Corso di Crittografia

Prova del 21 Gennaio 2022

1. Si definisca formalmente il concetto di indistinguibilità contro attacchi a messaggio scelto `ind-id-cpa` per cifrari basati sull'identità.

2. Si consideri la seguente variante del cifrario El Gamal.

   Algoritmo di Generazione della Chiave. L'algoritmo di generazione della chiave prende in input un parametro k e sceglie due primi q, p tali che $|q| = k$ e q divide $p-1$. Quindi procede come segue. Detto G un sottogruppo di $\mathbb{Z}_p^*$ di ordine q, pone $\mathcal{M} = \{1, \ldots, 100\}$ come spazio dei messaggi. Quindi sceglie un generatore g di G, sceglie (a caso secondo la distribuzione uniforme) $x_1, x_2 \in \{1, \ldots, q\}$ e pone $h_1 = g^{x_1} \bmod p, h_2 = g^{x_2} \bmod p$. Infine, restituisce $PK = (p, q, g, h_1, h_2, \mathcal{M})$ come chiave pubblica e $SK = (x_1, x_2)$ come chiave privata.

   Algoritmi di cifratura e decifratura

$\mathbf{Enc}(PK, m)$	$\mathbf{Dec}(SK, C_0, C_1, C_2)$
If $m \notin \mathcal{M}$ return $\perp$	$A \leftarrow C_0^{x_1} \bmod p$; $B \leftarrow C_0^{x_2} \bmod p$
$r, k \leftarrow_R \{1, \ldots, q\}$;	$Y_1 \leftarrow C_1/A \bmod p$
$C_0 \leftarrow g^r \bmod p$;	$Y_2 \leftarrow C_2/(B \cdot Y_1) \bmod p$
$C_1 \leftarrow h_1^r g^k \bmod p$;	$m = 0$
$C_2 \leftarrow h_2^r g^{k+m} \bmod p$	For $i = 1$ to 100 do
return (C_0, C_1, C_2)	if $(Y_2 = g^i \bmod p)$ $m \leftarrow i$;
	If $m \notin \mathcal{M}$ return $\perp$
	else return m

   Dimostrare che tale cifrario non è sicuro in senso ind-cca.

3. Definire formalmente il concetto di sicurezza (ovvero non falsificabilità relativamente ad attacchi a messaggio scelto) per schemi di firma digitale.

4. Si dimostri che il seguente schema di firma non è sicuro.

   Algoritmo di Generazione delle Chiavi. L'algoritmo prende in input un parametro k e sceglie un primo p tale che $|p| = k$. Si consideri, inoltre, un gruppo G ciclico avente ordine p. Sia g un generatore di G. L'algoritmo procede scegliendo $x \in \{1, \ldots, p-1\}$ (a caso) e ponendo $h = g^x$. La chiave pubblica è quindi $VK = (h, g, G, p)$, mentre la chiave privata è $SK = (x)$. Lo spazio dei messaggi è $\mathcal{M} = \mathbb{Z}_p$.

Algoritmi di firma e Verifica

Sign(SK, m)	**Verify**(VK, m, σ)
$r, k \leftarrow_R \mathbb{Z}_p^*$	Sia $\sigma = (R, r, s)$;
$R \leftarrow g^k$;	If $R^{s-rm} = h^r$ return 1
$s \leftarrow r(m + k^{-1}x) \bmod p$;	else return 0
return $\sigma = (R, r, s)$	

//Si noti che è possibile estrarre radici in G.

5. Si consideri il seguente problema computazionale, che chiameremo Linear-Diffie-Hellman (LDH), definito su un gruppo ciclico G avente ordine primo q. Sia g un generatore di G, definiamo il seguente esperimento

$$
\begin{array}{l}
\mathbf{Esp}^{\mathtt{LDH}}_{G,g}(\mathcal{B}) \\
\quad x, y, a, b \leftarrow_R \mathbb{Z}_q^*; \\
\quad g_1 \leftarrow g^x, g_2 \leftarrow g^y, h \leftarrow g^{xy}; \\
\quad A \leftarrow g_1^a, B \leftarrow g_2^b; \\
\quad y \leftarrow \mathcal{B}(g_1, g_2, h, A, B); \\
\quad \text{If } (y = h^{a+b}) \text{ return } 1 \text{ else return } 0
\end{array}
$$

Il vantaggio di $\mathcal{B}$ è definito come

$$\mathbf{Adv}^{\mathtt{LDH}}_{G,g} = \Pr\left[\mathbf{Esp}^{\mathtt{LDH}}_{G,g}(\mathcal{B}) = 1\right]$$

Si dimostri che, se esiste un avversario $\mathcal{A}$ capace di risolvere il problema computazionale Diffie-Hellman studiato a lezione, tale avversario può essere sfruttato per risolvere LDH in G.