5x_9y_3y_8 + x_7y_4y_8 + x_1y_{10}y_5y_8 + x_7y_2y_5y_8 + x_{10}y_4y_5y_8 + x_{10}y_7y_8 + x_1x_4y_7y_8 + x_{10}y_2y_7y_8 + x_9y_3y_7y_8 + x_1y_4y_7y_8 + x_{10}x_5x_6y_9 + x_1x_8x_9y_9 + x_2x_9y_1y_9 + x_7x_9y_1y_9 + x_8y_2y_9 + x_3x_8y_3y_9 + x_2x_9y_3y_9 + y_1y_{10}y_3y_9 + x_9y_{10}y_5y_9 + x_6y_6y_9 + x_9y_6y_9 + y_3y_5y_6y_9 + x_9y_{10}y_8y_9$$

(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.

Esercizio 3. *I primi 10 termini di una sequenza generata per ricorsione lineare di ordine ≤ 5 in $\mathbb{F}_2$ sono*

$$0110000111.$$

Determinare il polinomio minimo della sequenza utilizzando l'algoritmo di Berlekamp-Massey.

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

0	A	0.110626				
1	B	0.0112005				
2	C	0.0433659				
3	D	0.0412981				
4	E	0.10718				
5	F	0.0102527				
6	G	0.0213957				
7	H	0.00901781				
8	I	0.124095				
9	J	0.000574383				
10	K	0.00189546				
11	L	0.0698449				
12	M	0.0273406				
13	N	0.0671453				
14	O	0.091614				
15	P	0.0263929				
16	Q	0.00201034				
17	R	0.0674899				
18	S	0.0496554				
19	T	0.0610281				
20	U	0.026479				
21	V	0.0176623				
22	W	0.00114877				
23	X	0.000775416				
24	Y	0.00186674				
25	Z	0.00864446				

Indice di coincidenza: 0.0780504