Public-key Cryptography based on the DLP

An alternative to the RSA problem (which seemingly relies on the handness of factoring integers) is the discrete logarithm problem (DLP).

Definition 1 (Discrete Logarithm Problem (DLP))**.** *Let G a group and $g \in G$. The DLP is the problem of finding $x \in \mathbb{Z}$ such that $a = g^x$ given a and g.*

Remark. *The DLP is not hard in every group. For example, if $G = (\mathbb{R}_{>0}, x)$ and $a, g \in G$, then $x = \frac{\log(a)}{\log(g)}$ solves the DLP.*

Remark. *In all the serious proposals for DLP based cryptosystems, G is a finite group. Otherwise sketchy things may happen such as: as small a corresponds to a small x.*

The most widely used groups for DLP-based cryptosystems are:

(a) $G = (\mathbb{Z}/p\mathbb{Z})^*$ where p is a prime.

(b) The group of points of an elliptic curve over a finite field.

1 Diffie-Hellman key exchange protocol

The original motivatio for the use of the DLP in cryptography was the Diffie-Hellman protocol as shown in Figure 1. The public parameters are a group G and $g \in G$.

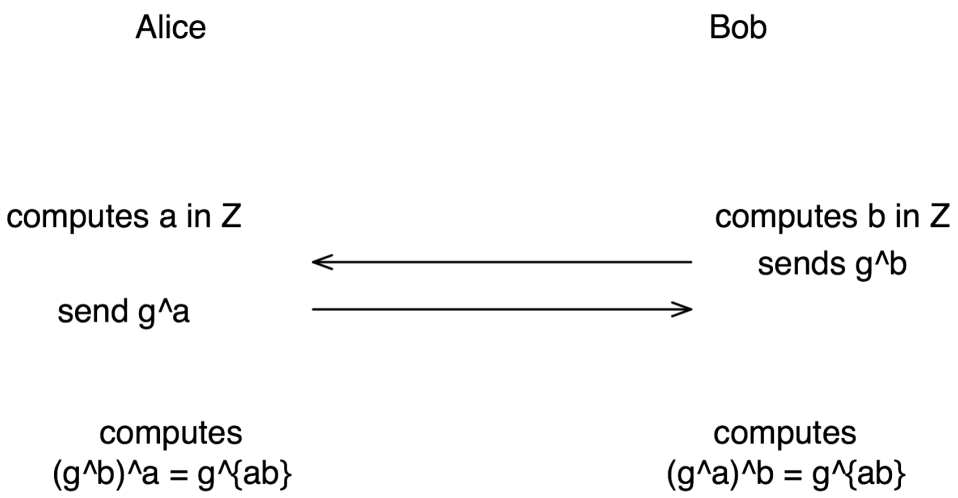
- Alice choses a secret $a \in \mathbb{Z}$.
- Bob chooses a secret $b \in \mathbb{Z}$.
- Alice sends g^a to Bob.
- Bob sends g^b to Alice.
- Alice computes $\left(g^b\right)^a = g^{ab}$.
- Bob computes $\left(g^a\right)^b = g^{ab}$.
- At the end, Alice and Bob share g^{ab}.

In the context of active attacks, there is one scenario that has to be mentioned: the "man-in-the-middle" attack.

- Eve talks to Alice pretending to be Bob.
- Eve talks to Bob pretending to be Alice.

At the end Eve has a shared secret with Alice and another shared secret with Bob. Eve can then pass messages from Alice to Bob (and read them).

Figure 1: The Diffie-Hellman key exchange protocol



2 El Gamal encryption scheme

Based on the same idea as the Diffie-Hellman protocol, we can derive a Public Key encryption scheme: the El Gamal cryptosystem.

- Public parameters: $G, g \in G, h \in < g >$.
- Private parameters : $x \in \mathbb{Z}$ such that $h = g^x$.
- Encryption: Choose $y \in \mathbb{Z}$, calculate g^y and $h^y = s$. Let $m \in G$, then $Enc(m, P_K) = (g^y, s, m) = c$.
- Decryption: Compute $(g^y)^x = s$. Recover $m = \frac{m \cdot s}{s}$.

