Corso di Crittografia

Prova in Itinere del 19 Novembre 2021

1. Definire formalmente il concetto di perfetta sicurezza.

2. Sia SE=(`KeyGen`,`Enc`,`Dec`) un cifrario simmetrico e siano $\mathcal{M}, \mathcal{K}, \mathcal{C}$ gli insiemi dei messaggi, delle chiavi e dei crittotesti, rispettivamente.

   Si considerino adesso i seguenti insiemi $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$ con n parametro pubblico. Supponiamo di voler cifrare un solo messaggio $m \in \mathcal{M}$, utilizzando una chiave (random) $k \in \mathcal{K}$, come segue

   $$C = (m \vee k)$$

   dove $\vee$ rappresenta l'operazione OR bit a bit (es. $1100 \vee 1001 = 1101$) E' tale sistema sicuro in senso perfetto? Giustificare la risposta fornita.

3. In classe, parlando del cifrario a blocchi AES, abbiamo discusso il campo di Galois GF(2^8). Abbiamo visto che, in tale insieme, ogni byte può essere rappresentato come un polinomio di grado (al più) 7. Ricordando che $m(x) = x^8 + x^4 + x^3 + x + 1$ è il polinomio irriducibile discusso a lezione, si calcoli la somma ed il prodotto dei seguenti due byte:

   $$x^7 + x^5 + x^3 + x + 1 \qquad x^6 + x^4 + x^3 + x$$

4. Definire formalmente il concetto di funzione pseudocasuale.

5. Sia $F : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ una funzione pseudocasuale. Vogliamo utilizzare F per costruire una funzione $G : \{0,1\}^k \times \{0,1\}^{2\ell} \to \{0,1\}^{2\ell}$, nel seguente modo (il simbolo $||$ denota l'operazione di concatenazione):

   $G_k(x)$
       Sia $x = x_1 || x_2$ $// \; |x_1| = |x_2| = \ell$
       $y \leftarrow F_k(x_1) \, || \, F_k(F_k(x_2))$
       return y

   Dimostrare formalmente che G non è una funzione pseudo-casuale.