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

M. PEDICINI

ESONERO DEL 9/01/2019 – TEMPO 3H00

COGNOME _____ NOME _____ MATRICOLA _____

Esercizio 1. *Ricordare la definizione di cifrario di tipo Feistel (cifratura e decifratura) e mostrare che non è necessario avere una* sostituzione *(s-box) invertibile.*

Siano ora due s-box $S_1 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *ed* $S_2 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *e sia la funzione di round*

$$G_i(A||B||C) = B||C||A \oplus S_1(B) \oplus S_2(C) \oplus K_i$$

($||$ *indica la concatenazione,* $\oplus$ *lo* xor *binario bit-a-bit e* K_i *la chiave dell'i-esimo round).*

(1) Definire il corrispondente round di decifratura.
(2) Mostrare se è possibile esprimere lo stesso cifrario con un'unica sostituzione (come nel caso di cifrario di tipo Feistel standard) e in tal caso quale sia la sostituzione da effettuare e specificarne la funzione di round.

Esercizio 2. *(KeyExpansion/AES-SubBytes) Sia* $p(x) = x^3 + x + 1$ *si consideri la S-box di AES/Rijndael adattata opportunamente a 3 bit e che incorpora le operazioni sul campo finito* $\mathbb{F}_{2^3} = \mathbb{F}_2[x]/p(x)$.

Eseguire un round di cifratura di AES del blocco $X =$ `0x022002332211` *ponendo la chiave* $k =$ `0xDEADEC1DE` *(*`0x` *è la notazione per indicare il sistema di numerazione esadecimale):*

(1) 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. *Siano* h_1 *ed* h_2 *due funzioni di hash di cui almeno una delle due è resistente alle collisioni.*

Stabilire quali delle seguenti costruzioni risultino resistenti alle collisioni dimostrandone la proprietà:

(1) $h(x) := h_1(x)||h_2(x)$
(2) $h(x) := h_1(h_2(x))||h_2(h_1(x))$
(3) $h(x) := h_1(h_2(x)||x)||h_2(h_1(x)||x)$