UNIVERSITÀ DEGLI STUDI "ROMA TRE"
CORSO DI STUDI IN MATEMATICA
IN450 - INFORMATICA 6
ALGORITMI PER LA CRITTOGRAFIA – A.A. 2014-2015

M. PEDICINI

ESONERO DEL 03/11/2014 – TEMPO 3H00

COGNOME _____ NOME _____ MATRICOLA _____

Esercizio 1. *(15pt) Il seguente crittogramma derivato da un testo in lingua italiana*

```
0001 HYRKF RQBCS  CPNFC UMPNA  FGUDJ FPTDO  DIMYC XMBQB  FXEZR LIPZH
0051 VRRMC EMASS  IVBSH VHVLC  EXVSI KXRZG  VRVDO XSYEW  RWRBC EHNCS
0101 CPBRD FVTDF  VIQDZ IMRMH  IEEDR ZUHDZ  CMIHS EUHZG  ZEHMH IEGSC
0151 RVVRH IMAFS  IWVDO GVRMR  VVPNF JSREW  XYEZR ZJVTA  VXEZI ETENA
0201 FRGNF ZSNCS  JXEZS LRNLD  ZEPNG KMRQO  UEYKO CXEZD  RVGDS ZPCNB
0251 KIPGS ZZVBC  EKVTB XIYDR  LIEHJ VTNQQ  YIEDB UENMQ  FVCHG VRFHP
0301 ZPRZZ CSPBV  ZSDTS JXNSF  RWSNF DEMHC  EIRRS XRVHZ  GYASC ZRPTW
0351 ZPYZU FGRRG  RIYZR UEEHB  TSZHB TMNOS  IVVOW XPVZF  GSVMC DIQHZ
0401 RKBCC MIYDF  ZZRZZ CSASO  EEACC JMQHB  LSINZ RWPHO  EPNBE LEQHG
0451 KIACS IWVDF  RPYDB KEERW  ZRATC MMTNZ  WMRHB EYBUW  JIAHZ RGBRH
0501 ZIEZT FVZZH  RHNKR VTBRW  KSQHH IITQC  JWVSC IVRMH  ZWPDB UINOD
0551 FKTHO KENCI  VQBMH ZGBMH  ZKHHZ LRBCS  KXBCW JEALO  IXVMC CEYSF
0601 FGBMJ FGRKC  DFNQR RMYQS  JITNB VHNHA  FPGHG LSVBC  TYMYC CMVMT
0651 ZPNBV VMAUS  ISYNT RRANG  FQVFZ ZEEDO  LRNRS XEGZZ  TLANB TLVZZ
0701 GVVLC MIQDF  CSCTF TLFHO  UMSQC EXRBC  DICDF VWRLD  ZSQHG LPRLI
0751 IEQHA ZPNMC  TLRFI RVQZB  FEFDH KIASF  ZSADB FRYNR  ZWPDF EEGNG
0801 KSNTB KEYBC  EXEZG JITMC  ZRDTS CPNKI  EKNDJ RWGZU  ZSTZW RHNFZ
0851 ZEYSF ZQBMH  ZHVMC DICHC  JGHQC VHVEC  IQNOW TSZTB  VTRQI EFHNB
0901 GIMYC CEPNG  KEFZZ VGBMI  ETRMR ZSYDB  KSRBC EXVMI  FTBHG ZVBLD
0951 VMAOC XKVDW  EZNKZ FRPDZ  CMVMS IXRDW  EMFOW RRNSS  JIPNB USYNG
1001 JEGTF RHRCI  VQBMH ZIVKZ  RZBQC UIYKO  TUHDW CPRLP  FIFSF VQBSO
1051 XPVZH FHNKZ  VJBBW UIGNF  IIASW HYNRW  KYGSC XLVZW  RIPHC KXBKC
1101 EMVKF VWGNQ  RQCHS MMTMS  JTNQG VHVSS  IVRCW MMYKS  UMPZG RPVHB
1151 HYNKQ YICZF  KIONG TLVBV  VWVOF FPHMU  RRBRI GIEKO  DSASO XRNKS
1201 TGBKO GVVMQ  ZTNKS UMDTS  CPRSS IVRDQ  YIQMC DINKH  VVEHH FVVNU
1251 ZEPDD FGBCW  JGBRH FHNKD  FRGDO CPNQW  MEQDZ CETNO  EDVUW VRRHB
1301 GEESS RXENJ  RVFHB VPYZU  FWGDG JSDTO  EHBPI VWGNW  EKENG JEHMU
1351 IEAAC IKBZZ  XMBQB FHBFU  ZIPGS JMABO  DQVMO RHVUS  EXNQQ ZXGZW
1401 KIZOW ZRPTW  RGPZR UIENW  WEGSW TLROF  VRQHO DSNQO  TGBMH RVRPI
1451 VPONF XSTHQ  FRFHR VVNAW  CIRQO RRPGS  LRPZG KIYKC  VEIDJ RTRQQ
1501 ZPBMC IIQZZ  CSTFW RVRTB  TSZZB UEASS  VMYUO EXNFU  ZSQHD FWFDR
1551 VVRTB RWGZP  ZPRFI RVAHU  ZSADR ZWBKR  RXVRD RKANZ  ZGUDW EWRFB
```

```
1601 RZNMZ RQBCS  JXVZO CPREO  EGVTZ CIRZZ  CIQNB EIQDZ  GERRS RGPZF
1651 VDMZJ RRQHH  VQCNW EXRLD  FPRRD RPYDO  HYNKQ YIZZF  ZXBZE LEYBV
1701 VTNCF VIFTZ  WMAHF UIYKS  JXNSS ESALO  EGNUO EQNHR  ZWCZB UIERW
1751 EIYKS MMTMS  GIECW IEQZF  CYIDS RPYDU  XIEHF VEPNB  KEQHB ZPREO
1801 KMPGS UIYKO  MIACS DQVZR  RPYTB REYKO  CXEZR ZUHDZ  CIGDF IIQZZ
1851 CEYSI IINKZ  RVVUO UEHMD  FKTHC RPYZZ  KVBBC IVRUO  ESRBC IVBMC
1901 KYGSO MMNRH  IEQDS JXEZR  VXGDD ZSZDB  IMCHR VSCHO  EIBFB ZXNMH
1951 FESEC EHNSS  JICNZ KIGQO  UYRLI IMQNB  UINKN RRQNZ  FWTTO IHBMC
```

