Corso di Crittografia
Anno Accademico 2018-2019
Homework II
30 Aprile 2019

Si ricorda che:

- Gli esercizi si risolvono individualmente.
- Le soluzioni vanno scritte in LaTeXe inviate al docente, in formato `pdf`, all'indirizzo di posta elettronica `ugo.dallago@unibo.it`. Vi chiedo la cortesia di definire l'oggetto della mail come "`[Crittografia] Consegna Homework II`". Si invitano gli studenti ad utilizzare il template `http://www.cs.unibo.it/~dallago/CRI1819/Homework-template-1819.tex`.
- La scadenza per l'invio delle soluzioni è il 10 di Maggio alle ore 24.00 CET.

Esercizio 1.
Data una funzione pseudocasuale F e un polinomio a coefficienti naturali p, come potremmo, a partire da F, costruire un generatore pseudocasuale G^p_F con fattore di espansione p? Si descriva formalmente G^p_F e si dimostri che tale costruzione è effettivamente un generatore pseudocasuale con coefficiente di espansione p sotto l'ipotesi che F sia una funzione pseudocasuale.

Esercizio 2.
Data una funzione pseoducasuale F, si consideri il MAC $\Pi^2_F = (\mathit{Gen}, \mathit{Mac}, \mathit{Vrfy})$ in cui:

- Gen restituisce una stringa binaria casuale lunga n ogniqualvolta invocato su 1^n.
- Mac_k è definito per messaggi lunghi $2|k|-2$ e restituisce su input m, la stringa $F_k(0||m_0)||F_k(1||m_1)$, dove $m = m_0||m_1$, $|m_0| = |m_1| = |k| - 1$, mentre $||$ è l'operatore di concatenazione.
- Vrfy è definito nel modo naturale.

Si discuta della sicurezza di Π^2_F, sotto l'ipotesi che F sia effettivamente pseudocasuale.

Esercizio 3.
Si consideri il modello delle substitution permutation networks, e si supponga di modificarlo nel modo che segue: anziché iterare n volte un round, *ciascuno* dei quali composto dalle fasi di mixing, substitution (ovvero le cosiddette S-BOX) e permutation, applichiamo all'input n volte la fase di mixing, a cui seguono n substitution, alle quali seguono n permutation. Si discuta della sicurezza di questo modello alternativo.