Practical Cryptographic Systems

Mathematical Background for Asymmetric Cryptography

Some Housekeeping

- Office hours:
  - Monday (Alishah) 2-3:30 in Malone 216
    Wednesday (Matt) 2-3:30 in Malone 307
    Thursday (Rohit) 2-3:30 in Malone 216
- Late day policy
- Assignment 1 due at midnight
- Weekly hw 1 due Wednesday at midnight
- Start looking for group members for course project

Fundamental Theorem of Arithmetic

- **Theorem:** *Every* $n \in \mathbb{Z}$, $n \neq 0$ *has a unique factorization* $n = \pm\, p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ *with* p_i *distinct primes and* e_i *positive integers*

Division and Remainder

- **Theorem:**
  $a, b \in \mathbb{Z}, b > 0, \exists\ unique\ q, r\ \in \mathbb{Z}\ s.t.\ a = bq + r, 0 \leq r \leq b.$

$r \equiv a\ mod\ b$

$a\ mod\ b = a - b\lfloor \frac{a}{b} \rfloor$

$a | b \Leftrightarrow a\ mod\ b = 0$

$a = b\ mod\ N \Leftrightarrow N | (a - b)$

GCDs and Extended Euclidean Algorithm

gcd(a, b) : **greatest common divisor** d **s.t.** $d \mid a$ **and** $d \mid b$

Theorem (Extended Euclidean Algorithm)

$a, b \in \mathbb{Z}$ $(and\ positive)$ $\exists x, y \in \mathbb{Z}$ $s.t.$ $ax + by =$ **gcd**(a, b)

Extended Euclidean Algorithm

Input: $a, b \in \mathbb{Z}$
Output: d, x, y with $d = \text{gcd}(a, b),\ ax + by = d$

If $b \mid a$:
    return b,0,1

Else:
    compute $a = qb + r$
    $d, x, y = \text{gcd}(b, r)$ \\\\ $(xb + yr = d)$
    return $(d, y, x - yq)$

Extended Euclidean Algorithm

- Runs in time $O(\log(a)\log(b))$

- Theorem:
  $If\ c \mid ab,\ \gcd(a,c) = 1 \Rightarrow c \mid b$

Modular Inverse

- Inverse of $a \ mod \ N : a \cdot a^{-1} \ mod \ N$
  - Only defined if a is invertible
  - 0 has no inverse
- Can use Extended Euclidean Algorithm to find inverse

$$a \ invertible \ mod \ N \Leftrightarrow \text{gcd}(a, N) = 1$$

$$\exists x, y \ s.t. \ ax + Ny = 1 \Rightarrow x = a^{-1} \ mod \ N$$

Groups

- A group $(G, \cdot\,)$ is a set G and an operation $\cdot$
- A group G must satisfy the following properties
  - Closed under operation: $\forall a, b \in G, a \cdot b \in G$
  - Identity: $\exists e \in G\ s.t.\ \forall a \in G, e \cdot a = a$
  - Inverses: $\forall a \in G, \exists b \in G\ s.t.\ a \cdot b = e$
  - Associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Groups

- A group is *Abelian* if it has the additional property:
  - Commutative: $\forall a, b \in G, a \cdot b = b \cdot a$
- Cyclic group:
  - G is generated by one element :
    $\exists a, \{e, a, a \cdot a, a \cdot a, a \cdot a \cdot a \cdot a, \ldots\} = G$
    $\exists a, \{a^0, a^1, a^2, a^3, \ldots, a^{n-1}\} = G,$ for some n (we call n the order of G)
  - Notationally we say, $G = (\langle a \rangle, \cdot\,)$

Examples of Groups

- $\mathbb{Z}$ is an abelian group under $+$
  identity $= 0$, inverse $= - g$, cyclic with $\mathbb{Z} = (\langle 1 \rangle, +)$

Examples of Groups

- $\mathbb{Z}$ is an abelian group under $+$
  identity $= 0$, inverse $= -g$, cyclic with $\mathbb{Z} = (\langle 1 \rangle, +)$
- $\mathbb{Z}$ is not a group under $\times$ (not all elements have inverses in $\mathbb{Z}$)

Examples of Groups

- $\mathbb{Z}$ is an abelian group under $+$
  identity $= 0$, inverse $= -g$, cyclic with $\mathbb{Z} = (\langle 1 \rangle, +)$
- $\mathbb{Z}$ is not a group under $\times$ (not all elements have inverses in $\mathbb{Z}$)
- $\mathbb{Z}_N$ $(\mathbb{Z}\ mod\ N)$ is an abelian group under $+$
  identity $= 0$, inverse $= -g$, cyclic with $\mathbb{Z}_N = (\langle 1 \rangle, +)$