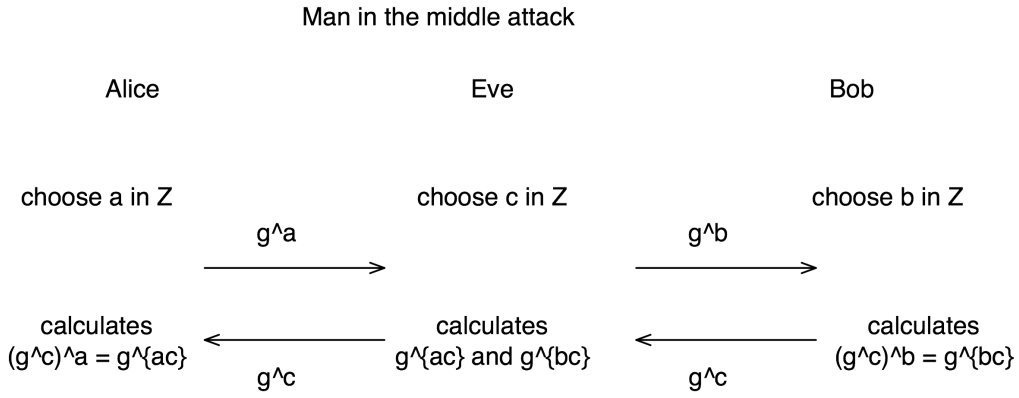
In the context of a passive adversary (i.e. a CPA attack), this "textbook El Gamal" is still secure (unlike RSA). However El Gamal without proper random padding on the message is not IND-CCA2 secure because just like "textbook RSA", it is malleable. If $c_0 = (g^{y_0}, s_0, m_0) = Enc(m_0, P_K)$, $c_1 = (g^{y_1}, s_1, m_1) = Enc(m_1, P_K)$, then $c_0 c_1 = (g^{y_0+y_1}, h^{y_0+y_1}, m_0 m_1) = Enc(m_0 m_1, P_K)$. Then the El Gamal scheme fails the IND-CCA2 security game just like RSA.

3 El Gamal signature scheme

Although the RSA signature scheme is the most widely used it is interesting to notice that El Gamal can also be used to sign messages. Here $G = (\mathbb{Z}/p\mathbb{Z})^*$. We assume that we have a public hash function H a public $g \in G$, public $h \in G$ and private $x \in \mathbb{Z}$ such that $h = g^x$.

Signature: Let m be a message and assume $H(m)$ is mapped on the integers.

Figure 2: The man-in-the-middle attack



- Choose $h \in \mathbb{Z}$.
- Compute $r = g^h$ and $s = (H(m) - xr)h^{-1} \mod p - 1$.
- Send (r, s) as the signature of m.

Verification

- Verify that $h^r \cdot r^s = g^{H(m)} \mod p$.

It is correct because:

$$\begin{aligned} h^r \cdot r^s &= g^{xr} \cdot g^{h(H(m)-xr)h^{-1}} \\ &= g^{xr} \cdot g^{-xr} \cdot g^{H(m)} \\ &= g^{H(m)} \end{aligned}$$

Figure 3: CPA against El Gamal

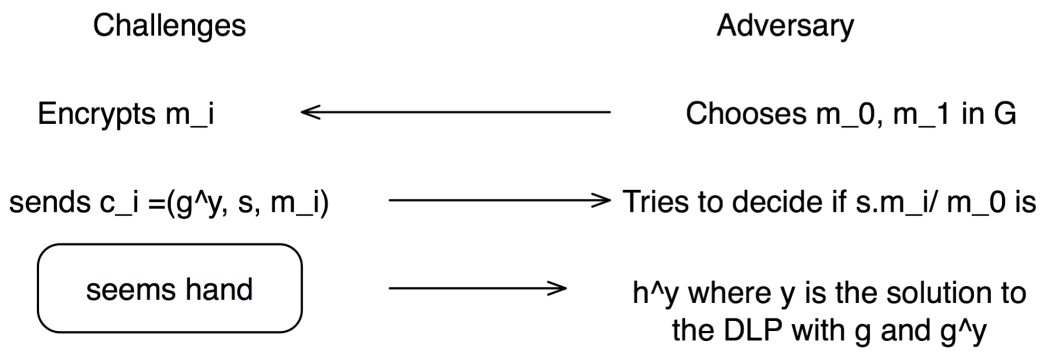


Figure 4: CCA against El Gamal