Corso di Crittografia
Anno Accademico 2018-2019
Homework III
23 Maggio 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 III`". 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 2 di Giugno alle ore 24.00 CET.

Esercizio 1.
Si dimostri che dato un predicato hc esiste una funzione one-way f per la quale hc non è hardcore.

Esercizio 2.
Si dimostri che in qualunque gruppo abeliano $\mathbb{G}$ identità e elementi inversi non solo esistono, ma sono unici.

Esercizio 3.
Un protocollo tra A e B si dice essere *a due fasi* se è strutturato come segue: A, dopo aver eseguito dei calcoli, invia ad B un messaggio, dopo la ricezione del quale B esegue dei calcoli e invia ad A un messaggio. Un esempio di protocollo a due fasi è il protocollo di DH, mentre NS non è di questo tipo. Si mostri come da ogni protocollo a due fasi per lo scambio delle chiavi si può ottenere uno schema di codifica a chiave pubblica. Si dimostri che se il protocollo è sicuro contro attacchi passivi, lo schema è CPA sicuro.