presenta il seguente schema di frequenze:

```
(A) 0.016 (B) 0.044 (C) 0.049 (D) 0.038 (E) 0.056 (F) 0.043 (G) 0.036 (H) 0.048 (I) 0.055
(J) 0.015 (K) 0.030 (L) 0.014 (M) 0.040 (N) 0.042 (O) 0.025 (P) 0.030 (Q) 0.032 (R) 0.077
(S) 0.053 (T) 0.030 (U) 0.021 (V) 0.057 (W) 0.028 (X) 0.020 (Y) 0.024 (Z) 0.070
```

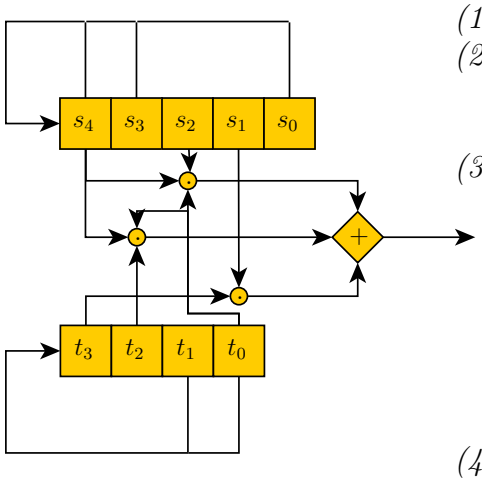
(1) verificare che il cifrario utilizzato è polialfabetico;
(2) eseguire il Kasiski test e stabilire la lunghezza della chiave;
(3) verificare che la lunghezza della chiave stabilita al punto precedente è corretta;
(4) decifrare il messaggio.

Esercizio 2. *Sia dato un crittosistema costituito da due LFSR a 5 e 4 bit temporizzati in modo sincrono con coefficienti rispettivamente:* $(c_4, c_3, c_2, c_1, c_0) = (1, 1, 0, 0, 1)$ *e* $(d_3, d_2, d_1, d_0) = (0, 0, 1, 1)$. *Posto lo stato del primo registro al tempo* t, *uguale a* $S_t = (s_4, s_3, s_2, s_1, s_0)$ *e quello del secondo registro* $T_t = (t_3, t_2, t_1, t_0)$ *la funzione di aggiornamento opera nel modo usuale*

$$S_{t+1} = (\sum_{i=0}^{4} c_i s_i, s_4, s_3, s_2, s_1) \qquad \textit{risp. } T_{t+1} = (\sum_{i=0}^{3} d_i t_i, t_3, t_2, t_1)$$

Il keystream del sistema sia infine ottenuto tramite la funzione di combinazione **non lineare** *(così come riportato in figura):*

$$z_t = s_4 s_2 t_0 + s_4 t_0 t_2 + s_1 t_3.$$



Rispondere ai seguenti quesiti:

(1) fornire un limite superiore al periodo del keystream;
(2) fornire una (unica) matrice $M \in \mathbb{F}_2^{9\times 9}$ *che applicata al vettore di stato* $S_t||T_t$ *rappresenti la funzione di aggiornamento dei registri;*[a]
(3) sia il cifrario inizializzato al tempo $t = 0$ *con i bit di chiave*

$$S_0 = (x_4, x_3, x_2, x_1, x_0)$$

il primo registro e con i bit di un vettore di inizializzazione

$$T_0 = (v_3, v_2, v_1, v_0)$$

il secondo registro. Determinare l'espressione algebrica di z_t *per* $t = 0, \ldots, 5$.
(4) Sia $p(x_0, x_1, x_2, x_3, x_4, v_0, v_1, v_2, v_3) = z_5$ *determinare tramite il cube-attack un suo maxterm nelle variabili pubbliche* (v_0, v_1, v_2, v_3) *ed il rispettivo superpolinomio.*

[a] $w_1||w_2$ denota la concatenazione di due vettori.