CSL759: Cryptography and Computer Security

Ragesh Jaiswal

CSE, IIT Delhi

Course Project

Course Project

- Let me know your team (at most 2 students per project) and your project topic by tomorrow (12th Mar.).
- We will set up meetings this Wed-Fri and early next week with all the groups.
- There will be a Demo/Presentation at the end of the course.

Towards Public Key Cryptography

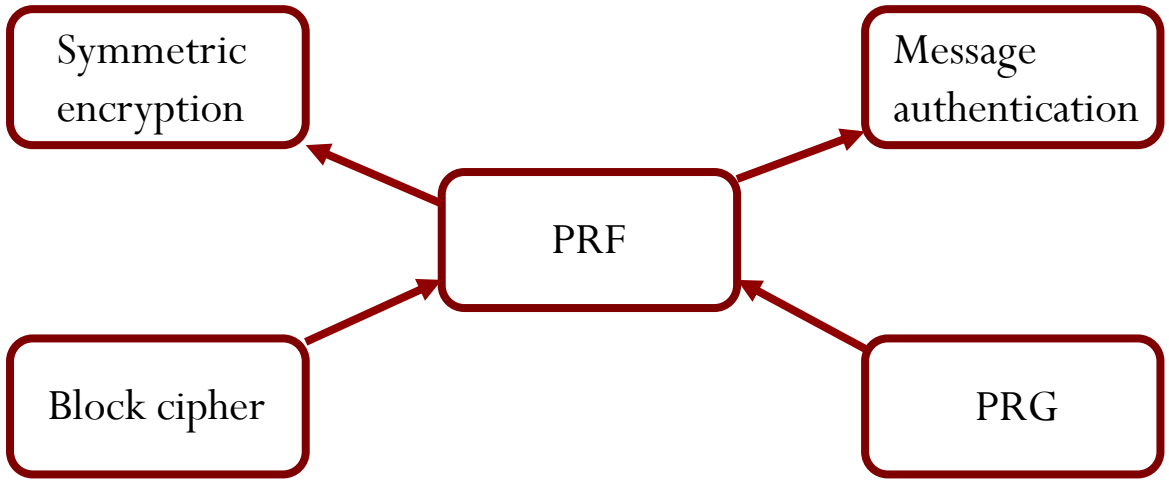
Number Theory

Towards Public Key Cryptography

- Until now, we have talked about *private key cryptography* where the interating parties are assumed to be sharing the same secret key.
- Public-key Cryptography:
  - Parties do not share a common secret key.
  - Each party has a pair of keys (pk, sk). One is public and other secret.
- The basic building blocks for private key cryptography:
  - Pseudorandom generator
  - Pseudorandom permutation

