Number Theory

Introduction

Why this lesson?

Many crypto schemes relies on

- Group properties
- Modular arithmetic
- Primes properties

What a group is…

Which properties exploited in crypto…

How asymmetric crypto works…

Many boring, but useful, things explained here

- I hope ☺

Groups

Let $\mathbb{G}$ be a set and $\circ(\bullet,\bullet)$ a binary operator

The pair $(\mathbb{G}, \circ)$ is a "group" if:

- Closure: $\forall g, h \in \mathbb{G} \Rightarrow g \circ h \in \mathbb{G}$
- Identity Element: $\exists e \in \mathbb{G}\ s.t. \forall g \in \mathbb{G} \Rightarrow e \circ g = g$
- Inverse Element: $\exists h \in \mathbb{G}\ s.t. \forall g \in \mathbb{G} \Rightarrow h \circ g = e$
- Associativity: $\forall g_1, g_2, g_3 \in \mathbb{G} \Rightarrow (g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$

- A group $(\mathbb{G}, \circ)$ is abelian if:
  - Commutativity: $\forall g, h \in \mathbb{G} \Rightarrow g \circ h = h \circ g$

If $\mathbb{G}$ has a finite number of elements ⇒ finite group

- The order of $\mathbb{G}$ is denoted by $|\mathbb{G}|$

Groups

Consider the set of integers $\mathbb{Z}$

- We have all value in $\{\mathbf{0}, \mathbf{1}, \mathbf{2}, \dots\} \cup \{-\mathbf{1}, -\mathbf{2}, -\mathbf{3}, \dots\}$
- What about $(\mathbb{Z}, \circ) = (\mathbb{Z}, +)$?

- Closure: $g + h \in \mathbb{Z}$?
- Identity Element: $g + e = g$?
- Inverse Element: $g + h = e$?
- Associativity: $(a + b) + c = a + (b + c)$?

- Commutativity: $a + b = \mathrm{b} + \mathrm{a}$?

- Finite group?

Groups

Consider the set of integers $\mathbb{Z}$

- We have all value in $\{\mathbf{0}, \mathbf{1}, \mathbf{2}, \dots\} \cup \{-\mathbf{1}, -\mathbf{2}, -\mathbf{3}, \dots\}$
- What about $(\mathbb{Z}, \circ) = (\mathbb{Z}, +)$?

- Closure: $g + h \in \mathbb{Z}$? ✓
- Identity Element: $g + e = g$? ✓
- Inverse Element: $g + h = e$? ✓
- Associativity: $(a + b) + c = a + (b + c)$? ✓

- Commutativity: $a + b = \mathrm{b} + \mathrm{a}$? ✓

- Finite group? ✗

Groups

Consider the set of integers $\mathbb{Z}$

- We have all value in $\{\mathbf{0}, \mathbf{1}, \mathbf{2}, \dots\} \cup \{-\mathbf{1}, -\mathbf{2}, -\mathbf{3}, \dots\}$
- What about $(\mathbb{Z}, \circ) = (\mathbb{Z}, \cdot)$?

- Closure: $g \cdot h \in \mathbb{Z}$?
- Identity Element: $g \cdot e = g$?
- Inverse Element: $g \cdot h = e$?
- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$?

- Commutativity: $a \cdot b = \mathrm{b} \cdot \mathrm{a}$?

- Finite group?

Groups

Consider the set of integers $\mathbb{Z}$

- We have all value in $\{\mathbf{0}, \mathbf{1}, \mathbf{2}, \dots\} \cup \{-\mathbf{1}, -\mathbf{2}, -\mathbf{3}, \dots\}$
- What about $(\mathbb{Z}, \circ) = (\mathbb{Z}, \cdot)$?

- Closure: $g \cdot h \in \mathbb{Z}$? ✓
- Identity Element: $g \cdot e = g$? ✓
- Inverse Element: $g \cdot h = e$? ✗
- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$? ✓

- Commutativity: $a \cdot b = \mathrm{b} \cdot \mathrm{a}$? ✓

- Finite group? ✗

Groups

Consider the set of real $\mathbb{R}$

- What about $(\mathbb{R}, \circ) = (\mathbb{R}, \cdot)$?

- Closure: $g \cdot h \in \mathbb{R}$?
- Identity Element: $g \cdot e = g$?
- Inverse Element: $g \cdot h = e$?
- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$?

- Commutativity: $a \cdot b = \mathrm{b} \cdot \mathrm{a}$?

- Finite group?

Groups

Consider the set of real $\mathbb{R}$

- What about $(\mathbb{R}, \circ) = (\mathbb{R}, \cdot)$?

