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

M. PEDICINI

ESAME DEL 19/01/2017 – TEMPO 3H00

COGNOME _____ NOME _____ MATRICOLA _____

Esercizio 1. *Dato il seguente polinomio di 16 variabili suddivise in variabili pubbliche v_i e segrete x_i*

$$p(v_1,\dots v_8,x_1,\dots,x_8) = x_1 + v_2x_1 + v_6x_1 + v_2v_4v_6x_1 + v_7x_1 + v_5v_7x_1 + v_1x_2 + v_2x_2 +$$
$$v_3v_5x_2 + v_5v_7x_2 + v_8x_2 + v_7x_1x_2 + v_5v_7x_1x_2 + v_1x_3 +$$
$$v_2x_3 + v_4x_3 + v_2v_6x_3 + v_2v_4v_6x_3 + v_7x_3 + v_5v_7x_3 +$$
$$v_7x_1x_3 + x_2x_3 + v_3v_5x_2x_3 + x_4 + v_1x_4 + v_2x_4 + v_2v_6x_4 +$$
$$v_5v_7x_4 + v_8x_4 + v_6v_8x_4 + v_5v_7x_1x_4 + x_2x_4 + v_3v_5x_2x_4 +$$
$$v_7x_2x_4 + v_3v_5x_3x_4 + v_7x_3x_4 + v_2x_5 + v_3x_5 + v_2v_4v_6x_5 +$$
$$v_7x_5 + x_2x_5 + v_3x_2x_5 + v_3v_5x_2x_5 + v_7x_2x_5 + v_5v_7x_2x_5 +$$
$$v_3v_5x_3x_5 + v_5v_7x_3x_5 + v_3x_4x_5 + v_7x_4x_5 + x_6 + v_1x_6 +$$
$$v_2x_6 + v_4x_6 + v_3v_5x_6 + v_2v_6x_6 + v_2v_4v_6x_6 + v_6v_8x_6 +$$
$$v_7x_1x_6 + x_2x_6 + v_7x_2x_6 + v_3v_5x_3x_6 + v_7x_3x_6 + v_3v_5x_4x_6$$

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

Esercizio 2. *Sia $h : \{0,1\}^* \to \{0,1\}^n$ una funzione di hash che è resistente alla seconda contro-immagine e resistente alla collisione.*

Si prenda $h' : \{0,1\}^* \to \{0,1\}^{n+1}$ come la funzione di hash definita nel modo seguente:

$$h'(x) = \begin{cases} 0||x & \text{se } x \in \{0,1\}^n, \\ 1||h(x) & \text{altrimenti.} \end{cases}$$

(1) Dimostrare che h' non è resistente alla controimmagine.
(2) Valutare la complessità dell'algoritmo randomizzato per la ricerca della controimmagine e confrontarlo con quella di una funzione di hash ideale nel ROM (Random Oracle Model).
(3) Mostrare che h' continua ad essere resistente alla seconda contro-immagine e restituente alla collisione.

Esercizio 3. *Si consideri la sequenza*

$$p = (100011)$$

trovare un LFSR di lunghezza minima che genera una sequenza definitivamente periodica con periodo p.

Esercizio 4. *Per errore, uno stesso messaggio è stato cifrato due volte con il crittosistema di Vigènere; il primo messaggio ricevuto è il seguente*

```
TVXVUEPMFP QSZACIDHDL IMXEBPOEZI ESEFXWTZEE DLSOWTKMRC
TWXSGQHZPN SXWRWRUJCS YSATEJPLSO SATETDMATG HQSETEGTFX
BMIPSHLJPV SJTDIEWTAM RAZOCCCWMC ERSDWSMRKT LWYEJQWZIO
FPSXLYVVII OWRQEJHIGE SCBMZAPFPG XLIEIEQZBP BXFSIBZPXT
ITDMATGTZE QXOBPAXLMJ HEQSSAIWVC TSYNPMVRKE BFHPMGYTIZ
RWJLMQXOSC OHBEKDTSCF XJMCTMORWA QQGTROECGM PRKEJLAXBM
XPTCWWCYYZ HIHZFTUMCT SGPZPAIEIE BKORWRUPNB LHDIQFGTSA
CXTIJHEWWF TAGIXTHZWB XIIXAZPZPX IEPCCXAJBE KPIBBIXVHZ
RIOYBXLMTP RQPFTLYIDD ODQDVXRGSW YSATEWDRHP NOIHZHPWPZ
QMVXGIGACH QWZPFOEHPT ZFAOBERXLM FTMWLWCBIE OICYSTZEMT
ROXSCBIUXR WNSKMVVSAQ CWHBMRCOEF SHBSFGRSYR DKSCEOSYCC
USJIROCSCV YKGIFPFXAI EIIAPBIWGF CTFZQWQGTW EGDWPQPGGE
GTRTVXVAOR WOBQEKGABB IXTPZIEATQ DVWZVLWLGT ZFRGLODSBX
VVSIQPBSWQ ZRHSOOFCIJ IAHCOCYYZA LWEDDBIRSI DPBSMVVAEG
```

mentre la seconda volta viene intercettato il messaggio:

```
EEXDESBSVZ HCICGTRHOU IUHSNVEOQS NUIQLWEIEM NZEUMDBWAE
XHLSRZHHZB EDMBNBDLGD MSLCERZZEU IKKOCFQLHG SZSMDSSZVH
SWRRWSZJAE SRDRUKMDRW ACDZQCNFMK OFEJMCDBTV PHMEUZWHSC
RVIHCIEXMT CWCZERRWSK IMSWICTQDG IUIMSSCFRZ SHOUMMNPIC
IBNAMZWDQO ZZSMDAIUMR RSCYIKZGEE XDMNAVVZUS NLXZDQHVMK
FWUUMYHCEI ERSOTFXDQF ISMKDAAXMK HAPVVZSCRV PZUSVRQHSW
GRXNKWNHYH RWTFVDLWLV WRDZAJIMSS NQEBNBDRRM ZHORQNQHEG
SHKSSJIHKF EJGQHHTFML OSRZEKDZAG IMZQODQTSO TRMMPIIEHH
BWAERHCWCR VBDFEUYQNR AJGNMHAIWH MSLCEENFTV DYZRIJTHDZ
BVVFQWSGSR HGIRJZSHAC ZNKCNKHHCW OVQHZWNKIM YWOEIDQOVV
VZLSNKICHF ITIUDFEUEB QWSKMZMCQL IRSCOIVDMR OTSKOCEESM
LCSKVZQSNE YSQWRVVHRS NKMLDBTFGN MHRFGGHQCY IRRWAZPOQS
SZHDMHECSC KOMZESQONH YHKZIKILHQ OEWHFZIRWD QPAIPZRSMG
VDCWCVRCNA ITLDCOQLIR SOTIEMPIIC PHSDOKIZCW PVRCDFECIR
```

(1) determinare la lunghezza delle due chiavi;

(2) determinare il testo e le chiavi con un metodo algebrico (non statistico).