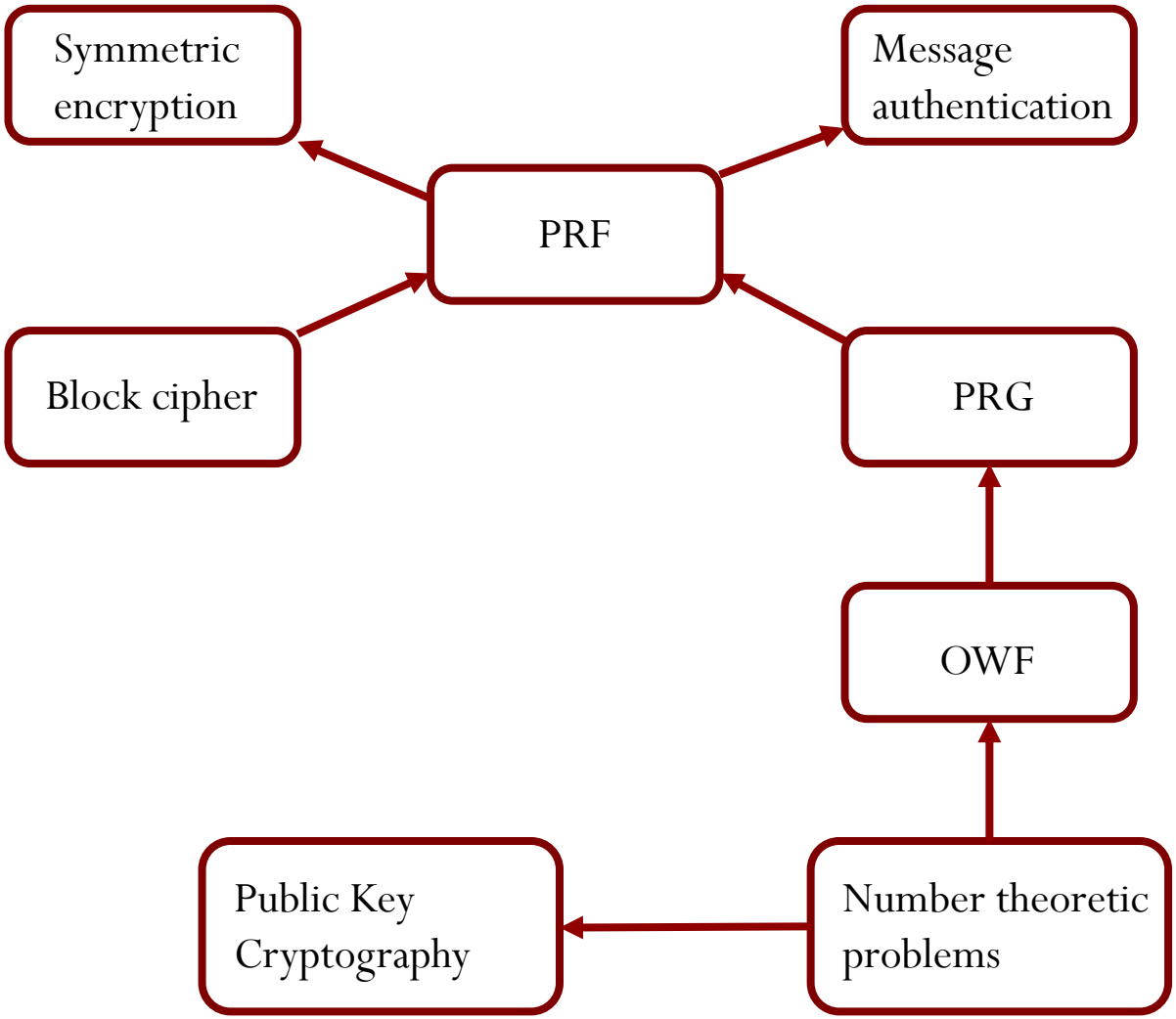
Towards Public Key Cryptography

- The basic building blocks for private key cryptography:
  - Pseudorandom generator
  - Pseudorandom permutation



- Can we start from a *milder* assumption?
  - Existence of *one-way functions* (easy to compute but hard to invert).

Towards Public Key Cryptography



Number Theory

Number Theory

- Z will denote integers.
- $a|b$ means a divides b. If $a \neq \{1, b\}$, then a is called a factor of b.
- Fact 1: Let a be an integer and b be a positive integer. Then there exist unique integers q, r for which $a = qb + r$ and $0 \leq r < b$.
- $\gcd(a, b)$ denotes the gcd of a and b.
- a and b are *relatively prime* if $\gcd(a, b) = 1$.
- Lemma 1: Let a, b be positive integers. Then there exist integers X, Y such that $Xa + Yb = \gcd(a, b)$. Furthermore, $gcd(a, b)$ is the smallest positive integer that can be expressed in this way.

Number Theory

- Lemma 2: If $c|ab$ and $\gcd(a, c) = 1$, then $c|b$. In particular, if p is prime and $p|ab$, then either $p|a$ or $p|b$.

- Lemma 3: If $p|N$, $q|N$, and $\gcd(p, q) = 1$, then $pq|N$.

- Modular Arithmetic:
  - Let a, N be integers such that $N > 1$. $[a\ (mod\ N)]$ is defined to be the remainder in the division of a by N.
    - Recall, there are unique integers q, r such that $0 \leq r < N$ and $a = qN + r$. $[a\ (mod\ N)] = r$.
    - What is $[16\ (mod\ 11)]$?
    - What is $[-6\ (mod\ 11)]$?