- Closure: $g \cdot h \in \mathbb{R}$? ✓
- Identity Element: $g \cdot e = g$? ✓
- Inverse Element: $g \cdot h = e$? ✗
- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$? ✓

- Commutativity: $a \cdot b = \mathrm{b} \cdot \mathrm{a}$? ✓

- Finite group? ✗

Groups

Consider the set of real $\mathbb{R}\backslash\{0\}$

- What about $(\mathbb{R}, \circ) = (\mathbb{R}, \cdot)$?

- Closure: $g \cdot h \in \mathbb{R}$? ✓
- Identity Element: $g \cdot e = g$? ✓
- Inverse Element: $g \cdot h = e$? ✓
- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$? ✓

- Commutativity: $a \cdot b = \mathrm{b} \cdot \mathrm{a}$? ✓

- Finite group? ✗

Modular Arithmetic

Let $a, N \in \mathbb{Z}$

- The relation between them is: $a = q\mathrm{N} + r$
- Where:

$$q = \left\lfloor \frac{a}{\mathrm{N}} \right\rfloor$$

$$r \equiv a \; mod N$$

While:

- $a, q, N \in \{\dots, -2, -1, 0, 1, 2, \dots\} \in \mathbb{Z}$

Observe that:

- The remainder r belongs to a different set!
- $r \in \{0, 1, 2, \dots, N-1\} \Rightarrow \mathbb{Z}_N : \{0, \dots, N-1\}$

Modular Arithmetic

It works exactly as you expect

- Define the module N
- Apply the $mod N$ operator to elements in $\mathbb{Z}$
- The obtained set has size $N: \{0, \dots, N-1\}$

- $N = 5 \Rightarrow \mathbb{Z}_5: \{0, 1, 2, 3, 4\}$
- $N = 12 \Rightarrow \mathbb{Z}_{12}: \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
  - $(8 + 17) mod 12 = 1 \in \mathbb{Z}_{12}$
  - $(5 \cdot 13) mod 12 = 5 \in \mathbb{Z}_{12}$

Exploit this set to obtain a finite group:

- Respect to sum ⇒ additive group
- Respect to product ⇒ multiplicative

Groups: Additive

Consider the set of integers $\mathbb{Z}_N$

- Let $N > 1 \Rightarrow \mathbb{Z}_N: \{0, \ldots, N-1\}$
- Define the addition as $a + b \stackrel{\text{def}}{=} [(a+b)\ mod N]$
- What about $(\mathbb{Z}_N, \circ) = (\mathbb{Z}_N, +)$?

- Closure: $g + h \in \mathbb{Z}_N$?
- Identity Element: $g + e = g$?
- Inverse Element: $g + h = e$?
- Associativity: $(a + b) + c = a + (b + c)$?

- Commutativity: $a + b = \mathrm{b} + \mathrm{a}$?

- Finite group?

Groups: Additive

Consider the set of integers $\mathbb{Z}_N$

- Let $N > 1 \Rightarrow \mathbb{Z}_N: \{0, \dots, N-1\}$
- Define the addition as $a + b \stackrel{\text{def}}{=} [(a+b)\ mod N]$
- What about $(\mathbb{Z}_N, \circ) = (\mathbb{Z}_N, +)$?

- Closure: $g + h \in \mathbb{Z}_N$? ✓
- Identity Element: $g + e = g \Rightarrow e = 0$ ✓
- Inverse Element: $g + h = e$? ✓
- Associativity: $(a + b) + c = a + (b + c)$? ✓

- Commutativity: $a + b = \mathrm{b} + \mathrm{a}$? ✓

- Finite group $\Rightarrow N$ elements: $\{0, \dots, N-1\}$ ✓

Groups: Multiplicative

Consider the set of integers $\mathbb{Z}_N$

- Let $N > 1 \Rightarrow \mathbb{Z}_N: \{0, \dots, N-1\}$
- Define the product as $a \cdot b \stackrel{\text{def}}{=} [(a \cdot b)\ mod N]$
- What about $(\mathbb{Z}_N, \circ) = (\mathbb{Z}_N, \cdot)$?

- Closure: $g \cdot h \in \mathbb{Z}_N$?
- Identity Element: $g \cdot e = g$?
- Inverse Element: $g \cdot h = e$?
- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$?

- Commutativity: $a \cdot b = \mathrm{b} \cdot \mathrm{a}$?

- Finite group?

Groups: Multiplicative

Consider the set of integers $\mathbb{Z}_N$

- Let $N > 1 \Rightarrow \mathbb{Z}_N: \{0, \dots, N-1\}$
- Define the product as $a \cdot b \stackrel{\text{def}}{=} [(a \cdot b)\ mod N]$
- What about $(\mathbb{Z}_N, \circ) = (\mathbb{Z}_N, \cdot)$?

