Chapter 5: RSA and Factorization

Math 495, Fall 2008

Hope College

October 15, 2008

Public-key Cryptography

- So far, we have studied cryptosystems in which a secret key K is chosen, and then the decryption function d_K is easy to compute by knowing K.
- This requires secret communication of the key from Alice to Bob, which might be difficult or impractical.
- In **public-key cryptography**, the full details of the encryption function e_K can be known publicly. The cryptosystem is designed so that it is computationally infeasible to determine d_K from e_K without additional information.

- An injective function $f : \mathcal{P} \to \mathcal{C}$ is called a **one-way function** if it is easy to compute $f(x)$ for all x, but, given y it is hard to find x such that $f(x) = y$.
- For public-key cryptography, we need the encryption function e_K to be a a one-way function with a trapdoor.
- A **trapdoor** consists of secret information that makes inversion of a one-way function easy.
- Thus, what is needed for public-key cryptography is a **trapdoor one-way function.**

Facts about $\mathbb{Z}_n$

- For a positive integer n, $\phi(n)$ is defined as the number of integers in $\{0, 1, 2, \ldots, n-1\}$ that are relatively prime to n.
- An element $a \in \mathbb{Z}_n$ is invertible under multiplication if and only if $\gcd(a, n) = 1$.
- Let
$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \ : \ a^{-1} \text{ exists in } \mathbb{Z}^n\}.$$
Then $\mathbb{Z}_n^*$ is a group under multiplication, and $|\mathbb{Z}_n^*| = \phi(n)$.

More about $\phi(n)$

- If p is prime, then $\phi(p) = p - 1$.
- If p is prime and $e \geq 2$, then $\phi(p^e) = p \cdot \phi(p^{e-1}$.
- If p is prime and $e \geq 1$, then $\phi(p^e) = p^e - p^{e-1}$.
- If p and q are relatively prime, then $\phi(pq) = \phi(p)\phi(q)$.
- If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is a prime factorization,

$$\phi(n) = \prod_{i=1}^{k} (p_i^{e_i} - p_i^{e_i - 1}).$$

Euclidean Algorithm

- The Euclidean Algorithm solves two problems:
  - Given positive integers a and b, find $\gcd(a, b)$.
  - Given positive integers b and n with $\gcd(b, n) = 1$, find b^{-1} in $\mathbb{Z}_n$.
- We will do two examples on the board in class:
  - Compute $\gcd(70, 26)$.
  - Find 19^{-1} in $\mathbb{Z}_{26}$.

Chinese Remainder Theorem

- The Chinese Remainder Theorem states that, if $m_1, \ldots, m_r$ are pairwise relatively prime positive integers and $a_1, \ldots, a_r$ are any positive integers, then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

  has a solution x that is unique modulo $M = m_1 m_2 \cdots m_r$.
- Another way of stating this result is to say that, if $m_1, \ldots, m_r$ are pairwise relatively prime positive integers, then the function $\chi : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ defined by

$$\chi(x) = (x \mod m_1, x \mod m_2, \ldots, x \mod m_r)$$

  is a bijection.

Proof of the Chinese Remainder Theorem

- Let $M = m_1 m_2 \ldots m_r$. Let $M_i = M/m_i$, and note that $\gcd(M_i, m_i) = 1$. Let $y_i = M_i^{-1} \mod m_i$.
- Let $X = \sum_{i=1}^{r} a_i M_i y_i \mod M$.
- Note that $X \equiv a_i \pmod{m_i}$ since $M_i y_i \equiv 1 \pmod{m_i}$ and $M_j \equiv 0 \pmod{m_j}$ for $j \neq i$.
- We can show that X is unique by counting elements of $\mathbb{Z}_M$ and $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$.

A Bit of Group Theory

- If G is a multiplicative group, the **order** of an element $g \in G$ is the minimum positive number m such that $g^m = 1$.
- Example: What is the order of 7 in $\mathbb{Z}_{20}^*$? Answer: 4.
- Theorem: (Lagrange) If G is a multiplicative group with n elements, then the order of any element of G divides n.
- Corollary: If $b \in \mathbb{Z}_n^*$, then $b^{\phi(n)} \equiv 1 \pmod{n}$.
- Corollary: Suppose p is prime and $b \in \mathbb{Z}_p$. Then $b^p \equiv b \pmod{p}$.
- Theorem: If p is prime, there is an element $\alpha \in \mathbb{Z}_p^*$ such that
$$\mathbb{Z}_p^* = \{\alpha^i \,:\, i \geq 0\}.$$
We say that $\mathbb{Z}_p^*$ is a **cyclic group** and α is a **primitive element** (or a **generator**).
- Theorem: Suppose $p > 2$ is prime and $\alpha \in \mathbb{Z}_p$. Then α is primitive if and only if $\alpha^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all primes q such that $q|(p-1)$.