Number Theory

- Lemma 2: If $c|ab$ and $\gcd(a, c) = 1$, then $c|b$. In particular, if p is prime and $p|ab$, then either $p|a$ or $p|b$.

- Lemma 3: If $p|N$, $q|N$, and $\gcd(p, q) = 1$, then $pq|N$.

- Modular Arithmetic:
  - Let a, N be integers such that $N > 1$. $[a\ (mod\ N)]$ is defined to be the remainder in the division of a by N.
  - Congurence: Integers a and b are said to be congruent modulo $N > 1$ if $[a\ (mod\ N)] = [b\ (mod\ N)]$. This is denoted by

$$a \equiv b\ (mod\ N)$$

Number Theory

- Modular Arithmetic:
  - Let a, N be integers such that $N > 1$. $[a\ (mod\ N)]$ is defined to be the remainder in the division of a by N.
  - Congurence: Integers a and b are said to be congruent modulo $N > 1$ if $[a\ (mod\ N)] = [b\ (mod\ N)]$. This is denoted by
$$a \equiv b\ (mod\ N)$$
  - Inverse:If for a given integer b there exists an integer b^{-1} such that $bb^{-1} \equiv 1\ (mod\ N)$, we say that b^{-1} is a multiplicative inverse of b modulo N and call b invertible modulo N.
  - Modular division: $\left[\frac{a}{b}\ (mod\ N)\right]$ is defined to be $[ab^{-1}\ (mod\ N)]$ only when b is invertible modulo N.

Number Theory

- Modular Arithmetic:
  - Let a, N be integers such that $N > 1$. $[a\ (mod\ N)]$ is defined to be the remainder in the division of a by N.
  - Congurence: Integers a and b are said to be congruent modulo $N > 1$ if $[a\ (mod\ N)] = [b\ (mod\ N)]$. This is denoted by
$$a \equiv b\ (mod\ N)$$
  - Inverse:If for a given integer b there exists an integer b^{-1} such that $bb^{-1} \equiv 1\ (mod\ N)$, we say that b^{-1} is a multiplicative inverse of b modulo N and call b invertible modulo N.
  - Modular division: $\left[\frac{a}{b}\ (mod\ N)\right]$ is defined to be $[ab^{-1}\ (mod\ N)]$ only when b is invertible modulo N.
- Lemma 4: Let a, N be integers with $N > 1$. Then a is invertible modulo N if and only if $\gcd(a, N) = 1$.

Number Theory

Groups

Groups

- Definition(Group): A group is a set G along with a binary operator $\circ$ for which the following conditions hold:
  - Closure: For all $g, h \in G$, $g \circ h \in G$.
  - Identity: There exists an identity $e \in G$ such that for all $g \in G$, $e \circ g = g = g \circ e$.
  - Inverse: For all $g \in G$, there exists an element $h \in G$, such that $g \circ h = e = h \circ g$. Such an h is called an inverse of g.
  - Associativity: For all $g_1, g_2, g_3 \in G$, $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.
- Definition(Finite group): When G has a finite number of elements we say G is a finite group of *order* $|G|$.
- Definition(Abelian group): G is called an abelian group if it is a group and also satisfies the following condition:
  - Commutativity: For all $g, h \in G$, $g \circ h = h \circ g$.

Groups

- Lemma 1: Identity element in any group is unique.
- Lemma 2: Every element in any group has a unique inverse.
- Definition(Additive notation): The operator is denoted using $+$, the identity element is 0 and the inverse of any element $g \in G$ is denote by $-g$.
  - $g + g + \cdots + g$ ($m$operations) is denoted by mg.
- Definition(Multiplicative notation): The operator is denoted using $\cdot$, the identity element is 1 and the inverse of any element $g \in G$ is denote by g^{-1}.
  - $g \cdot g \cdot \ldots \cdot g$ (m operations) is denoted by g^m.
- Lemma 3: Let G be a group and $a, b, c \in G$. If $ac = bc$, then $a = b$. In particular, if $ac = c$, then a is the identity.