- Closure: $g \cdot h \in \mathbb{Z}_N$? ✓
- Identity Element: $g \cdot e = g \Rightarrow e = 1$ ✓
- Inverse Element: $g \cdot h = e$? ✗
- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$? ✓

- Commutativity: $a \cdot b = \mathrm{b} \cdot \mathrm{a}$? ✓

- Finite group $\Rightarrow N$ elements: $\{0, \dots, N-1\}$ ✓

Groups: Inverse

Must be redefined in $\mathbb{Z}_N$

- $a^{-1} \cdot a = 1$ cannot be applied
- $y \in \mathbb{Z}_N$ s.t. $x \cdot y = 1$ in $\mathbb{Z}_N$

In $\mathbb{Z}_N$:

- $gcd(\mathrm{a}, b)$ is the great common divisor
- $a \cdot X + b \cdot \mathrm{Y} = \mathrm{gcd}(\mathrm{a}, \mathrm{b})$ → Euclidean Algorithm
  - X, Y → Extended Euclidean Algorithm
- $gcd(x, N) = 1 \Leftrightarrow x$ and N are **relative primes**

Whenever N is odd:

- 2 is always invertible in $\mathbb{Z}_N$: $(N + 1)/2$

Groups: Multiplicative

Define a multiplicative group over $\mathbb{Z}_N$

- For elements of $\mathbb{Z}_N$ s.t. $gcd(x, N) = 1$

$$\mathbb{Z}_N^* = \{set\ of\ invertible\ elements\ in\ \mathbb{Z}_N\} =$$
$$= \{x \in \mathbb{Z}_N : \gcd(x, N) = 1\}$$

$\mathbb{Z}_N^*$ is $\mathbb{Z}_N$ subset of invertible elements

- $\mathbf{p}$ prime $\Rightarrow \mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{0\} = \{1,2,3, \dots, p-1\}$
- $\boldsymbol{N = 6} \Rightarrow \mathbb{Z}_6^* = \mathbb{Z}_6 \backslash \{0,2,3,4\} = \{1,5\}$
- $\boldsymbol{N = 12} \Rightarrow \mathbb{Z}_{12}^* = \mathbb{Z}_{12} \backslash \{0,2,3,4,6,8,9,10\} = \{1,5,7,11\}$

Groups: Multiplicative

Consider the set of integers $\mathbb{Z}_N^*$

- Let $N > 1 \Rightarrow \mathbb{Z}_N^*: \{x \in \mathbb{Z}_N: \gcd(x, N) = 1\}$
- Define the product as $a \cdot b \stackrel{\text{def}}{=} [(a \cdot b)\ mod N]$
- What about $(\mathbb{Z}_N^*, \circ) = (\mathbb{Z}_N^*, \cdot)$?

- Closure: $g \cdot h \in \mathbb{Z}_N^*$? ✓
- Identity Element: $g \cdot e = g \Rightarrow e = 1$ ✓
- Inverse Element: $g \cdot h = e$? ✓
- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$? ✓

- Commutativity: $a \cdot b = \mathrm{b} \cdot \mathrm{a}$? ✓

- Finite group? ✓

Cyclic Groups

Let $\mathbb{G}$ be a finite group of order m

- $\mathbb{G}$ is a cyclic group if:

$$\exists g : \{g^0, g^1, g^2, \dots, g^{m-1}\} = \mathbb{G}$$

- The generator of $\mathbb{G}$ is g

$$N = 7 \Rightarrow \mathbb{Z}_N^* = \{1, 2, 3, 4, 5, 6\}$$

- $g = 2 \Rightarrow \{2^0, 2^1, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4, \mathbf{1}, \mathbf{2}, \mathbf{4}\}$
- $g = 3 \Rightarrow \{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} \equiv \mathbb{G}$
- $g = 4 \Rightarrow \{4^0, 4^1, 4^2, 4^3, 4^4, 4^5\} = \{1, 4, \mathbf{1}, \mathbf{4}, \mathbf{1}, \mathbf{4}\}$
- $g = 5 \Rightarrow \{5^0, 5^1, 5^2, 5^3, 5^4, 5^5\} = \{1, 4, 5, 6, 2, 3\} \equiv \mathbb{G}$
- $g = 6 \Rightarrow \{6^0, 6^1, 6^2, 6^3, 6^4, 6^5\} = \{1, 6, \mathbf{1}, \mathbf{6}, \mathbf{1}, \mathbf{6}\}$

Cyclic Groups: generator

The group generated by g

$$< \mathrm{g} >= \{g^0, g^1, g^2, \ldots \ldots\}$$

Defines a sub-group of $\mathbb{Z}_N$

- The order of $< g >$ is the smallest a s.t.

$$g^a = 1 \text{ in } \mathbb{Z}_N$$

- $|< 3 >| = 6 \; in \; \mathbb{Z}_7$
- $|< 2 >| = 3 \; in \; \mathbb{Z}_7$

- Prime order groups ⇒ **all elements are generators**
- Identity: cannot be a generator!

