EE 720: An Introduction to Number Theory and Cryptography (Spring 2018)

Lecture 19 — March 27, 2018

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Chinese Remainder Theorem
- Discrete Logarithm Problem
- Diffie-Hellman Protocol

2 Recap

- **Chinese Remainder Theorem:** Let $N = pq$ where p, q are integers greater than 1 which are relatively prime, i.e. $\gcd(p, q) = 1$. Then

$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q \text{ and } \mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*.$$

  Moreover, the function $f : \mathbb{Z}_N \mapsto \mathbb{Z}_p \times \mathbb{Z}_q$ defined by

$$f(x) = (x \bmod p, x \bmod q)$$

  is an isomorphism from $\mathbb{Z}_N$ to $\mathbb{Z}_p \times \mathbb{Z}_q$, and the restriction of f to $\mathbb{Z}_N^*$ is an isomorphism from $\mathbb{Z}_N^*$ to $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

- Example: $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. This group is isomorphic to $\mathbb{Z}_3^* \times \mathbb{Z}_5^*$.
- An extension of the Chinese remainder theorem says that if $m_1, m_2 \ldots, m_l$ are pairwise relatively prime (i.e., $\gcd(m_i, m_j) = 1$ for all $i \neq j$) and $N = \Pi_{i=1}^{l} m_i$, then

$$\mathbb{Z}_N \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_l} \text{ and } \mathbb{Z}_N^* \simeq \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \cdots \times \mathbb{Z}_{m_l}^*.$$

- Usage
  - Compute $14 \cdot 13 \bmod 15$
  - Compute $11^{53} \bmod 15$
  - Compute $18^{25} \bmod 35$

3 Chinese Remainder Theorem (continued)

- How to go from $(x_p, x_q) = (x \bmod p, x \bmod q)$ to $x \bmod N$ where $\gcd(p, q) = 1$?
  - Compute X, Y such that $Xp + Yq = 1$.

- Set $1_p \coloneqq Yq \bmod N$ and $1_q \coloneqq Xp \bmod N$.
- Compute $x \coloneqq x_p \cdot 1_p + x_q \cdot 1_q \bmod N$.

- Example: $p = 5, q = 7$ and $N = 35$. What does $(4, 3)$ correspond to?

- Let $m_1, m_2, \ldots, m_l$ be pairwise relatively prime positive integers. Then the unique solution modulo $M = m_1 m_2 \cdots m_l$ of the system of congruences

$$\begin{aligned} x &= a_1 \bmod m_1 \\ x &= a_2 \bmod m_2 \\ &\vdots \\ x &= a_l \bmod m_l \end{aligned}$$

  is given by

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_l M_l y_l$$

  where $M_i = \frac{M}{m_i}$ and $M_i y_i = 1 \bmod m_i$.

- Example: Solve for x modulo 105 which satisfied the following congruences.

$$\begin{aligned} x &= 1 \bmod 3 \\ x &= 2 \bmod 5 \\ x &= 3 \bmod 7 \end{aligned}$$

4 Discrete Logarithms in Cyclic Groups

- **Definition:** If G is a cyclic group of order q with generator g, then for $h \in G$ the unique $x \in \mathbb{Z}_q$ which satisfies $g^x = h$ is called the discrete logarithm of h with respect to g.

- The discrete logarithm problem is believed to be hard in cyclic groups of prime order. A subgroup of $\mathbb{Z}_p^*$ having prime order q is a good choice.

5 Diffie-Hellman Protocol

- How do parties which use private-key cryptographic schemes share a secret key in the first place?

- One solution is to have a trusted party act as the key distribution center. But this center is a single point of failure. The DH protocol presents an alternative.

- **The Diffie-Hellman key-exchange protocol:**

  1. Alice runs a group generation algorithm to get (G, q, g) where G is a cyclic group of order q with generator g.
  2. Alice chooses a uniform $x \in \mathbb{Z}_q$ and computes $h_A = g^x$.
  3. Alice sends (G, q, g, h_A) to Bob.

4. Bob chooses a uniform $y \in \mathbb{Z}_q$ and computes $h_B = g^y$. He sends h_B to Alice. He also computes $k_B = h_A^y$.
5. Alice computes $k_A = h_B^x$.

By construction, $k_A = k_B$.

6 References and Additional Reading

- Sections 8.1.5, 8.3.2 from Katz/Lindell
- Sections 10.1,10.2,10.3 from Katz/Lindell