# Crypto math II

Alin Tomescu
alinush@mit.edu

May 19, 2015

**Abstract**

A quick overview on group theory from Ron Rivest's 6.857 course in Spring 2015.

## 1 Overview

- Group theory review
- Diffie-Hellman (DH) key exchane
- Five crypto groups:
  - $\mathbb{Z}_p^*$
  - $\mathbb{Q}_n$
  - $\mathbb{Z}_n^*$
  - $\mathbb{Q}_n$
  - elliptic curves

## 2 Group theory review

Here, we are talking about multiplicative groups (where the operation between group elements is something *resembling* multiplication)

**Definition:** $(\mathbb{G}, \cdot)$ is a *finite abelian group* of size $t$ if:

- $\exists$ identity 1 such that $\forall a \in \mathbb{G}, a \cdot 1 = 1 \cdot a = a$
- $\forall a \in \mathbb{G}, \exists b \in \mathbb{G}$ such that $a \cdot b = 1$
- $\forall a, b, c \in \mathbb{G}, a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- $\forall a, b \in \mathbb{G}, a \cdot b = b \cdot a$

## 2.1 Order and generators

**Definition:** The *order* of $a$ in $\mathbb{G}$ is denoted by $order(a)$ and is equal to the least $u$ such that $a^u = 1$

**Lagrange's Theorem:** In a finite abelian group of size $t$, for all $a \in \mathbb{G}$, $order(a) \mid t$

**Theorem:** In a finite abelian group of size $t$, $\forall a \in \mathbb{G}, a^t = 1$

*Example:* $a^{(p-1)} = 1, \forall a \in \mathbb{Z}_p^*$ because $|\mathbb{Z}_p^*| = 1$

**Definition:** $\langle a \rangle = \{a^i : i \geqslant 0\}$ = subgroup generated by $a$.

**Definition:** If $\langle a \rangle = \mathbb{G}$ then $\mathbb{G}$ is *cyclic* and $a$ is a *generator* of $\mathbb{G}$.

*Note:* $|\langle a \rangle| = order(a)$

*Exercise:* In a finite abelian group $\mathbb{G}$ of order $t$, where $t$ is prime, we have: $\forall a \in \mathbb{G}$, if $a \neq 1 \Rightarrow a$ is a generator of $\mathbb{G}$.

*Solution:* We know that the size of any subgroup of $\mathbb{G}$ must divide $t$. Since $t$ is prime, any subgroup can either have size 1 or $t$. Thus, only trivial subgroups can exist: the subgroup made up of the identity element ($\{1\}$) and $\mathbb{G}$ itself. Since $a \neq 1$, any subgroup generated by $a$ cannot be equal to $\{1\}$ because it will have to contain $a$ itself which is different than 1. Thus, if $a$ generates any subgroup, it has to generate $\mathbb{G}$ itself. How do we know that $a$ generates any subgroup at all then? We know $a \in G \Rightarrow a^u \in G, \forall u$ and, informally, we know that there cannot be a $u, 1 < u < t$ such that $a^u = 1$ because that would create a subgroup of $\mathbb{G}$ of size $u$, which would imply $u \mid t$, which would be false since $t$ is prime.

**Theorem:** $\mathbb{Z}_p^*$ is always cyclic (i.e. there exists a generator within $\mathbb{Z}_p^*$)

## 2.2 Discrete logs

**Theorem:** If $\mathbb{G}$ is a cyclic group of order $t$ and generator $g$ then the relation $x \leftrightarrow g^x$ is one-to-one between $[0, 1, \ldots, t-1]$ and $\mathbb{G}$.

$$x \mapsto g^x : \text{exponentiation, "powering-up"}$$
$$g^x \mapsto x : \text{discrete logarithm (DL)}$$

Computing *discrete logarithms* (the DL problem) is commonly assumed to be hard/infeasible for well-chosen groups $\mathbb{G}$ (e.g. $\mathbb{Z}_p^*$ for $p$ a large randomly chosen prime).

In practice, we need to be able to translate *bits of data* or *messages* from a message space $M$ as group elements of $\mathbb{G}$. We need an one-to-one correspondence (injective, and surjective) function $f : M \rightarrow \mathbb{G}$ such that $f(m) \in \mathbb{G}$ can be chosen to represent message $m \in M$.