
TD 6 – Key exchange

Exercise 1.*Insecure key exchange*

We consider the following key exchange protocol.

- 1 Alice samples k_A , $r \leftarrow \{0, 1\}^n$ and sends $s = k_A \oplus r$ to Bob.
 - 2 Bob samples $t \leftarrow \{0, 1\}^n$ and sends $u = s \oplus t$ to Alice.
 - 3 Alice computes $w = u \oplus r$ and sends w to Bob.
 - 4 Bob computes $k_B = w \oplus t$.
1. Prove that Alice and Bob share a common key $k_A = k_B$.
 2. Describe the transcript of the protocol.
 3. Prove that an adversary that has access to the transcript can compute the common key.

Exercise 2.*Discrete logarithms*

Let $G = \langle g \rangle$ be a multiplicative cyclic group of order n (that is, $\#G = n$), and $h \in G$.

1. Prove that $h^n = 1$. Use the discrete logarithm of h .
2. An *inverse* of h is an element ℓ such that $h \cdot \ell = \ell \cdot h = 1$.
 - i. Express the discrete logarithm of ℓ with respect to the discrete logarithm of h . Deduce the unicity of the inverse.
 - ii. Give a formula for ℓ that uses only h and n .
 - iii. Deduce an algorithm to compute ℓ from h and analyze its complexity in terms of the number of multiplications in G .
 - iv. Analyze the bit complexity of the algorithm when $G = (\mathbb{Z}/p\mathbb{Z})^\times$ for some prime number p .
3. The group $(\mathbb{Z}/29\mathbb{Z})^\times$ is generated by 2.
 - i. What is the order of $(\mathbb{Z}/29\mathbb{Z})^\times$. Describe a largest possible subgroup that has prime order.
 - ii. Compute the discrete logarithm (in base 2) of 17 in this group.

Exercise 3.*Random self-reducibility of the DLP*

Let $G = \langle g \rangle$ be a group of prime order p . We prove that given an algorithm that is able to compute the discrete logarithms of a constant fraction of the elements of G , we can build a (Las Vegas randomized) algorithm that computes the discrete logarithms of all the elements of G in the same (expected) time.

Let $h = g^t$ for some t , that we want to compute.

1. Let $r \in \{1, \dots, p-1\}$. Prove that given the discrete logarithm of h^r , one can compute the discrete logarithm of h .
2. Assume we sample $r \leftarrow \{1, \dots, p-1\}$. Prove that for all $x \in G$, $\Pr[h^r = x] = 1/p$. *Use discrete logarithms.*
3. Let $\mathcal{A}$ be a deterministic algorithm that takes as input an element $h \in G$ and either returns its discrete logarithm, or FAIL. Assume that the number of elements of which $\mathcal{A}$ returns the discrete logarithm is $\geq \alpha p$ for some $\alpha > 0$. Design an efficient Las Vegas algorithm that returns the discrete logarithm of any $h \in G$.