Cifrario di ElGamal

Cifrario a chiave pubblica basato su logaritmo discreto (subesponenziale, stessa difficoltà di RSA).

Creazione delle chiavi

Simile al protocollo Diffie-Hellman:

- si sceglie p primo grande e un generatore g di $\mathbb{Z}/p\mathbb{Z}^*$;
- si sceglie a caso $x \in \{2, \dots, p-2\}$;
- si calcola $y = g^x \bmod p$

$$k_{\text{pub}} = (p, g, y) \qquad k_{\text{priv}} = x.$$

Cifratura

Messaggio $m < p$ (altrimenti cifratura a blocchi di $\log_2 p$ bit) come in RSA.

- si sceglie a caso $r \in \{2, \dots, p-2\}$;
- $c = g^r \bmod p$;
- $d = my^r \bmod p$;
- crittogramma (c, d).

Visto che r è casuale, c e d appaiono come valori casuali al crittoanalista.

Decifrazione

$$m = dc^{-x} \bmod p$$

c^{-1} esiste ed è unico perché siamo modulo un primo.

$$\begin{aligned} dc^{-x} &= my^r \cdot c^{-x} \bmod p \\ &= my^r \cdot (g^r)^{-x} \bmod p \\ &= m(g^x)^r \cdot g^{-rx} \bmod p \\ &= m \bmod p \\ &= m && m < p \end{aligned}$$

Attacchi

- man in the middle nello scambio di chiavi pubbliche – certificati digitali;
- calcolo di $x = \log_g y \bmod p$ – difficile;
- se si conosce (o trova con forza bruta) r, $m = dy^{-r} \bmod p$;
- se si riutilizza lo stesso r:

  $$\begin{aligned} m_1 &: (c = g^r \bmod p, d_1 = y^r m_1 \bmod p) \\ m_2 &: (c = g^r \bmod p, d_2 = y^r m_2 \bmod p) \end{aligned}$$

  se Eve conosce m_1, può calcolare $y^{-r} = m_1 d_1^{-1}$ e $m_2 = d_2 y^{-r}$.