Exercise Sheet #6

Advanced Cryptography 2022

Exercise 1 A Special Discrete Logarithm

Let p be a prime and G be the set of all elements $x \in \mathbb{Z}_{p^2}$ satisfying $x \equiv 1 \pmod{p}$.

1. Show that G is a group with the multiplication of $\mathbb{Z}_{p^2}$.
2. Show that $|G| = p$.
3. Show that $L : G \to \mathbb{Z}_p$ defined by $L(x) = \frac{x-1}{p} \bmod p$ is a group isomorphism.
4. Show that $p+1$ is a generator of G and that the isomorphism L is the logarithm with respect to the basis $p+1$ in G. In other words, we have

$$(p+1)^{L(x)} \bmod p^2 = x$$

for any $x \in G$.

Exercise 2 Okamoto-Uchiyama Cryptosystem

Let p be a prime number and let G be the set of all $x \in \mathbb{Z}_{p^2}$ such that $x \equiv 1 \pmod{p}$. In the previous exercise, we have proven that G is a group with the multiplication of $\mathbb{Z}_{p^2}$, that $|G| = p$, that $L : G \to \mathbb{Z}_p$ defined by $L(x) = \frac{x-1}{p}$ is a group isomorphism, that $p+1$ is a generator of G, and that L is the logarithm with respect to the basis $p+1$ in G.

We now define the public-key cryptosystem of Okamoto-Uchiyama [1] which was proposed in 1998.

Key Generation: We first choose two large primes p and q greater than 2^k for some fixed k and we compute $n = p^2 q$. Then, we randomly choose $g \in \mathbb{Z}_n^*$ such that $g^{p-1} \pmod{p^2}$ has the multiplicative order of p. Finally, we compute $h = g^n \bmod n$. The public key is (n, g, h) and the secret key is (p, q).

Encryption: Let $m \in \mathbb{N}$ such that $0 < m < 2^{k-1}$ be a plaintext. Pick $r \in \mathbb{Z}_n^*$ uniformly at random. The ciphertext c is defined by

$$c = g^m h^r \bmod n.$$

[1] U. Okamoto and S. Uchiyama. A new public-key cryptosystem as secure as factoring. In K. Nyberg, editor, *Advances in Cryptology – EUROCRYPT'98: International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May/June 1998. Proceedings*, volume 1403 of *Lecture Notes in Computer Science*, pages 308–318. Springer-Verlag, 1998.

Decryption: One can recover the message m with

$$m = \frac{L(c^{p-1} \bmod p^2)}{L(g^{p-1} \bmod p^2)} \bmod p.$$

Show that the decryption is well defined, i.e., that $L(c^{p-1} \bmod p^2)$ and $L(g^{p-1} \bmod p^2)$ are two elements in $\mathbb{Z}_p$. Show that the decryption indeed recovers the original plaintext.

Exercise 3 Graph Colorability

Reminder: SAT is the language of all satisfiable boolean formulas. Informally, a boolean formula is defined as a tree in which every inner node is labeled by a boolean gate AND, OR, or NOT (the latter gate being on nodes with degree one only) and every leaf is labeled by a variable v_i. The formula is satisfiable if there exists an assignment of all variables to true or false such that the root node is evaluated to true. We assume that we have defined an efficient encoding rule over an alphabet in order to represent a Boolean formula.

A 3-SAT problem consists of finding a satisfiable boolean expression in 3-CNF (conjunctive normal form), which means that the problem input consists of formulae in conjunctive normal form (AND gates) with the limitation to a maximum of three literals per clause. A *literal* is either a variable or the negation of a variable (i.e. x_i or $\neg x_i$). *Clauses* here are disjunctions (OR gates) of literals (i.e. $(x_1 \vee x_2 \vee x_3)$).

Show by reduction that if the decision version of the 3-SAT problem has a polynomial time algorithm, then so does the decision problem of the 3-colorability of a graph.