UNIVERSITÀ DEGLI STUDI "ROMA TRE"
CORSO DI STUDI IN SCIENZE COMPUTAZIONALI
IN450 - ALGORITMI PER LA CRITTOGRAFIA – A.A. 2022-2023

M. PEDICINI

ESONERO DEL 22/04/2022 – TEMPO 3H00

COGNOME _____ NOME _____ MATRICOLA _____

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

```
0001 XHZDR NNOGB MJWNI XNMNY NYLVW WZECX CIMLI PBCIU YKJLJ UYYRW
0051 JDMDW JJBNZ RHAAI ICYVU FVAND LIGXL VLWCR OYNPV WIKJL HROIJ
0101 FOXMZ WMJYI GRNDL IZLIH YYIMC VEUIX CILYM CIHXX JUUNL CZWTV
0151 MYGVI OXMJL CVUYI NFNNW JUISR RZPFD UYKAI ANLDE UKJLG JHYXU
0201 GUIUB WCXEF NYUBW CXEFN WVWOO XGVMU IRGVP CJECI NYMNJ PKVGR
0251 WVWUG NLVLW JPFDN PVLII JGJAY ZUYMN ADBNM JPVRH AAIIC YVDHN
0301 DIGRV MXCIC LVEPZ MYIMI QROIJ JMXZZ ICVMC QRNOX LDJYY RWDEC
0351 GCKPJ HYXWJ DMDWJ VAFVE ULDYG UYKJL JUYGJ ZMJHX RUZAU NLBDJ
0401 PVJOI MCKAY NBIXX GJPAD WIDBC VVIDV CMJWJ UCMNJ PKVGR WVWCO
0451 XLIJN DRHID FGJFZ LIMAO OCYGN XZPIQ NLIRH PUFDR HONLH NXDOL
0501 VUUXX HQNHU RIINY WXHVY UMCYG NMZAP DUCOM YGUCH YYMXW CNNMJ
0551 MKJLD EUIXU OCLVE YMBID UGVWN JMCBU IMRUN CYNXX VUAZW CJMYG
0601 UOJVI YNFYN MORHJ YIDUU ORLVW HDMYY NFMRM OXLVV YICIG NVMRA
0651 CNMVL YMMIO JFDNA ZBODC CXQYG NXZUO NRIIR YGJWJ ANDPC VWYMR
0701 UKAYQ JFZWN ZJPZE UIXXD OZPBI PWMJW HJBOG UYHNH ORXZP FDDIH
0751 RHDMY GUOIJ JVLYN CUILU PWMDU YIICJ MCMXP DWUXQ YQRYO JPVXA
0801 IRMKN LVWTV MCHNA GRIGN ZJATZ MYGUU BNHZA UURII NHVCU AAUDM
0851 OZBYX XFDGP DRCZG CSBYM JHJLI IBOHJ NZWYD ZOVAU ICUVW HDMCB
0901 DYMAU JBNDW UOJYY RMVPL DOCXR MKNMD JLDLU YNLZW YGOUI PIYXH
0951 YNUQN UQXFP CIGNP VAMDP FDDIH RHDLB ZJPZJ HJEYY DNJRF KACHX
1001 YGDFO RGJPC JAHJM OIJLD EIGDT DXHZM YNCCI JNVJG PCUMN FZBIM
1051 CCZDL JYYZM CNYYM JPVWI YNFKA IBAYN BIOJH ONWMN XZWTZ BYMJH
1101 JJWXD GPUUO NCIZO ZUFJB JVICJ MCONG KXYOJ HONPJ UNZUU KAYKX
1151 NZWTV MYAJN ORFZJ PZJMJ OZJLU ONWCN AGRUI RGDNL VWIBR OICCV
1201 ACIWY BJLZX AIRZZ MYZPF DWNZU FZCND PCVLY QJHJB WJWZJ ANVCC
1251 VEPDU CORMA RXPLC VCCYN FGJPQ NHDAY GNNZX LDLBZ OCGXM JOCXQ
1301 YKNLY DNVXA IRUOC CQRNY NMVVY JPHDN WXRNV VYICI YRWJW NMJMO
1351 XXJAG DEUIX HZUGV CYMRU GRMHX XZUMZ LIGXR QRCDN WJWZD WUQJH
1401 JUOJV IINFG NMZAW DICJM YGUYA JWJUN DWXDE CYDUG RFZCN ZAUOD
1451 LVWII EYMJN MJHIN HZUFZ JWXJX ZVCZE YIMOO NUGYI ONLZZ OVUOI
```

(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. *(1) Si consideri il campo finito $\mathbb{F}_9 \approx \mathbb{F}_3[x]/x^2 + x + 2$: si descriva la definizione delle operazioni di somma e prodotto per gli elementi del campo e si fornisca un esempio di somma e prodotto per elementi non banali.*
(2) calcolare l'inverso moltiplicativo di 5.
(3) Il periodo di lunghezza 80 di una sequenza LFSR di ordine ≤ 4 in $\mathbb{F}_9 \approx \mathbb{F}_3[x]/x^2+x+2$ è

(20581846877086563264406282172330276754711074248345504373613880314125166015357852).

(a) Determinare il polinomio minimo della sequenza utilizzando l'algoritmo di Berlekamp-Massey.
(b) Discutere un metodo alternativo per ricavare il polinomio minimo della sequenza.

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

0	A	0.1078					
1	B	0.0084					
2	C	0.0410					
3	D	0.0384					
4	E	0.1173					
5	F	0.0118					
6	G	0.0198					
7	H	0.0099					
8	I	0.1123					
9	J	0.0001					
10	K	0.0001					
11	L	0.0677					
12	M	0.0260					
13	N	0.0758					
14	O	0.0944					
15	P	0.0289					
16	Q	0.0048					
17	R	0.0666					
18	S	0.0492					
19	T	0.0609					
20	U	0.0296					
21	V	0.0206					
22	W	0.0001					
23	X	0.0002					
24	Y	0.0001					
25	Z	0.0080					

Indice di coincidenza: 0.07346