N.B. $g^{|\mathbb{Z}_N|} = 1$ in $\mathbb{Z}_N$

Cyclic Groups: order

For an integer N define

- $\varphi(N) = |\mathbb{Z}_N^*| \Rightarrow$ Euler's φ totient function

What about $\varphi(N)$ value?

- N prime: $\varphi(N) = N - 1$
- $\boldsymbol{N = p * q}$: $\varphi(N) = (p-1) * (q-1)$
- $\boldsymbol{N = \prod_i p_i^{e_i}}$: $\varphi(N) = \mathrm{N} * \prod_i (1 - \mathrm{p_i^{-1}})$

- $\forall x \in \mathbb{Z}_N^* \Rightarrow x^{\varphi(N)} = 1$ in $\mathbb{Z}_N^*$ → Euler Thm.
- $\forall x \in \mathbb{Z}_N^* \Rightarrow x^i$ in $\mathbb{Z}_N^* = x^{i \, mod \varphi(N)}$

RSA exploit such properties!

Cyclic Groups: finding primes

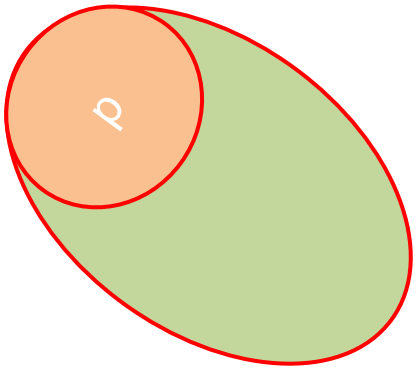
Taking a prime modulus

- $\varphi(p) = p - 1$
- $\forall x \in \mathbb{Z}_p^* \Rightarrow \boldsymbol{x^{\varphi(N)} = x^{p-1} = 1}$ in $\mathbb{Z}_p^*$

Fast generation of a prime of $\ell - bits$

- Choose a random $x \in \{-2^{\ell}, 2^{\ell+1} - 1\}$
- Compute $y = 2^{x-1}$ in $\mathbb{Z}_p$
- If $y = 2^{x-1} = 1$ in $\mathbb{Z}_p \Rightarrow \boldsymbol{x\ is\ prime}$
- Warning

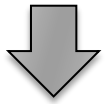
  $P[x\ not\ prime] < 2^{-60}$
- ~ 100 iterations



Linear Equations

The following equation can be solved

$$ax + b = 0 \text{ in } \mathbb{Z}_N$$



$$ax = -\mathrm{b} \cdot a^{-1} \text{ in } \mathbb{Z}_N$$

Still inverse computation needed

- $3x + 2 = 7$ in $\mathbb{Z}_{19}$
- $x = 5 \cdot 3^{-1}$ in $\mathbb{Z}_{19}$
- $ExtendedGCD[3, 19] = \{1, \{-6, 1\}\}$
- $x = 5 \cdot -6$ in $\mathbb{Z}_{19} \Rightarrow x = 8$

Euclid Algorithm

Runs on linear time $o(N)$

- Recursively compute module between operands

```
def gcd(a, b):
    if (b|a):
        return b
    else:
        return gcd(b, a % b)
```

gcd(1970, 1066) ⇒ gcd(1066, 904)
gcd(904, 162) ⇒ gcd(162, 94)
gcd(94, 68) ⇒ gcd(68, 26)
gcd(26, 16) ⇒ gcd(16, 10)
gcd(10, 6) ⇒ gcd(6, 4)
gcd(4, 2) ⇒ gcd(2, 0)

Extended Algorithm

- Compute $a = qb + r$
- Resolve $a \cdot X + b \cdot \mathrm{Y} = \gcd(\mathrm{a}, \mathrm{b})$

