Introduction to Modern Cryptography
Recitation 2

Orit Moskovich
Tel Aviv University
November 9, 2016

Based on chapter 7 in Introduction to Modern Cryptography, Katz-Lindell

Groups

Definition. A **group** is a non-empty set G with a binary operation $\circ$ if:

- Closure: For all $g, h \in G \Longrightarrow g \circ h \in G$
- Existence of an Identity: There exists an identity $e \in G$ such that for all $g \in G \Longrightarrow e \circ g = g = g \circ e$
- Existence of Inverses: For all $g \in G$ there exists an inverse $h \in G$ such that $g \circ h = e = h \circ g$
- Associativity: For all $g_1, g_2, g_3 \in G \Longrightarrow (g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$

- $|G|$ denote the order G, if it has a finite number of elements
- A group G with operation $\circ$ is abelian if the following holds:
  Commutativity: For all $g, h \in G \Longrightarrow g \circ h = h \circ g$

Sub-Groups

Definition. Let $(G,\circ)$ be a group. Then, $(H,\circ)$ is called a **sub-group** of $(\mathrm{G},\circ)$ if H itself is a group, and $H \subseteq G$

- The identity element in a group G is unique
  - usually denoted by 0 or 1
- Each element g of a group has a unique inverse
  - usually denoted by $-g$ or g^{-1}

Sub-Groups

Definition. Let $(G,\circ)$ be a group. Then, $(H,\circ)$ is called a **sub-group** of $(\mathrm{G},\circ)$ if H itself is a group, and $H \subseteq G$

- The identity element in a group G is unique
  - usually denoted by 0 or 1
- Each element g of a group has a unique inverse
  - usually denoted by $-g$ or g^{-1}

Additive notation:
$g + h$

Sub-Groups

Definition. Let $(G,\circ)$ be a group. Then, $(H,\circ)$ is called a **sub-group** of $(\mathrm{G},\circ)$ if H itself is a group, and $H \subseteq G$

- The identity element in a group G is unique
  - usually denoted by 0 or 1
- Each element g of a group has a unique inverse
  - usually denoted by $-g$ or g^{-1}

Multiplicative notation:
$g \cdot h$

The group: $\mathbb{Z}_N$

- Let $N \geq 2$ be an integer
- The set $\{0, \dots, N-1\}$ with respect to addition modulo N is an abelian group of order N
  - Identity: 0
  - Inverse of a is $N - a \; mod \; N$

Group Exponentiation

- The group operation applied $m \geq 0$ times to a fixed group element g

- Additive notation:
  - $m \cdot g = mg = \underbrace{g + g + \cdots + g}_{m \text{ times}}$

    NOT group operation

- Multiplicative notation:
  - $g^m = \underbrace{g \cdot g \cdot \ldots \cdot g}_{m \text{ times}}$

Group Exponentiation

Theorem. Let G be a finite group of order $m = |G|$. Then for any element

$$g \in G \Longrightarrow g^m = 1$$

The group: $\mathbb{Z}_N^*$

- $\mathbb{Z}_N = \{0, \ldots, N-1\}$ is a group under addition modulo N
- What about **multiplication** modulo N?
  - 1 will be the identity
  - 0 has no multiplicative inverse
  - Moreover, if $N = 6$, then 3 is not invertible modulo N

Theorem. Let a, N be integers, with $N > 1$.
Then a is invertible modulo $N \Leftrightarrow \gcd(a, N) = 1$

The group: $\mathbb{Z}_N^*$

- Let $N \geq 2$ be an integer
- The set $\mathbb{Z}_N^* = \{a \in \{1, \dots, N-1\} \mid \gcd(a, N) = 1\}$ with respect to multiplication modulo N is an abelian group
  - Identity: 1
  - Inverse of a exists
  - Closure?

Euler ϕ function

- Define the order of the group: $\phi(N) = |\mathbb{Z}_N^*|$

- $\phi(N) = ?$
  - $N = p$ prime ➔ $\phi(p) = p - 1$
  - $N = pq$ where $p \neq q$ primes ➔ $\phi(p) = (p-1)(q-1)$

Theorem. Let $N = \prod_i p_i^{e_i}$, where p_i's are distinct primes and $e_i \geq 1$.
Then $\phi(N) = \prod_i p_i^{e_i - 1} \cdot (p_i - 1)$

The group: $\mathbb{Z}_N^*$

- Let $N \geq 2$ be an integer
- The set $\mathbb{Z}_N^* = \{a \in \{1, \dots, N-1\} \mid \gcd(a, N) = 1\}$ with respect to multiplication modulo N is an abelian group of order $\phi(N)$

Corollary. Let $N > 1$ and $a \in \mathbb{Z}_N^*$. Then

$$a^{\phi(N)} = 1 \, mod \, N$$

If $N = p$ prime and $a \in \mathbb{Z}_N^* = \{1, \dots, p-1\}$. Then

$$a^{p-1} = 1 \, mod \, p$$

Cyclic Groups and Generators

- Let G be a finite group of order $|G| = m$
- For arbitrary $g \in G$ define $\langle g \rangle = \{g^0, g^1, g^2, \dots\}$
- Why is $\langle g \rangle$ a finite set?
- $\langle g \rangle$ is actually a subgroup of G for any $g \in G$

Definition. Let G be a finite group and $g \in G$. The **order** of g is the smallest positive integer i such that $g^i = 1$

Cyclic Groups and Generators

- $\langle 1 \rangle = \{1\}$
- What if there exists $g \in G$ of order m (where $|G| = m$)?
  - $\langle g \rangle = G$

Definition. Let G be a finite group of order $|G| = m$.
If there exist an element $g \in G$ of order m, then
G is called a **cyclic group** and g is a **generator** of $G = \{g^0, g^1, \dots, g^{m-1}\}$.

- If g is a generator of G, then for every element $h \in G$ there exist $x \in \{0, \dots, m-1\}$ such that $h = g^x$

Cyclic Groups and Generators

Theorem. Let G be a finite group of order m, and $\mathrm{g} \in \mathrm{G}$ has order i. Then $i|m$

Corollary. If G is a group of prime order p, then G is cyclic and all elements (except 1) are generators

This is not $\mathbb{Z}_p^* = \{1, \dots, \mathrm{p}-1\}$!
$\left|\mathbb{Z}_p^*\right| = p - 1$ not prime!

Cyclic Groups and Generators

Theorem. If p is prime, then $\mathbb{Z}_p^*$ is cyclic

Sage

- https://cloud.sagemath.com/
  - Create new project → Start project → New terminal → Sage
- https://doc.sagemath.org/html/en/tutorial/


OH ALICE... YOU'RE THE ONE FOR ME
BUT BOB... IN A QUANTUM WORLD HOW CAN WE BE SURE?
ψ^+ or ψ^- ?