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

M. PEDICINI

ESONERO DEL 9/6/2022 – TEMPO 3H00

COGNOME _____ NOME _____ MATRICOLA _____

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

$$\begin{aligned} p(v_1,\dots v_8,x_1,\dots,x_8) = {} & v_1v_2v_3v_6x_5 + v_1v_2v_3v_6x_6 + v_1v_2v_3v_6x_7 + v_1v_6x_1 + v_1v_6x_8 + v_2 \\ & v_4v_7x_2 + v_2v_4v_7x_4 + v_2v_4v_7x_5 + v_2v_4v_7x_6 + v_2v_4v_7x_7 + v_2v_7 \\ & x_1 + v_2v_7x_7 + v_2v_8x_2 + v_2v_8x_3 + v_2v_8x_7 + v_3v_4v_5v_6x_3 + v_3v_4v_5v_6 \\ & x_4 + v_3v_4v_5v_6x_7 + v_3v_4v_5v_6x_8 + v_3v_6v_7x_1x_4x_6x_7 + v_3v_6x_4 \\ & x_7x_8 + v_3v_8x_1 + v_3v_8x_2 + v_3v_8x_3 + v_3v_8x_4 + v_3x_1x_2x_7 + v_4v_5x_2 \\ & x_4 + v_5v_7x_1x_7 + v_5x_3x_7 + v_5x_6 + v_5x_8 + v_6v_7x_7 + v_6v_8x_4 \end{aligned}$$

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

Esercizio 2. *(KeyExpansion/AES-SubBytes) Sia $p(x) = x^2 + 2x + 2$ si consideri la S-box di AES/Rijndael adattata opportunamente con elementi che incorporano le operazioni sul campo finito $\mathbb{F}_{3^2} = \mathbb{F}_3[x]/p(x)$.*

Eseguire un round di cifratura di AES del blocco $X =$ `2133876504372102` *ponendo la chiave $k =$* `800073550841` *(la notazione va considerata già espressa nel campo $\mathbb{F}_{3^2}$):*

(1) Verificare che $p(x)$ sia irriducibile in $\mathbb{F}_3[x]$;
(2) Adattare opportunamente l'algoritmo AES alle dimensioni del campo discutendo la scelta effettuata (in particolare nel caso della SubBytes*).*

Nel seguito le funzioni SubBytes, ShiftRows, MixColumns *e* AddKey *sono quelle dell'algoritmo adattato:*

a. Calcolare $S_1 =$ SubBytes(X);
b. Calcolare $S_2 =$ ShiftRows(S_1);
c. Calcolare $S_3 =$ MixColumns(S_2);
d. Calcolare $S_4 =$ AddKey(S_3, key_0) dove key_0 è il primo elemento del KeySchedule *calcolato a partire dalla chiave k.*

Esercizio 3. *(Differential Cryptanalysis) Calcolare la tabella delle caratteristiche differenziali per la S-BOX $f : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ definita da:*

$$f(x_1, x_2, x_3, x_4) = (x_2\, x_3, x_1x_4 + 1, x_1 + x_2 + 1, x_1 + x_2 + x_4).$$