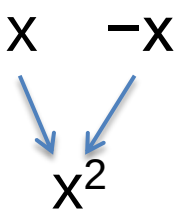
Quadratic Residue

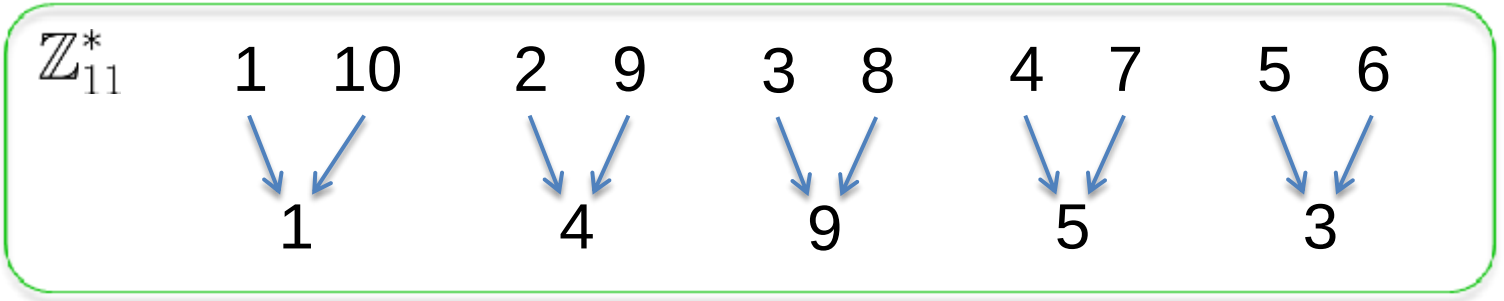
Given $\boldsymbol{p}$ prime $\Rightarrow \gcd(2, p-1) = 2$

- $p-1$ is even

Define quadratic residue the element $y \in \mathbb{Z}_p^*$:

- If $\exists x \in \mathbb{Z}_p^*$ s.t. $x^2 = y \; mod p$
- In $\mathbb{Z}_{\boldsymbol{p}}^* \Rightarrow f(x): x \longrightarrow x^2$ is one-way
- x in $\mathbb{Z}_{\boldsymbol{p}}$ is Q.R. if $x^{\frac{1}{2}}$ is computable in $\mathbb{Z}_{\boldsymbol{p}}$





Quadratic Residue

If $\boldsymbol{p}$ is prime

- Set of Q.R. is a sub-group of $\mathbb{Z}_p^*$
  - $\mathbb{QR}_p \subset \mathbb{Z}_{\boldsymbol{p}}^*$

The square modulo p is two-to-one function:

- $\left|\mathbb{QR}_p\right| = \frac{\left|\mathbb{Z}_{\boldsymbol{p}}^*\right|}{2} = \frac{p-1}{2}$

Strategic choice:

- Get a prime $\boldsymbol{q}$
- If $\boldsymbol{p} = \boldsymbol{2} * \boldsymbol{q} + \boldsymbol{1}$ is also prime $\Rightarrow \boldsymbol{p}$ is strong prime

$$\left|\mathbb{QR}_p\right| = \frac{\left|\mathbb{Z}_{\boldsymbol{p}}^*\right|}{2} = \frac{p-1}{2} = \frac{2*q}{2} = q$$

Quadratic Residue

1. Take
   $\boldsymbol{q = 5}$ ⇒ It's a prime

2. Compute
   $\boldsymbol{p = 2 * q + 1 = 11}$ ⇒ It's a prime! Not so strong…

3. Cyclic group
   $\mathbb{Z}_{11}^{*} = \{1,2,3,4,5,6,7,8,9,10\} \Rightarrow |\mathbb{Z}_{11}^{*}| = 10$

4. Sub-group
   $\mathbb{QR}_{11} = \{1,3,4,5,9\} \Rightarrow |\mathbb{QR}_{11}| = 5$ ⇒ Prime order $\boldsymbol{q}$!

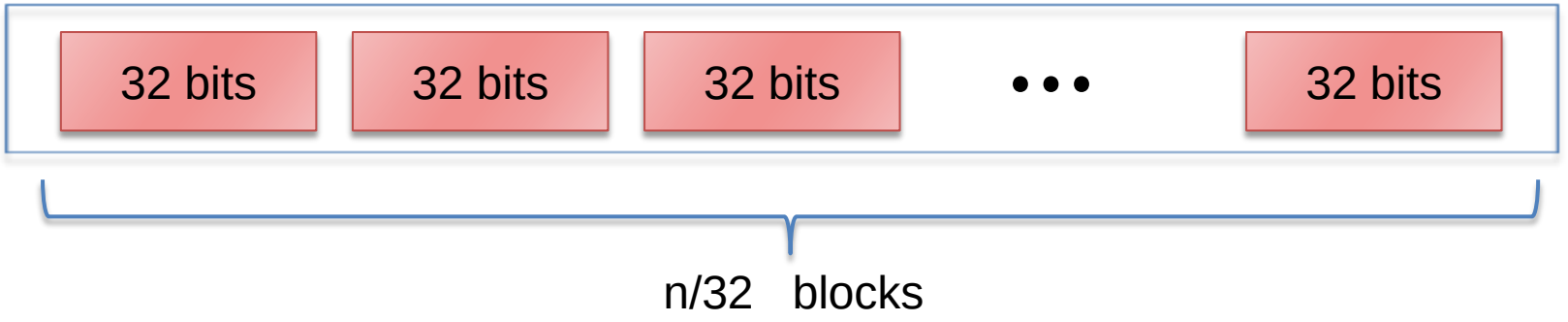
All elements except the identity are generators!

