Lecture 1:
Course Introduction

Thomas Johansson

Course intro - Mathematical Cryptology

- Welcome to Mathematical cryptology (EDI075)!
- Everything in English.
- **Course information:**
  - 4 weeks work, 6hp.
  - Lectures L1-L12 (Tuesdays 8.15-10, Thursdays 13.15-15, in E:3139)
  - Hand-in exercises (6 "weeks", one sheet available for each week), include two small projects, exercise hours if needed.
  - Exam, written (time to be decided)
- **Course book:** Nigel Smart's Cryptography: An Introduction, third edition, available online only
- Everything is to be found on the course web page!

Chapter 1: Modular Arithmetic, Groups, Finite Fields and Probability

- 1. Modular Arithmetic (Groups, Rings, Finite Fields)
- 2. Finite Fields
- 3. Basic Algorithms (Euklidean, CRT,...

Chinese Remainder Theorem (CRT).

- CRT: if we have the two equations

$$x = a \bmod N \text{ and } x = b \bmod M$$

  then there is a unique solution modulo $M \cdot N$ if and only if $\gcd(N, M) = 1$.
- $\mathbb{Z}_n$ isomorphic to $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \mathbb{Z}_{n_k}$ if $n = n_1 n_2 \cdots n_k$ and $\gcd(n_i, n_j) = 1$, $i \neq j$.

3.3. Legendre and Jacobi Symbols.

- Look at the map
$$x \mapsto x^2$$
in $\mathbb{F}_p$.
- This mapping is exactly two-to-one on the non-zero elements of $\mathbb{F}_p$.
- if an element x in $\mathbb{F}_p$ has a square root, then it has exactly two square roots (unless $x = 0$).
- The set of squares in $\mathbb{F}_p$ = *the quadratic residues* and they form a subgroup of order $(p-1)/2$ of the multiplicative group $\mathbb{F}_p$.
- The elements of $\mathbb{F}_p$ which are not squares = *the quadratic non-residues*.

The Legendre symbol

- To make it easy to detect squares modulo p we define the *Legendre symbol* $\left(\frac{a}{p}\right)$ as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue} \pmod{p} \\ -1 & \text{if } a \text{ is a quadratic nonresidue} \pmod{p} \\ 0 & \text{if } p \text{ divides } a \end{cases}$$

- It is easy to compute the Legendre symbol, for example via

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}.$$

The Legendre symbol

- Using the above formula turns out to be very inefficient.
- *The law of quadratic reciprocity* (p, q primes)

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{(p-1)(q-1)/4}$$

- Famous result, no proof given here.

More

The following additional formulae gives rise to a recursive algorithm

- $\left(\frac{q}{p}\right) = \left(\frac{q \bmod p}{p}\right)$
- $\left(\frac{q \cdot r}{p}\right) = \left(\frac{q}{p}\right) \cdot \left(\frac{r}{p}\right)$
- $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

Requires factoring...

Computing square roots of elements in $\mathbb{F}_p$

- ShanksŠ Algorithm, computing the square root of a modulo p, when such a square root exists. Easy and quick!
- When $p = 3 \bmod 4$, we can use the following formulae

$$x = a^{(p+1)/4} \bmod p,$$

which has the advantage of being deterministic and more efficient.

The Jacobi symbol

- to be completed

The Birthday paradox

- to be completed