UNIVERSITÀ DEGLI STUDI "ROMA TRE"
CORSO DI STUDI IN MATEMATICA
IN450 - INFORMATICA 6
ALGORITMI PER LA CRITTOGRAFIA – A.A. 2014-2015

M. PEDICINI

ESONERO DEL 09/01/2015 – TEMPO 3H00

COGNOME _____ NOME _____ MATRICOLA _____

Esercizio 1. *(20pt) (KeyExpansion/AES-SubBytes)*

Sia $p(x) = x^4 + x^3 + 1$ si consideri la S-box di AES/Rijndael adattata opportunamente a 4 bit e che incorpora le operazioni sul campo finito $\mathbb{F}_{2^4} = \mathbb{F}_2[x]/p(x)$.

Eseguire un round di cifratura di AES del blocco $X =$ `0x0000023322111212` *ponendo la chiave $k =$* `0xF0D0DEADBEEFF00D` *(*`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 (nel seguito le funzioni SubBytes*,* ShiftRows*,* MixColumns *e* AddKey *sono quelle dell'algoritmo adattato);*
(2) Calcolare $S_1 =$ SubBytes(X);
(3) Calcolare $S_2 =$ ShiftRows(S_1);
(4) Calcolare $S_3 =$ MixColumns(S_2);
(5) Calcolare $S_4 =$ AddKey(S_3, Key_0) dove Key_0 è il primo elemento del KeySchedule *calcolato a partire dalla chiave k.*

Esercizio 2. *(18pt) (Hash Functions)*

L'attacco di Joux alle hash iterate consiste nella ricerca di una collisione in una hash function iterata:

(1) Ricordare che per una generica funzione di hash (con dominio ad n bit) nel ROM (Random Oracle Model) esiste un $(1/2, o(2^{n/2}))$-algoritmo randomizzato per la ricerca delle collisioni;
(2) Sia $H : \{0,1\}^* \to \{0,1\}^{2n}$ costruita utilizzando due funzioni di hash:

$$H(M) = F(M)||G(M)$$

dove

- *$F : \{0,1\}^* \to \{0,1\}^n$ funzione ideale nel ROM e*
- *$G : \{0,1\}^* \to \{0,1\}^n$ è ottenuta iterando una funzione di compressione $C : \{0,1\}^{n+t} \to \{0,1\}^n$ a partire da un vettore di inizializzazione*

$$\begin{cases} h_0 = IV \\ h_{i+1} = C(h_i, M_i) \end{cases}$$

e $G(M) = h_k$.

Si consideri il generico attacco alla funzione di compressione C e per ogni i si stabilisca la probabilità di trovare una coppia di messaggi $M_i^{(0)}$ ed $M_i^{(1)}$ tale che

$$C(h_i, M_{i+1}^{(0)}) = C(h_i, M_{i+1}^{(1)}) = h_{i+1}.$$

(3) dimostrare che ripetendo k volte la procedura al punto precedente, ognuno dei 2^k messaggi ottenuti concatenando gli $M_i^{(b)}$:

$$M_1^{(b_1)} || \dots || M_k^{(b_k)} \qquad \text{dove } b_i \in 0, 1$$

ha stesso hash;

(4) ponendo $k = n/2$ senza fare ipotesi su G calcolare la probabilità di trovare una collisione per H;

(5) dedurre dal punto precedente che la funzione di hash H ha una resistenza inferiore a quella prevista dal ROM per una generica funzione di hash.

Esercizio 3. *(7pt) (Linear Cryptanalysis)*
Calcolare la tabella di approssimazione lineare per la S-BOX $f : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ definita da:

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