Big Numbers

Representing big numbers

- How to represent $n - \text{bits}$ $(n \gg 1)$ values?
- Modern architectures:
  - 32 bits
  - 64 bits
  - 128 bits

Combine more registers…



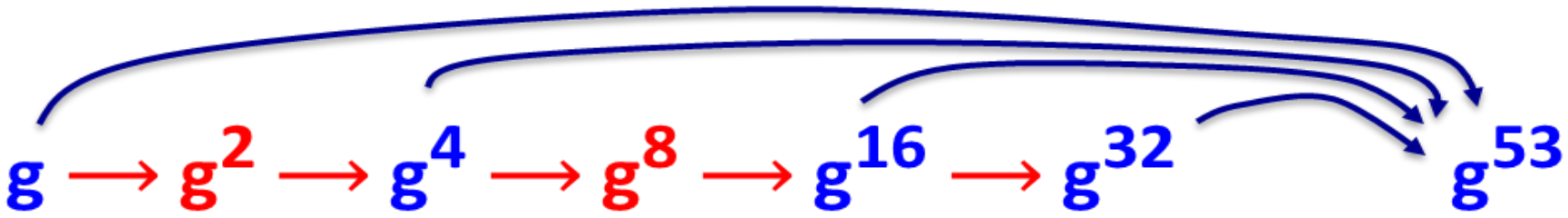
Big Numbers

Given an n-bits integer N

- Sum in $\mathbb{Z}_N$: $\boldsymbol{T_+ = O(n) \Rightarrow linear}$
- Multiplication in $\mathbb{Z}_N$: $\boldsymbol{T_* = O(n^2)}$
- Division in $\mathbb{Z}_N$: $\boldsymbol{T_\div = O(n^2)}$
- Exponentiation in $\mathbb{Z}_N$: $\boldsymbol{T_{exp} < O(log(n) * n^2)}$

Efficiently compute exponentiation:

- $x = 53 = (110101)_2 = 32 + 16 + 4 + 1$
- $g^{53} = g^{32} * g^{16} * g^4 * g^1$



Number Theory

Hard Problems

Easy Problems

Given modulo N and $x \in \mathbb{Z}_N$

- Find x^{-1} in $\mathbb{Z}_N$
  - Use Extended Euclid Algorithm!

Given prime p and polynomial $f(x)$ in $\mathbb{Z}_N$

- find x in $\mathbb{Z}_p$ s.t. $f(x) = 0$ in $\mathbb{Z}_p$
  - Need to solve the equation in $\mathbb{Z}_p$
  - Running time is linear in $deg(f)$

… but many other problems are difficult

Hard Problems

Integer Factoring

- RSA

Discrete Logarithm

- Computational Diffie Hellman
- Decisional Diffie Hellman

Groups product

Pairings

Lattices

Many others….

Factoring Problem

Gauss - 1805

"The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic."

Given p, q primes compute the composite $\boldsymbol{N = p * q}$

- Fatoring N is hard ⇒ NOT impossible ⇒ No teorethic!

It depends on $\boldsymbol{p, q}$ generation

- Length
- Randomness
- Distance between $\boldsymbol{p, q}$

Many algorithms to solve the factoring problem

- All of that can't factor well generated big N

RSA Assumption

Assumed that the factorization of $N = p \cdot q$ is hard

Given N and not knowing p or q:

- It's hard to compute $\varphi(N) = (p-1)(q-1)$

Euler Theorem not exploitable:

- $x^i \, mod N = x^{i \, mod \varphi(N)}$
- $x^{i^{-1}} \, mod N = x^{i^{-1} \, mod \varphi(N)}$

Build a trapdoor based on such assumption!