Examples of Groups

- $\mathbb{Z}$ is an abelian group under $+$
  identity $= 0$, inverse $= -g$, cyclic with $\mathbb{Z} = (\langle 1 \rangle, +)$
- $\mathbb{Z}$ is not a group under $\times$ (not all elements have inverses in $\mathbb{Z}$)
- $\mathbb{Z}_N$ $(\mathbb{Z}\ mod\ N)$ is an abelian group under $+$
  identity $= 0$, inverse $= -g$, cyclic with $\mathbb{Z}_N = (\langle 1 \rangle, +)$
- $\mathbb{Z}_N$ is not a group under $\times$ (need gcd$(a, N) = 1$)
- $\mathbb{Z}_p$ is a group under $\times$ if p is prime
  We call this the "multiplicative group mod p": $\mathbb{Z}_p^* = \mathbb{Z}_p \backslash\ 0$

$\mathbb{Z}_p^*$

- Suppose $p = 7$:
  $3^0\ mod\ 7 = 1,\ 3^1\ mod\ 7 = 1,\ 3^2\ mod\ 7 = 2,\ 3^3\ mod\ 7 = 6,\ 3^4\ mod\ 7 = 4,\ 3^5\ mod\ 7 = 5,\ 3^6\ mod\ 7 = 1$
  $\mathbb{Z}_7^* = (\langle 3 \rangle, \times)$

- $\mathbb{Z}_p^*$ is cyclic, there is always a generator.

$\mathbb{Z}_p^*$

- Suppose $p = 7$:
  $3^0\ mod\ 7 = 1,\ 3^1\ mod\ 7 = 1,\ 3^2\ mod\ 7 = 2,\ 3^3\ mod\ 7 = 6,\ 3^4\ mod\ 7 = 4,\ 3^5\ mod\ 7 = 5,\ 3^6\ mod\ 7 = 1$
  $\mathbb{Z}_7^* = (\langle 3 \rangle, \times)$

- $\mathbb{Z}_p^*$ is cyclic, there is always a generator.

- Not all elements will be the generator:
  $2^0\ mod\ 7 = 1,\ 2^1\ mod\ 7 = 2,\ 2^2\ mod\ 7 = 4,\ 2^3\ mod\ 7 = 1,\ 2^4\ mod\ 7 = 2,\ 2^5\ mod\ 7 = 4,\ 2^6\ mod\ 7 = 1$

Group Orders and $\mathbb{Z}_p^*$

- $|G|$ is called the *order* of the group. The order of an element g is $|\langle g \rangle|$
- **Theorem (Langrange):** order$(g) \,|\, p-1$
- For $\mathbb{Z}_7^*$, $|\langle 3 \rangle| = 6$, $|\langle 2 \rangle| = 3$

Group Orders and $\mathbb{Z}_p^*$

- $|G|$ is called the *order* of the group. The order of an element g is $|\langle g \rangle|$
- **Theorem (Langrange):** order$(g) \,|\, p-1$
- For $\mathbb{Z}_7^*$, $|\langle 3 \rangle| = 6$, $|\langle 2 \rangle| = 3$

$\exists$ efficient algorithm to find generator is factorization of $p-1$ is known

Fermat's Little Theorem

- **Theorem:** $\forall g \in \mathbb{Z}_P^*,\ g^{p-1} = 1$

Fermat's Little Theorem

- **Theorem:** $\forall g \in \mathbb{Z}_P^*,\ g^{p-1} = 1$
- Ex: $3^4 = 81 \equiv 1\ mod\ 5$

Fermat's Little Theorem

- **Theorem:** $\forall g \in \mathbb{Z}_P^*,\ g^{p-1} = 1$
- Ex: $3^4 = 81 \equiv 1\ mod\ 5$
- Ex: $3^6 = 729 \equiv 1\ mod\ 7$

Fermat's Little Theorem

- **Theorem:** $\forall g \in \mathbb{Z}_P^*,\ g^{p-1} = 1$
- Ex: $3^4 = 81 \equiv 1\ mod\ 5$
- Ex: $3^6 = 729 \equiv 1\ mod\ 7$
- Ex $2^6 = 64 \equiv 1\ mod\ 7$

Arithmetic modulo Composites

- What if we have $\mathbb{Z}_N$ where N is composite?

Arithmetic modulo Composites

- What if we have $\mathbb{Z}_N$ where N is composite?
- Only have inverses if gcd$(a, N) = 1$
  - Can still be found using extended euclidean algorithm

Arithmetic modulo Composites

- What if we have $\mathbb{Z}_N$ where N is composite?
- Only have inverses if gcd$(a, N) = 1$
  - Can still be found using extended euclidean algorithm
- $\mathbb{Z}_N^*$ is the set of invertible elements in $\mathbb{Z}_N$

Arithmetic modulo Composites

- What if we have $\mathbb{Z}_N$ where N is composite?
- Only have inverses if gcd$(a, N) = 1$
  - Can still be found using extended euclidean algorithm
- $\mathbb{Z}_N^*$ is the set of invertible elements in $\mathbb{Z}_N$
- How do we know how many elements are in $\mathbb{Z}_N^*$?

