Sécurité des Systèmes d'Information
Exercise sheet 7 : Key Generation Protocols

11 December 2019

Non-mandatory exercise sheet. Please upload your answers on Moodle before Monday **16/12/2019 17h15**.

All answers should be carefully justified.

The Diffie-Hellman protocol

The Diffie-Hellman protocol is a key generation protocol that only requires a public channel :

- **Initialisation** : Choose a big prime number p and a generator $\alpha \in \mathbb{Z}_{p-1}$ in the multiplicative group $\mathbb{Z}_p^*$.
- **Key generation** :
  1. A chooses a secret number $x \in \mathbb{Z}_{p-1}$ and sends $\alpha^x \mod p$ to B.
  2. In the same way, B chooses a secret number $y \in \mathbb{Z}_{p-1}$, and sends $\alpha^y \mod p$.
  3. A and B can thus respectively compute $(\alpha^y)^x \mod p$ and $(\alpha^x)^y \mod p$ which will give them both the shared symmetric key $\alpha^{xy} \mod p$. A and B are the only one to share this secret.

Blom Key Predistribution Scheme

The simplest version of Blom's protocol works as follows :

- **Initialisation** :
  1. Generate a prime number p and an element $r_u \in \mathbb{Z}_p^*$ for each user u (all r_u's are different people). p and r_u's are public informations.

2. A Trusted Authority then chooses three random numbers $a, b, c \in \mathbb{Z}_p^*$, and computes $f(x, y) = (a + b(x + y) + cxy) \mod p$.
3. This Thrusted Authority then computes a polynomial for each user : $q_u(x) = f(x, r_u) \mod p$, and shares this polynomial only with user u through a secured channel.

- **Shared key computation** : Each pair of users (u,v) can then communicate with each other using a key they only share with one another : u computes $q_u(r_v)$, V computes $q_v(r_u)$, and these two values are both equal to K_{uv}.

Exercise 1 : General questions, Diffie-Hellman

- What is the difference between a KAP (Key Agreement Protocol) and a KTP (Key Transfer Protocol) ?
- In the two protocols (Diffie-Hellman, Blom) described above, which ones are KAP or KTP ?
- We use Diffie-Hellman protocol to generate keys. Let $p = 17$, $\alpha = 3$. A chooses $x = 5$, B chooses $y = 11$. Describe the exchange, what messages do they send to one another and what is the symmetric key they obtain ?
- What kind of attack is efficient against such protocol ? Explain why.

Exercice 2 : Blom's Scheme

- Show that u and v indeed compute the same key K_{uv}.
- Show that an attacker w (different from u and v) cannot find the key K_{uv} using only public informations from u and v. **Hint** : Write $q_w(x)$ as $a_w + b_w(x)$.
- Show that two attackers w and x working together, different from u and v, can find the key K_{uv}. **Hint** : Use the same trick as before to express $q_w(x)$ as $a_w + b_w(x)$, and do the same with $q_x(x)$.
- This protocole resists against a single attacker but not against two attackers. How would you modify it to make it resistant against k attackers but breakable by $k + 1$ attackers ?