Groups

- Lemma 4: Let G be a finite abelian group with $m = |G|$. Then for any element $g \in G$, $g^m = 1$.
- Corollary 5: Let G be a finite group with $m = |G| > 1$. Then for any $g \in G$ and any integer i, we have $g^i = g^{[i \ (mod\ m)]}$.
- Corollary 6: Let G be a finite group with $m = |G| > 1$. Let $e > 0$ be an integer, and define the function $f_e: G \to G$ by $f_e(g) = g^e$. If $\gcd(e, m) = 1$, then f_e is a permutation. Moreover, if $d = [e^{-1} \ (mod\ m)]$, then f_d is the inverse of f_e.

Groups: The group Z_n^*

- Operation: Multiplication modulo N.
- Set: Z_N^*=Subset of $\{1, \dots, N\}$ that are invertible modulo N.
- Lemma 1: $Z_N^* = \{a \in \{1, \dots, N\} | \gcd(a, N) = 1\}$.
- Lemma 2: Z_N^* is an abelian group under multiplication modulo N.
- Definition(Euler phi function): The order of group Z_N^* is denoted by the Euler phi function $\phi(N)$.
  - Let N be prime. What is $\phi(N)$?
  - Let $N = p \cdot q$ for primes p, q. What is $\phi(N)$?
- Theorem 3: Let $N = \prod_i p_i^{e_i}$, where p_i's are distinct primes and $e_i \geq 1$. Then $\phi(N) = \prod_i p_i^{e_i - 1} \cdot (p_i - 1)$.

Groups: The group Z_n^*

- Operation: Multiplication modulo N.
- Set: Z_N^*=Subset of $\{1, \dots, N\}$ that are invertible modulo N.
- Lemma 1: $Z_N^* = \{a \in \{1, \dots, N\} | \gcd(a, N) = 1\}$.
- Lemma 2: Z_N^* is an abelian group under multiplication modulo N.
- Definition(Euler phi function): The order of group Z_N^* is denoted by the Euler phi function $\phi(N)$.
- Theorem 3: Let $N = \prod_i p_i^{e_i}$, where p_i's are distinct primes and $e_i \geq 1$. Then $\phi(N) = \prod_i p_i^{e_i - 1} \cdot (p_i - 1)$.
- Corollary 4: Take arbitrary $N > 1$ and $a \in Z_N^*$. Then $a^{\phi(N)} \equiv 1 \ (mod\ N)$. For the case when $N = p$ is prime and $a \in \{1, \dots, p-1\}$, we have $a^{p-1} \equiv 1 \ (mod\ p)$.

Groups: The group Z_n^*

- Definition(Euler phi function): The order of group Z_N^* is denoted by the Euler phi function $\phi(N)$.
- Theorem 3: Let $N = \prod_i p_i^{e_i}$, where p_i's are distinct primes and $e_i \geq 1$. Then $\phi(N) = \prod_i p_i^{e_i - 1} \cdot (p_i - 1)$.
- Corollary 4: Take arbitrary $N > 1$ and $a \in Z_N^*$. Then $a^{\phi(N)} \equiv 1 \ (mod\ N)$. For the case when $N = p$ is prime and $a \in \{1, \ldots, p-1\}$, we have $a^{p-1} \equiv 1 \ (mod\ p)$.
- Corollary 5: Fix $N > 1$. For integer $e > 0$ define $f_e: Z_N^* \rightarrow Z_N^*$ by $f_e(x) = [x^e \ (mod\ N)]$. If e is relatively prime to $phi(N)$, then f_e is a permutation. Moreover, if $d = [e^{-1} \ (mod\ \phi(N))]$, then f_d is the inverse of f_e.

Chinese Remaindering Theorem (CRT)

Chinese Remaindering Theorem

- Lemma 1(Group cross product): Let G, H be group under operations $\circ_G, \circ_H$ respectively. Then $G \times H$ under the operations $\circ$ defined as $(g, h) \circ (g', h') = (g \circ_G g', h \circ_H h')$ is also a group.
- Definition(Isomorphism): Let G, H be groups under operations $\circ_H, \circ_G$ respectively. A function $f: G \to H$ is an isomorphism from G to H if
  1. f is a bijection, and
  2. For all $g_1, g_2 \in G$ we have $f(g_1 \circ_G g_2) = f(g_1) \circ_H f(g_2)$.

  If there exists an isomorphism from G to H, then we say that these groups are isomporphic and write this as $G \simeq H$.