Euler's Totient Function

- The Euler totient function $\varphi(n)$ denotes the number of elements in $\mathbb{Z}_N^*$.
- $\varphi(p) = p - 1$ for prime p
- For primes p, q and $N = pq$, $\varphi(N) = (p-1)(q-1)$

Euler's Totient Function

- The Euler totient function $\varphi(n)$ denotes the number of elements in $\mathbb{Z}_N^*$.
- $\varphi(p) = p - 1$ for prime p
- For primes p, q and $N = pq$, $\varphi(N) = (p-1)(q-1)$
- Ex: $\varphi(15 = 3 \times 5) = |\{1,2,4,7,8,11,13,14\}| = 8 = 2 \times 4$

Euler's Totient Function

- The Euler totient function $\varphi(n)$ denotes the number of elements in $\mathbb{Z}_N^*$.
- $\varphi(p) = p - 1$ for prime p
- For primes p, q and $N = pq$, $\varphi(N) = (p-1)(q-1)$
- Ex: $\varphi(15 = 3 \times 5) = |\{1,2,4,7,8,11,13,14\}| = 8 = 2 \times 4$
- **Euler's Theorem:** $\forall a \in \mathbb{Z}_N^*,\ a^{\varphi(N)} = 1$

Chinese Remainder Theorem

- **Theorem:** Let $N = pq$, where p, q are relatively prime (not necessarily prime). *Given* a_1, a_2 *there is a unique* $x \in \mathbb{Z}_N$ *such that*
  $x \equiv a_1 \ mod \ p, x \equiv a_2 \ mod \ q$

Chinese Remainder Theorem

- **Theorem:** Let $N = pq$, where p, q are relatively prime (not necessarily prime).
  Given a_1, a_2 *there is a unique* $x \in \mathbb{Z}_N$ *such that*
  $x \equiv a_1 \ mod \ p, x \equiv a_2 \ mod \ q$

- *Ex: for* $2 \ mod \ 3, \ 3 \ mod \ 5$
  $8 \equiv 2 \ mod \ 3, \ 8 \equiv 3 \ mod \ 5$

Chinese Remainder Theorem

- **Theorem:** Let $N = pq$, where p, q are relatively prime (not necessarily prime). *Given* a_1, a_2 *there is a unique* $x \in \mathbb{Z}_N$ *such that* $x \equiv a_1 \ mod\ p, x \equiv a_2 \ mod\ q$

- *Ex: for* $2\ mod\ 3,\ 3\ mod\ 5$
  $8 \equiv 2\ mod\ 3,\ 8 \equiv 3\ mod\ 5$

Can use gcd algorithm to find x in the case of only 2 moduli

Number Theory and Hardness

- We have many operations that are efficient to compute:
  - Addition
  - Subtraction
  - Multiplication
  - Inversion (Through GCD)
  - Modular Exponentiation?

Computing Modular Exponentiations

- Inefficient approach:
  $g^a = g \cdot g \ldots \cdot g$ a times

Computing Modular Exponentiations

- Inefficient approach:
  $g^a = g \cdot g \ldots \cdot g$ a times
- Better approach: Square-and-Multiply

```
SquareMult(x, e, N):
  let e_n, ..., e_1 be the bits of e
  y ← 1
  for i = n down to 1 {
    y ← Square(y)                (S)
    y ← ModReduce(y, N)          (R)
    if e_i = 1 then {
      y ← Mult(y, x)             (M)
      y ← ModReduce(y, N)        (R)
    }
  }
  return y
```

https://matthewdgreen.files.wordpress.com/2012/10/1e9d6-squaremultiply.png

Discrete Logarithm

- Given y, g find x such that $g^x \equiv y \ mod \ p$, (undoes modular exponentiation)

Discrete Logarithm

- Given y, g find x such that $g^x \equiv y \ mod \ p$, (undoes modular exponentiation)

- We do not have a general purpose efficient algorithm
  - We do have some algorithms for specific instances (index calculus)
  - Best algorithm: Number field sieve
- Quantum Setting?

Factoring Assumption

- **Assumption:** Given $N = pq$, hard to compute p, q efficiently
- Assumed to be hard for properly chosen large factors p, q (>1024 bits)
- Best Algorithm: General Number Field Sieve or Quadratic Sieve Algorithm
- Quantum Setting?

Next time

- Public Key Encryption and RSA