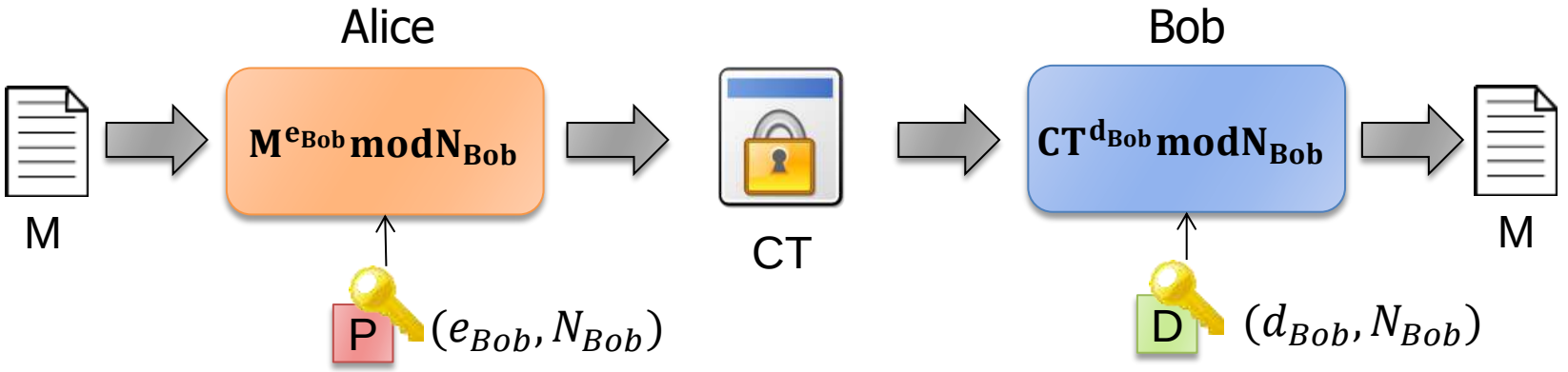
RSA

1. Find big primes: $\boldsymbol{p}$ and $\boldsymbol{q}$
2. Compute the modulo: $\mathbf{N} = \mathrm{p} \cdot \mathrm{q}$
3. Compute the order: $\boldsymbol{\varphi(N)} = (p-1)(q-1)$
4. Find a random: $\boldsymbol{e} \in \mathbb{Z}_N^*$ s.t. $\gcd\big(e,\ \varphi(N)\big) = 1$
5. Compute: $\boldsymbol{d} = e^{-1} mod\ \boldsymbol{\varphi(N)} \Rightarrow d^{-1} \cdot e = 1$

Obtained two pairs:

- $< d, \mathrm{N} > \Longrightarrow$ Private Key
- $< e, N > \Longrightarrow$ Public Key

Textbook RSA



Compare RSA vs Symmetric Security:

Key Size	Modulus Size
80 bits	1024 bits
128 bits	3072 bits
256 bits	15360 bits

Textbook RSA is insecure

Textbook RSA encryption:

- Public key: (N,e)
- Private key: (N,d)
- Encrypt: $c \leftarrow m^e$
- Decrypt: $c^d \longrightarrow m$

Insecure cryptosystem

- Not semantically secure and many attacks exist

The RSA is a trapdoor not an encryption scheme

- Recovery of encrypted message
  - Padded RSA for encryption: PKCS1, OAEP
- Common modulus attack
  - Use different modulus for different pairs

Discrete Logarithm Problem

Fixed a prime $p > 2$ and g in $\mathbb{Z}_p^*$ of order q:

- Consider the function: y $= g^x$ in $\mathbb{Z}_p$
- Now, consider the inverse function: $x = log_g(y) = log_g(g^x)$
- It's hard to compute for some $\mathbb{Z}_p$ cyclic groups

Computing discrete log of g^x is hard

- Because no efficient algorithm exists
- Same as factoring ⇒ No teorethic!
- Hardness depends on the selection of $\mathbb{G}$

in $\mathbb{Z}_{11}$:	1,	2,	3,	4,	5,	6,	7,	8,	9,	10
$log_2(\cdot)$:	0,	1,	8,	2,	4,	9,	7,	3,	6,	5

