

Solution Sheet #6

Advanced Cryptography 2022

Solution 1 A Special Discrete Logarithm

1. We show that $G = \{x \in \mathbb{Z}_{p^2} \mid x \equiv 1 \pmod{p}\}$ with the multiplication modulo p^2 is a group. Below, we prove the different conditions G should fulfill to be a group.

- **(Closure)** Let $a, b \in G$. By definition of G , we have $a \equiv b \equiv 1 \pmod{p}$. Hence, $ab \equiv 1 \pmod{p}$, which means that $ab \in G$.
- **(Associativity)** The associativity follows from the associativity of the multiplication in \mathbb{Z}_{p^2} .
- **(Neutral element)** The neutral element $e \in G$ has to satisfy $a \cdot e = e \cdot a = a$ for any $a \in G$. The element $1 \in G$ satisfies this property since it is the neutral element in \mathbb{Z}_{p^2} .
- **(Inverse element)** We have to show, that for any $a \in G$, there exists an element $b \in G$ such that $a \cdot b \equiv 1 \pmod{p}$. We can write $a = 1 + kp$ for an integer k such that $0 \leq k < p$. Similarly, we set $b = 1 + \ell p$ for an integer ℓ such that $0 \leq \ell < p$. From the equation

$$(1 + kp) \cdot (1 + \ell p) \equiv 1 + (k + \ell)p \pmod{p^2},$$

we deduce that b is the inverse of a if and only if $k + \ell \equiv 0 \pmod{p}$. Thus, each element $a = 1 + kp \in G$ has $b = 1 + (p - k)p$ as inverse.

Since the multiplication in \mathbb{Z}_{p^2} is commutative, note that G is commutative as well.

- Any element a of \mathbb{Z}_{p^2} can be written in the unique form $a = a_1 + a_2p$, where a_1 and a_2 are unique integers satisfying $0 \leq a_1, a_2 \leq p - 1$. We can conclude the proof by noticing that any element a of \mathbb{Z}_{p^2} lies in G if and only if the corresponding integer $a_1 = 1$.
- We show that $L : G \rightarrow \mathbb{Z}_p$ defined by $L(x) = \frac{x-1}{p} \pmod{p}$ is a group isomorphism.

- **(Homomorphism)** We first show that L is a group homomorphism. Let $a = 1 + kp$ with $0 \leq k < p$ and $b = 1 + \ell p$ with $0 \leq \ell < p$ be elements of G . We have

$$\begin{aligned} L(a \cdot b) &= L((1 + kp)(1 + \ell p) \pmod{p^2}) \\ &= L(1 + (k + \ell)p) \\ &= \frac{1 + (k + \ell)p - 1}{p} \pmod{p} \\ &= k + \ell \pmod{p} \end{aligned}$$

and

$$\begin{aligned} L(a) + L(b) &= \frac{1 + kp - 1}{p} + \frac{1 + \ell p - 1}{p} \pmod{p} \\ &= k + \ell \pmod{p}. \end{aligned}$$

- **(Injectivity)** Since L is an homomorphism, it suffices to show that its kernel contains only the neutral element. Let $a = 1 + kp$ with $0 \leq k < p$ such that $L(a) = 0$. This is equivalent to

$$\frac{1 + kp - 1}{p} = k = 0,$$

which shows that the kernel is trivial, i.e., is equal to $\{0\}$.

- **(Surjectivity)** The surjectivity simply follows from the injectivity, since the two sets G and \mathbb{Z}_p have the same finite cardinality.

4. We have to show that any element $a \in G$ can be written as a power of $p + 1$. Using the binomial theorem, we have

$$\begin{aligned} (p + 1)^n \pmod{p^2} &= \sum_{i=0}^n \binom{n}{i} p^i \pmod{p^2} \\ &= 1 + np. \end{aligned}$$

Thus, it is clear that $p + 1$ generates G . For $y \in G$,

$$y = \log_{p+1}(x) \iff x = (p + 1)^y \pmod{p^2}.$$

Since $(p + 1)^y \pmod{p^2} = 1 + py$, we finally obtain

$$y = \frac{x - 1}{p} \pmod{p} = L(x).$$

This logarithm function plays an important role for the Okamoto-Uchiyama cryptosystem¹. This cryptosystem is studied in the next exercise.

Solution 2 Okamoto-Uchiyama Cryptosystem

By Fermat's Little Theorem, we know that $g^{p-1} \equiv 1 \pmod{p}$ and that $c^{p-1} \equiv 1 \pmod{p}$. Therefore, $c^{p-1} \pmod{p^2} \in G$ and $g^{p-1} \pmod{p^2} \in G$, so that the decryption function is well defined.

Now, we show that the decryption works. First, we have

$$\begin{aligned} c^{p-1} \pmod{p^2} &\equiv (g^m h^r)^{p-1} \pmod{p^2} \\ &\equiv \left(g^m g^{p^2 q r} \right)^{p-1} \pmod{p^2} \\ &\equiv \left(g^{p(p-1)} \right)^{p q r} g^{m(p-1)} \pmod{p^2} \\ &\equiv 1 \cdot (g^{p-1})^m \pmod{p^2}. \end{aligned}$$

¹U. 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.

Thus, we have

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

Since, L is a group homomorphism, we deduce that

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

Thus,

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

which proves that the decryption function indeed recovers the original plaintext.

More details on the Okamoto-Uchiyama cryptosystem are given in the original article ².

Solution 3 Graph Colorability

We adopt some notations, as follows. Let $c_i = (c_i^1, c_i^2, c_i^3)$ denote the color of the node v_i , which is a 3-bit binary vector. We put the constraints

$$\begin{aligned} (c_i^1 c_i^2) \text{ OR } (c_i^1 c_i^3) \text{ OR } (c_i^2 c_i^3) &= 0 \\ c_i^1 \text{ OR } c_i^2 \text{ OR } c_i^3 &= 1 \end{aligned}$$

to describe that one and only one of the coordinate of c_i must equal one for each v_i . For each edge e_{ij} , we add the constraint

$$c_i^1 c_j^1 \text{ OR } c_i^2 c_j^2 \text{ OR } c_i^3 c_j^3 = 0$$

to describe that adjacent nodes must have different colors. Therefore, we can transform the above constraints into determining existence of a truth value of each literal such that the following expression is TRUE:

$$\begin{aligned} & (c_1^1 \text{ OR } c_1^2 \text{ OR } c_1^3) \text{ AND} \\ & (\neg c_1^1 \text{ OR } \neg c_1^2) \text{ AND } (\neg c_1^1 \text{ OR } \neg c_1^3) \text{ AND } (\neg c_1^2 \text{ OR } \neg c_1^3) \text{ AND} \\ & \vdots \\ & (c_n^1 \text{ OR } c_n^2 \text{ OR } c_n^3) \text{ AND} \\ & (\neg c_n^1 \text{ OR } \neg c_n^2) \text{ AND } (\neg c_n^1 \text{ OR } \neg c_n^3) \text{ AND } (\neg c_n^2 \text{ OR } \neg c_n^3) \text{ AND} \\ & \vdots \\ & (\neg c_i^1 \text{ OR } \neg c_j^1) \text{ AND } (\neg c_i^2 \text{ OR } \neg c_j^2) \text{ AND } (\neg c_i^3 \text{ OR } \neg c_j^3) \text{ AND} \\ & \vdots \end{aligned}$$

It is therefore easy to see 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.

²U. 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.