Corso di Sicurezza e Crittografia
Anno Accademico 2010-2011
Homework III
17 Dicembre 2010

Si ricorda che:

- Gli esercizi vanno risolti individualmente.
- Le soluzioni vanno scritte in LaTeX e inviate al docente, seguendo le indicazioni presenti nella pagina web del corso[1].
- La scadenza per l'invio delle soluzioni è il 24 di Dicembre alle 24.00.

Esercizio 1.
Si supponga di avere a disposizione uno schema di codifica a chiave *pubblica* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ e si supponga che Π sia sicuro. Quale potrebbe essere un modo naturale per definire uno schema di codifica a chiave *privata* Ψ in modo da utilizzare le funzionalità messe a disposizione dagli algoritmi Gen, Enc e Dec? Di che proprietà gode Ψ?

Esercizio 2.
Si dimostri che per ogni schema di codifica asimmetrico che sia CPA-sicuro, la lunghezza di ogni crittogramma ottenuto cifrando un singolo bit deve essere asintoticamente più che logaritmica nel parametro di sicurezza. In altre parole deve valere che $|\mathsf{Enc}_{pk}(b)| = \omega(\log n)$ per ogni $b \in \{0,1\}$ ogniqualvolta $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$.

Esercizio 3.
Date le seguenti coppie di espressioni nel linguaggio della crittografia formale, si dica quali di esse sono equivalenti e perché:

- $(K_1, \{0\}_{K_1})$ e $(\{0\}_{K_1}, K_1)$;
- $(K_1, \{(0, \{1\}_{K_3})\}_{K_1})$ e $(K_1, \{(0, \{(1,0)\}_{K_2})\}_{K_1})$;
- $(\{0\}_{K_1}, (K_1, \{1\}_{K_2}))$ e $(\{0\}_{K_2}, (K_1, \{1\}_{K_1}))$.

[1] http://www.cs.unibo.it/~dallago/SEC1011