Chinese Remaindering Theorem

- Recall:
  - $Z_N = \{0, \ldots, N-1\}$ is a group under addition modulo N.
  - $Z_N^* = \{a \in \{1, \ldots, N-1\} | \gcd(a, N) = 1\}$ is a group under multiplication modulo N.
- Theorem 2: Let $N = p \cdot q$ where p and q are relatively prime (i.e., $\gcd(p, q) = 1$). Then

$$Z_N \simeq Z_p \times Z_q \text{ and } Z_N^* \simeq Z_p^* \times Z_q^*.$$

Moreover, let f be the function mapping elements $x \in \{0, \ldots, N-1\}$ to pairs (x_p, x_q) with $x_p \in \{0, \ldots, p-1\}$ and $x_q \in \{0, \ldots, q-1\}$ defined by

$$f(x) = ([x \ (mod\ p)], [x \ (mod\ q)])$$

Then f is am isomorphism from Z_N to $Z_p \times Z_q$ as well as an isomorphism from Z_N^* to $Z_p^* \times Z_q^*$.

Chinese Remaindering Theorem

- Theorem 2: Let $N = p \cdot q$ where p and q are relatively prime (i.e., $\gcd(p, q) = 1$). Then

$$Z_N \simeq Z_p \times Z_q \text{ and } Z_N^* \simeq Z_p^* \times Z_q^*.$$

  Moreover, let f be the function mapping elements $x \in \{0, \dots, N-1\}$ to pairs (x_p, x_q) with $x_p \in \{0, \dots, p-1\}$ and $x_q \in \{0, \dots, q-1\}$ defined by

$$f(x) = ([x \ (mod\ p)], [x \ (mod\ q)])$$

  Then f is am isomorphism from Z_N to $Z_p \times Z_q$ as well as an isomorphism from Z_N^* to $Z_p^* \times Z_q^*$.

- Lemma 3: f is efficiently computable.
- Lemma 4: f^{-1} is efficiently computable.

Chinese Remaindering Theorem

- Theorem 2: Let $N = p \cdot q$ where p and q are relatively prime (i.e., $\gcd(p, q) = 1$). Then

$$Z_N \simeq Z_p \times Z_q \text{ and } Z_N^* \simeq Z_p^* \times Z_q^*.$$

Moreover, let f be the function mapping elements $x \in \{0, \dots, N-1\}$ to pairs (x_p, x_q) with $x_p \in \{0, \dots, p-1\}$ and $x_q \in \{0, \dots, q-1\}$ defined by

$$f(x) = ([x \ (mod\ p)], [x \ (mod\ q)])$$

Then f is am isomorphism from Z_N to $Z_p \times Z_q$ as well as an isomorphism from Z_N^* to $Z_p^* \times Z_q^*$.

- Lemma 4: f^{-1} is efficiently computable.
  - Since $\gcd(p, q) = 1$, there exists integers X, Y such that $X \cdot p + Y \cdot q = 1$.
  - Let $1_p = [Y \cdot q \ (mod\ N)]$ and $1_q = [X \cdot p \ (mod\ N)]$.
  - Claim: $f^{-1}(x_p, x_q) = \left[\left(x_p \cdot 1_p + x_q \cdot 1_q\right)(mod\ N)\right]$.
  - How efficient is this computation?

Extended Euclid Algorithm for GCD

- Problem: Given integers $a, b > 0$, design an algorithm for computing $\gcd(a, b)$.
- Euclid-GCD(a, b)
  - If $b|a$, then return b.
  - Else return Euclid-GCD$(b, [a \ (mod \ b)])$.
- Lemma 5: The above algorithm is correct.
- What is the running time of Euclid-GCD?
- Problem: Given integers $a, b > 0$, design an algorithm for computing integers X, Y such that $X \cdot a + Y \cdot b = \gcd(a, b)$.

