Introduction to Cryptography

Ayelet Yablon and Daniela Yablon

May 19, 2022

Introduction to Number Theory

Modulo - Two numbers a and b are congruent to each other $\mod c$ if they leave the same remainder after dividing by c.

Modular Arithmetic

- If $x \equiv y \mod n$, then $ax \equiv ay \mod n$
- If a is coprime to a number n, and b is coprime to n, then ab is coprime to n
- If a number is coprime to a number n, then reducing it by n yields a number coprime to n

Introduction to Group Theory

A group is defined as a set of elements with a binary operation that satisfy the four group axioms.

Group Axioms

- Associativity - given three real numbers a, b, and c, $a \star (b \star c) = (a \star b) \star c$
- Closure - $a \in G$ and $b \in G$, $a \star b \in G$
- Identity Existence - given group G, there exists element $i \in G$ such that $a \star i = a$
- Inverse Existence - given group G, there exists element $e \in G$ such that $a \star e = i$

Euler's Totient Function

- $\varphi(n) = |Z_n^*| = |\{a : 1 \leq a \leq n, \gcd(a, n) = 1\}|$
- If $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ is a product of k primes, then the size of the group Z_n^* is $\varphi(n) = \varphi(p_1 \cdot p_2 \cdot \ldots \cdot p_k) = (p_1 - 1)(p_2 - 2) \ldots (p_k - 1)$
- If n is prime, then Z_p^* will contain the set of integers from 1 to $p - 1$

Euler's Totient Function

- $\varphi(n) = |Z_n^*| = |\{a : 1 \le a \le n, \gcd(a, n) = 1\}|$
- If $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ is a product of k primes, then the size of the group Z_n^* is $\varphi(n) = \varphi(p_1 \cdot p_2 \cdot \ldots \cdot p_k) = (p_1 - 1)(p_2 - 2) \ldots (p_k - 1)$
- If n is prime, then Z_p^* will contain the set of integers from 1 to $p - 1$

Euler's Theorem

For two positive integers x, n, such that x, n are relatively prime $x^{\varphi(n)} \equiv 1 \mod n$.

Proof

Modular Arithmetic

- If $x \equiv y \mod n$, then $ax \equiv ay \mod n$
- If a is coprime to a number n, and b is coprime to n, then ab is coprime to n
- If a number is coprime to a number n, then reducing it by n yields a number coprime to n

Proof

Modular Arithmetic

- If $x \equiv y \mod n$, then $ax \equiv ay \mod n$
- If a is coprime to a number n, and b is coprime to n, then ab is coprime to n
- If a number is coprime to a number n, then reducing it by n yields a number coprime to n

$A = \{a_1, a_2, ...a_\varphi\}$

Proof

Modular Arithmetic

- If $x \equiv y \mod n$, then $ax \equiv ay \mod n$
- If a is coprime to a number n, and b is coprime to n, then ab is coprime to n
- If a number is coprime to a number n, then reducing it by n yields a number coprime to n

$A = \{a_1, a_2, ...a_\varphi\}$
$B = \{x \cdot a_1, x \cdot a_2, ...x \cdot a_\varphi\}$

Proof

Modular Arithmetic

- If $x \equiv y \mod n$, then $ax \equiv ay \mod n$
- If a is coprime to a number n, and b is coprime to n, then ab is coprime to n
- If a number is coprime to a number n, then reducing it by n yields a number coprime to n

$$A = \{a_1, a_2, ...a_\varphi\}$$
$$B = \{x \cdot a_1, x \cdot a_2, ...x \cdot a_\varphi\}$$
$$C = \{x \cdot a_1 \pmod{n}, x \cdot a_2 \pmod{n}, ...x \cdot a_\varphi \pmod{n}\}$$

RSA - Keys

- Key - piece of information that can be used to decrypt a message
- Most encryption algorithms: n keys for someone to communicate with n people
- RSA: 1 key for someone to communicate with n people
- Public key - a key that can be accessed by the public
- Private key - a key that can be accessed only by the intended receiver of a message
- Public keys: (N, e)
- Private key: (d)

RSA - Algorithm

- Trapdoor function - modular arithmetic
- Encryption: $y \equiv x^e \mod (N)$
- Decryption: $x \equiv y^d \mod (N)$