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

M. PEDICINI

ESAME DEL 22/01/2019 – TEMPO 3H00

COGNOME _____ NOME _____ MATRICOLA _____

Esercizio 1. *Si consideri il seguente crittosistema operante in modalità contatore (counter mode, ovvero con un vettore di inizializzazione incrementato ad ogni utilizzo della cifratura):*

$$C = Hill(IV) + P$$

- *In questo esercizio la funzione Hill corrisponde alla cifratura di Hill operante su* $\mathbb{F}_{2^3} \simeq \mathbb{F}_2[x]/g(x)$ *con* $g(x) = x^3 + x + 1$ *ed è definito dall'equazione:*

$$(y_1\, y_2) = (x_1\, x_2)M \text{ con } x_1, x_2, y_1, y_2 \in \mathbb{F}_{2^3}$$

- *La chiave è data dalla matrice*

$$M = \begin{pmatrix} x^2 & x+1 \\ 0 & 1 \end{pmatrix}$$

  i cui elementi sono in questo caso espressi come polinomi di $\mathbb{F}_2[x]/g(x)$.
- *Il valore iniziale del contatore è* $IV = 39$.

(1) Verificare che la chiave del cifrario di Hill è valida.
(2) Definire la funzione di decifratura esplicitando la matrice inversa e verificare.
(3) Cifrare il messaggio 101101011111.

Sapendo che sono state intercettate delle coppie plaintex-ciphertext cifrate con una chiave incognita M *in modalità ECB,* $P = 001\,100\ 010\,111\ 000\,111\ 110\,101$ *corrispondente al testo cifrato* $C = 111\,100\ 000\,011\ 010\,010\ 100\,011$*, sapendo inoltre che l'IV iniziale è* 39 *trovare la chiave (ovvero la matrice* M*).*

Esercizio 2. *Sia* $S_{RD}(x) = g(f(x))$ *adattata al campo* $\mathbb{F}_{2^4} \simeq \mathbb{F}_2[x]/x^4 + x + 1$ *a partire dalla funzione dell'AES, dove*

$$f(x) = \begin{cases} x^{-1} & \text{se } x \neq 0 \\ 0 & \text{altrimenti} \end{cases}$$

$$g(z) = (x^3 + x^2 + 1)z + (x^3 + 1) \mod x^4 + x^3 + 1.$$

Si consideri il cifrario dimensionato per uno stato a 8 bit con chiave di 4 bit:

$$\mathsf{Enc}_k(x) = \mathsf{AddKey}(k_2, \mathsf{SubBytes}(\mathsf{AddKey}(k_1, x)))$$

(1) si adatti l'algoritmo di key scheduling di AES per ottenere (k_1, k_2) *a partire da* k*;*
(2) si fornisca la tabella di sostituzione di SubBytes*;*
(3) si cifri il messaggio rappresentato in esadecimale: $P =$ 0xAB05 *con la chiave* $k =$ 0x00 *modo operativo ECB;*

(4) Siano note le seguenti coppie di plaintext-ciphertext:

$$T = \{(0000, 1110), (0110, 0101), (0101, 1000), (1111, 0100)\}$$

descrivere un possibile attacco known-plaintext *per ottenere la chiave.*

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

$$\begin{aligned}
p(v_1, \dots v_8, x_1, \dots, x_8) = {} & x_1 + v_2x_1 + v_6x_1 + v_2v_4v_6x_1 + v_7x_1 + v_5v_7x_1 + v_1x_2 + v_2x_2 + \\
& v_3v_5x_2 + v_5v_7x_2 + v_8x_2 + v_7x_1x_2 + v_5v_7x_1x_2 + v_1x_3 + \\
& v_2x_3 + v_4x_3 + v_2v_6x_3 + v_2v_4v_6x_3 + v_7x_3 + v_5v_7x_3 + \\
& v_7x_1x_3 + x_2x_3 + v_3v_5x_2x_3 + x_4 + v_1x_4 + v_2x_4 + v_2v_6x_4 + \\
& v_5v_7x_4 + v_8x_4 + v_6v_8x_4 + v_5v_7x_1x_4 + x_2x_4 + v_3v_5x_2x_4 + \\
& v_7x_2x_4 + v_3v_5x_3x_4 + v_7x_3x_4 + v_2x_5 + v_3x_5 + v_2v_4v_6x_5 + \\
& v_7x_5 + x_2x_5 + v_3x_2x_5 + v_3v_5x_2x_5 + v_7x_2x_5 + v_5v_7x_2x_5 + \\
& v_3v_5x_3x_5 + v_5v_7x_3x_5 + v_3x_4x_5 + v_7x_4x_5 + x_6 + v_1x_6 + \\
& v_2x_6 + v_4x_6 + v_3v_5x_6 + v_2v_6x_6 + v_2v_4v_6x_6 + v_6v_8x_6 + \\
& v_7x_1x_6 + x_2x_6 + v_7x_2x_6 + v_3v_5x_3x_6 + v_7x_3x_6 + v_3v_5x_4x_6 + \\
& v_7x_4x_6 + v_5v_7x_4x_6 + v_3v_5x_5x_6 + v_7x_5x_6 + v_2x_7 + v_3x_7 + \\
& v_2v_6x_7 + v_2v_4v_6x_7 + v_8x_7 + v_5v_7x_1x_7 + v_3x_2x_7 + \\
& v_3v_5x_2x_7 + x_3x_7 + v_3v_5x_3x_7 + v_7x_3x_7 + v_5v_7x_3x_7 + x_4x_7 + \\
& v_3x_4x_7 + v_7x_4x_7 + x_5x_7 + v_7x_5x_7 + x_6x_7 + v_3v_5x_6x_7 + \\
& v_2x_8 + v_6x_8 + v_2v_4v_6x_8 + v_7x_8 + v_6v_8x_8 + v_7x_1x_8 + \\
& v_5v_7x_1x_8 + v_3v_5x_2x_8 + x_3x_8 + v_3v_5x_3x_8 + x_4x_8 + v_7x_4x_8 + \\
& x_5x_8 + v_5v_7x_5x_8 + x_6x_8 + v_3v_5x_6x_8 + v_7x_6x_8 + v_5v_7x_6x_8 + \\
& v_7x_7x_8 + v_5v_7x_7x_8
\end{aligned}$$

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