Extended Euclid Algorithm for GCD

- Problem: Given integers $a \geq b > 0$, design an algorithm for computing $\gcd(a, b)$.
- Euclid-GCD(a, b)
  - If $b|a$, then return b.
  - Else return Euclid-GCD$(b, [a \ (mod \ b)])$.
- Problem: Given integers $a \geq b > 0$, design an algorithm for computing integers X, Y such that $X \cdot a + Y \cdot b = \gcd(a, b)$.
- Extended-Euclid-GCD(a, b)
  - If $b|a$, then return $(b, 0, 1)$.
  - Else
    - Compute integers q, r such that $a = q \cdot b + r$ and $0 \leq r < b$.
    - Let (d, X, Y) =Extended-Euclid-GCD(b, r).
    - return $(d, Y, X - Y \cdot q)$.

Extended Euclid Algorithm for GCD

- Problem: Given integers $a \geq b > 0$, design an algorithm for computing integers X, Y such that $X \cdot a + Y \cdot b = \gcd(a, b)$.
- Extended-Euclid-GCD(a, b)
  - If $b|\mathrm{a}$, then return $(b, 0, 1)$.
  - Else
    - Compute integers q, r such that $a = q \cdot b + r$ and $0 \leq r < b$.
    - Let (d, X, Y) =Extended-Euclid-GCD(b, r).
    - return $(d, Y, X - Y \cdot q)$.
- Problem: Given positive integers $1 \leq a < N$ such that $\gcd(a, N) = 1$. Compute the inverse of a in the group Z_N^* under multiplication modulo N.

The Factoring Problem

The Factoring Problem

- We would like to understand the success of polynomial time algorithms in factoring integers. We formally define this in terms of an experiment:
- Experiment Weak-Factor(A, n)
  - Choose two n-bit integers x_1 and x_2 at random.
  - Compute $N = x_1 \cdot x_2$
  - Adversary A is given N and let it output (x_1', x_2').
  - If $(x_1' \cdot x_2' = N)$ then output 1 else output 0.
- Can we show that for all PPT algorithms A, $\Pr[Weak -$

The Factoring Problem

- We would like to understand the success of polynomial time algorithms in factoring integers. We formally define this in terms of an experiment:
- Experiment Factor(A, n)
  - Choose two n-bit primes x_1 and x_2 at random.
  - Compute $N = x_1 \cdot x_2$
  - Adversary A is given N and let it output (x_1', x_2').
  - If $(x_1' \cdot x_2' = N)$ then output 1 else output 0.
- How do we randomly generate an n-bit prime number?

The Factoring Problem

- How do we randomly generate an n-bit prime number?
- GRP(1^n)
  - For $i = 1$ to t
    - Randomly pick $p' \in \{0,1\}^{n-1}$
    - $p \leftarrow 1|p'$
    - If (p is prime) then output p
  - Output "fail"
- What is the probability (in terms of t) that the above algorithm outputs a prime number?

The Factoring Problem

- How do we randomly generate an n-bit prime number?
- GRP(1^n)
  - For $i = 1$ to t
    - Randomly pick $p' \in \{0,1\}^{n-1}$
    - $p \leftarrow 1|p'$
    - If (p is prime) then output p
  - Output "fail"
- What is the probability (in terms of t) that the above algorithm outputs a prime number?
- Theorem (Prime Number Theorem): There exists a constant c such that for any $n > 1$, the number of n bit primes is at least $c \cdot \frac{2^{n-1}}{n}$.

The Factoring Problem

- How do we randomly generate an n-bit prime number?
- GRP(1^n)
  - For $i = 1$ to t
    - Randomly pick $p' \in \{0,1\}^{n-1}$
    - $p \leftarrow 1|p'$
    - If (p is prime) then output p
  - Output "fail"
- Problem(Primality Testing): Given an integer $N > 1$, how do we check that it is prime or not?

The Factoring Problem

- How do we randomly generate an n-bit prime number?
- GRP(1^n)
  - For $i = 1$ to t
    - Randomly pick $p' \in \{0,1\}^{n-1}$
    - $p \leftarrow 1|p'$
    - If (p is prime) then output p
  - Output "fail"
- Problem(Primality Testing): Given an integer $N > 1$, how do we check that it is prime or not?
  - There is a randomized algorithm (Miller-Rabin) with one-sided error when the given number is composite. This algorithm runs very fast.
  - There is a polynomial time deterministic algorithm (AKS) too but it runs slower than the randomized algorithm.

End