Diffie-Hellman Assumption

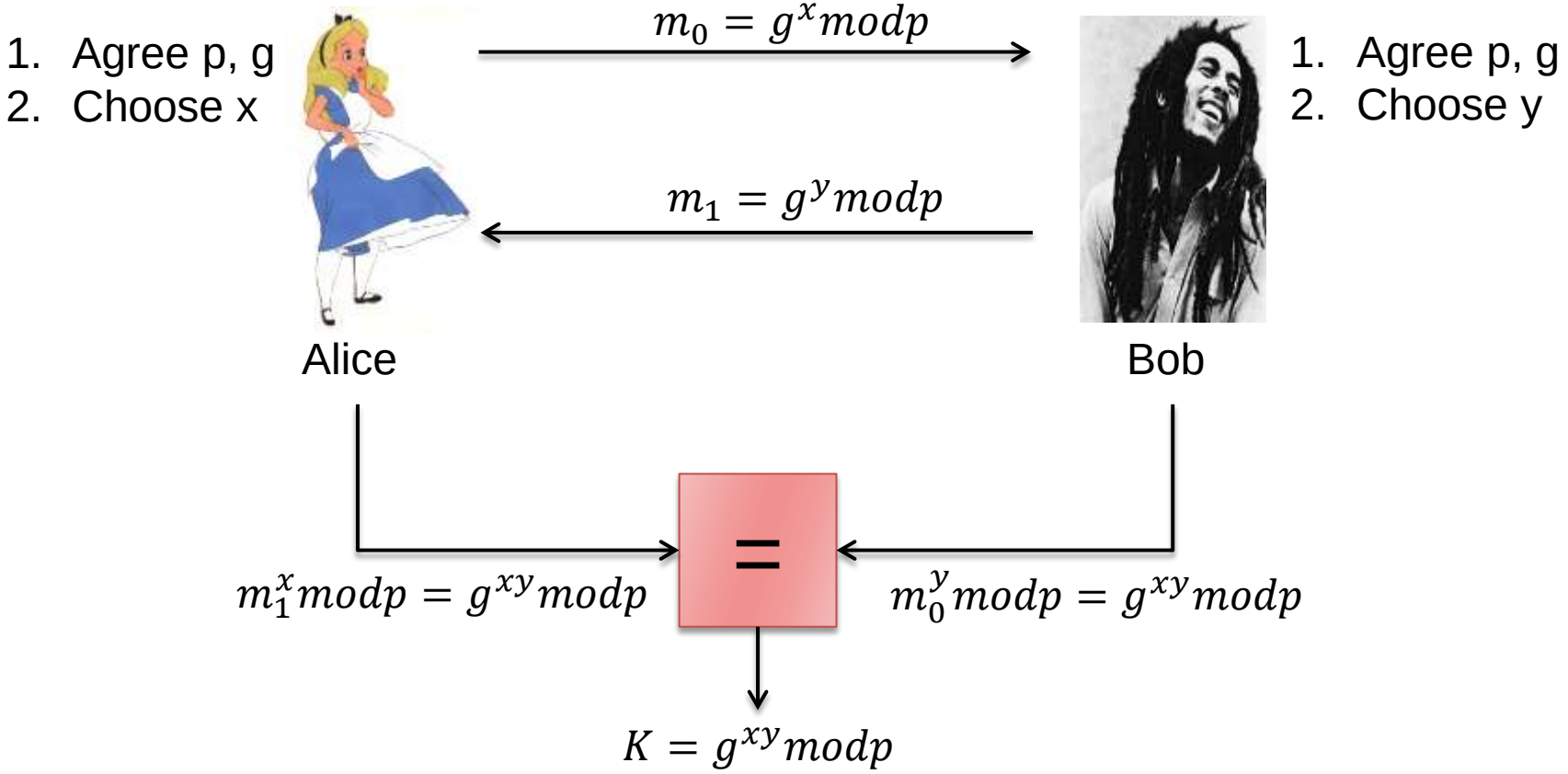
Computational DH (CDH)

- Given $\mathbb{G}$ cyclic group with generator g
- Observing only $\mathrm{T}_{CDH} = (g, g^a, g^b)$
- It's hard to compute: $\mathrm{h} = g^{\mathrm{ab}} \neq g^a \cdot g^b$
- e.g. *DH Key Exchange*

Decisional DH (DDH)

- Given $\mathbb{G}$ cyclic group with generator g
- Given $\mathrm{T}_{\mathrm{DDH}} = (g^a, g^b, g^c) \overset{ex}{\rightarrow} (g^a, g^b, g^{ab})$
- The tuple $\mathrm{T}_{\mathrm{DDH}}$ looks random in $\mathbb{G}$
- Elements of $\mathrm{T}_{\mathrm{DDH}}$ undistiguishable
- e.g. El-Gamal Encryption

Diffie-Hellman Key Exchange



Strong Primes

Strong primes generates special groups

- All elements except the identity are generators!

RSA Cryptosystems:

- Improve the factoring hardness of the system
- Gives sub-group where all elements has an inverse!

DH Cryptosystems:

- Discrete-Log problem hardest in prime-order groups
- Gives sub-group where all elements are generator!