Nanjing University
Introduction to Cryptography
Fall 2023

Solution of Homework 5

1. A group of a prime order.

   Consider the set of squares modulo p, denoted as $\mathbb{G} = \{a^2 \mod p \mid a \in \mathbb{Z}_p^*\}$, where $\mathbb{Z}_p^*$ is the reduced residue group of p. To show $\mathbb{G}$ is a group, we need to verify the three group criteria:

   - **Closure:** For any $x, y \in \mathbb{G}$, xy must also be in $\mathbb{G}$.
     Let $x = a^2$ and $y = b^2$ for some $a, b \in \mathbb{Z}_p^*$. Then, $(ab)^2 = a^2b^2 \mod p$, which is also a square modulo p, and therefore $xy \in \mathbb{G}$.
   - **Identity:** $1^2 = 1 \mod p$, so the identity element is in $\mathbb{G}$.
   - **Inverse:** For any $x \in \mathbb{G}$, its inverse x^{-1} must also be in $\mathbb{G}$.
     If $x = a^2$, then $a^{-2} = (a^{-1})^2$ is the inverse of x, and a^{-1} is in $\mathbb{Z}_p^*$ because a is.

   The order of $\mathbb{G}$ is the number of distinct squares modulo p. Clearly, $x^2 = (-x)^2 \bmod p$. Furthermore, $x \neq -x \bmod p$. Therefore $|\mathbb{G}| = |\mathbb{Z}_p^*|/2 = q$.

   Hence, $\mathbb{G}$ is a group of order q.

2. Quadratic residue group.

   $\mathbb{G}$ is a group of prime order q, then $\mathbb{G}$ is cyclic by *COROLLARY 8.55*. Furthermore, all elements of $\mathbb{G}$ except the identity are generators of $\mathbb{G}$.

   Here, we provide a brief proof, for a detailed proof, please refer to *COROLLARY 8.55* in the textbook.

   For arbitrary $g \in \mathbb{G}$, consider the generated subgroup $\langle g \rangle$, and let $i \leq q$ be the smallest positive integer for which $g^i = 1$.

   $$\langle g \rangle \stackrel{\text{def}}{=} \{g^0, g^1, \cdots g^{i-1}\}.$$

   Because $q = |\mathbb{G}|$ and $g \in \mathbb{G}$, $g^q = 1$. Therefore, $i \mid q$. Since q is prime, $i = 1$ or $i = q$. Only the identity has order 1, and so all other elements have order q and generate $\mathbb{G}$.

3. Exercise 11.7.

   There appears to be a typo in the textbook where it states "$m \in \mathbb{Z}_q$" It should be "$m \in \mathbb{Z}_p$" instead.

   This scheme is not secure. In particular, consider an adversary $\mathcal{A}$ that gives $m_0 = 0$ and m_1 uniformly chosen from $\mathbb{Z}_p$ and then receives the challenge ciphertext $\langle c_1, c_2 \rangle$.

Observe that since $c_2 = h^y + m \bmod p$ it is not necessarily the case that $c_2 \in \mathbb{G}$ (since addition is not the group operation). However, when $b = 0$, it is guaranteed that c_2 is in $\mathbb{G}$.

The question remains as to the probability that c_2 is also in $\mathbb{G}$ when $b = 1$. As we know, $\mathbb{G}$ includes exactly half of the elements of $\mathbb{Z}_p^*$. Since m_1 is a random value, it follows that $c_2 \in \mathbb{G}$ with probability only $1/2$ when $b = 1$.

Thus, $\mathcal{A}$'s strategy is to check if $c_2 \in \mathbb{G}$. If so, then $\mathcal{A}$ outputs $b' = 0$. Otherwise, it outputs $b' = 1$.

The probability of success is $1/2 + 1/2 \cdot 1/2 = 3/4$, which is non-negligible. Therefore, the scheme is not CPA-secure.

For a more detailed answer, please refer to the discussion on Adversary for attack on one variant of elgamal.

4. Computing by hand.

   (a) To find the greatest common divisor of 589 and 722, we can use the Euclidean algorithm. Therefore, the greatest common divisor of 589 and 722 is 19.

   (b) The decryption exponent $d = e^{-1} \bmod \phi(N) = 31^{-1} \bmod 60$. Using the extended Euclidean algorithm to solve $31x + 60y = 1$, where $x = 31$. Therefore the decryption exponent $d = 31$. The ciphertext $c = m^e \bmod N = 4^{31} \bmod 77 \leftrightarrow ([4^{31} \bmod 11], [4^{31} \bmod 7]) = ([4 \bmod 11], [4 \bmod 7]) \leftrightarrow 4 \bmod 77$.

5. Exercise 11.20.

   Let $\gamma \overset{\text{def}}{=} [2^{-1} \bmod N]$. The intuition is that $x^e \cdot \gamma^e = (x\gamma)^e \bmod N$; thus, multiplication by γ^e can be used to effect a bitwise right-shift, which can in turn be used to learn all the bits of x one-by-one.

   For a more detailed answer, please refer to the solution on this link.

Algorithm 1: GetBits

Data: $\langle N, e \rangle$; $c \in \mathbb{Z}_N^*$; ℓ
Result: the ℓ least significant bits of $[c^{1/e} \bmod N]$
if $\ell = 1$ **then**
  return $\mathcal{A}(N, e, c)$
else
  $\gamma := [2^{-1} \bmod N]$
  $x_0 := \mathcal{A}(N, e, c)$
  $x' := \mathit{GetBits}(N, e, [c \cdot \gamma^e \bmod N], \ell - 1)$
  if $x_0 = 0$ **then**
    return $x' || x_0$
  else
    return $2x' - N \bmod 2^\ell$

When $\mathbf{lsb}(x) = 0$ then $[\gamma \cdot x \bmod N]$ is indeed just a right-shift of x (since x, viewed as an integer, is divisible by 2). But when $\mathbf{lsb}(x) = 1$, then $[\gamma \cdot x \bmod N] = \frac{x+N}{2}$.(Note that N is odd.) We take this into account in Algorithm 1, which is described recursively.

The algorithm relies on the assumed algorithm $\mathcal{A}$ for computing $\mathbf{lsb}(x)$. When called with $\ell = ||N||$ it returns all the bits of $x = [c^{1/e} \bmod N]$.

6. Security of signature schemes.

   (a) The modified signature scheme remains secure. If the adversary $\mathcal{A}$ can forge a valid (message, signature) pair (m, σ) for the modified scheme with a probability of $\epsilon(n)$, then another adversary $\mathcal{A}'$ can compromise the security of the original signature scheme with $\mathcal{A}$. This can be achieved by randomly selecting a prefix *pre* from $\{0,1\}^2$ and concatenating it with σ, $(m, pre||sigma)$ is a valid (message, signature) pair for the original scheme with a probability of $1/4 \cdot \epsilon(n)$.

   (b) The modified signature scheme remains secure. Because c is a constant, the number of possible permutations is also a constant. If the adversary $\mathcal{A}$ can forge a valid (message, signature) pair (m, σ) for the modified scheme with a probability of $\epsilon(n)$, then another adversary $\mathcal{A}'$ can compromise the security of the original signature scheme with $\mathcal{A}$. This can be achieved by randomly selecting a permutation π from the set of all possible permutations and applying π to σ, $(m, \pi(\sigma))$ is a valid (message, signature) pair for the original scheme with a probability of $1/c! \cdot \epsilon(n)$.