Introduction to Cryptography – LMAT2450
Practical Lesson 5

Clément Hoffmann (clement.hoffmann@uclouvain.be)
Yaobin Shen (yaobin.shen@uclouvain.be)

November 02, 2022

Reminder of basic facts about groups

1. The *order* of $\mathbb{G}$ is $|\mathbb{G}|$.
2. The *order* of an element $x \in \mathbb{G}$ the smallest i s.t. $x^i = 1$.
3. Fermat's little theorem: for commutative group $\mathbb{G}$ with $m = |\mathbb{G}|$, $x^m = 1$ for all $x \in \mathbb{G}$. Corollaries:
   - For all $x \in \mathbb{G}$, $x^i = x^{(i \mod m)}$.
   - For all $x \in \mathbb{G}$, $\text{ord}\,(x)$ divides m.
   - For all $x \in \mathbb{G}$, $x^{-1} = x^{m-1}$.
4. A group is *cyclic* if $\exists g \in \mathbb{G} : \mathbb{G} = \{g, g^2, g^3, \ldots, g^{|\mathbb{G}|}\}$, such a g is a *generator*.
5. If $\text{ord}\,(g) = |\mathbb{G}|$, then g is a generator of $|\mathbb{G}|$.
6. $\mathbb{Z}_p^*$ is the set of invertible integers modulo p.
7. If p is prime, $\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$.

Exercise 1 (Group order) In this exercise we consider the group $\mathbb{G} = \mathbb{Z}_{59}^*$.

1. What is the order of $\mathbb{G}$?
2. What is the order of 58?
3. What are the possible orders of an element of this group?
4. Find an element of order more than 20.
5. Is 2 generator?
   (Hint: $16^7 \mod 59 = 29$.*)*

Exercise 2 (Inverses in $\mathbb{Z}_n^*$)

1. Is 5 inversible in $\mathbb{Z}_{59}^*$? If yes, compute its inverse.
2. Is 42 inversible in $\mathbb{Z}_{135}^*$? If yes, compute its inverse.

Exercise 3 (Exponentiation in $\mathbb{Z}_{11}^*$)

1. Compute $2^5 \mod 11$ and $2^{2021} \mod 11$.
2. Show that 2 is a generator of $\mathbb{Z}_{11}^*$.
3. Compute $\frac{4}{7} \mod 11$.

Exercise 4 (Cyclic group)

1. List the elements of $\mathbb{G} = \mathbb{Z}_{18}^*$, then compute $|\mathbb{G}|$.
   (Hint: a is invertible mod N iff $\gcd(a, N) = 1$*.)*
2. Show that $\mathbb{G}$ is a cyclic group.

Exercise 5 ($\mathbb{Z}_p^*$ and QR_p) For a prime number p, we denote QR_p the set $\{x \in \mathbb{Z}_p^* | \exists a \in \mathbb{Z}_p^* : a^2 = x\}$, and such x are called quadratic residues modulo p. Let us show some properties of QR_p when p is odd (i.e., $p \neq 2$).

1. Show that if g is a generator of $\mathbb{Z}_p^*$, then $g \notin \mathrm{QR}_p$.
2. Show that if g is a generator of $\mathbb{Z}_p^*$, then for any integer i, $g^{2i} \in \mathrm{QR}_p$ and $g^{2i+1} \notin \mathrm{QR}_p$.
3. Show that QR_p is a cyclic group.
4. Give the order of QR_p.
5. Show that $x \in \mathrm{QR}_p$ has exactly two square roots in $\mathbb{Z}_p^*$.
   (Hint: observe that for any $x \in \mathbb{Z}_p^*$, $x \neq -x$ when p is an odd prime.)
6. Show that $x \in \mathrm{QR}_p \Leftrightarrow x^{\frac{p-1}{2}} = 1 \mod p$ and $x \notin \mathrm{QR}_p \Leftrightarrow x^{\frac{p-1}{2}} = -1 \mod p$.
7. Show that for any $x \in \mathbb{Z}_p^*$, any integers a, b, $x^{ab} \notin \mathrm{QR}_p$ iff $x^a \notin \mathrm{QR}_p$ and $x^b \notin \mathrm{QR}_p$.