Modular Arithmetic

1. Intro · $a / b = q$ remainder r → { a = dividend, b = divisor, q = quotient, r = remainder

$\Downarrow$

$a \bmod b = r$

$\Downarrow$

$a \bmod b = r \iff a \bmod b = (a + k \cdot b) \bmod B$ for any k

Ex: $3 \bmod 10 = 3$ $\quad 23 \bmod 10 = 3$

$13 \bmod 10 = 3$

2. Congruence modulo ($\equiv$)

$A \equiv B \bmod C \Rightarrow$ { A, B are in the same equivalence class, $\bmod C$ = operation

$\Downarrow$

$A \bmod C = B \bmod C \iff C \mid (A - B) \iff A = B + k \cdot C \; ; \; k \in \mathbb{Z}$

Obs $\equiv$ is an equivalence relation $\Rightarrow$ {
- $A \equiv A \bmod C$
- $A \equiv B \bmod C \Rightarrow B \equiv A \bmod C$
- $A \equiv B \bmod C \; ; \; B \equiv D \bmod C \Rightarrow A \equiv D \bmod C$

• Modular addition

$$\begin{cases} A + B \bmod C = (A \bmod C + B \bmod C) \bmod C \\ A - B \bmod C = (A \bmod C - B \bmod C) \bmod C \end{cases}$$

• Modular multiplication

$$A \cdot B \bmod C = (A \bmod C \cdot B \bmod C) \bmod C$$

• Modular exponentiation

$$A^B \bmod C = (A \bmod C)^B \bmod C$$

$a \equiv b \bmod n \Rightarrow a^k \equiv b^k \bmod n \quad \forall k \in \mathbb{N}$

Modular inverse $\begin{cases} \text{modinv}(A \bmod c) = A^{-1} \\ (A \cdot A^{-1}) \equiv 1 \bmod c \\ \text{! only } m \text{ coprime with } c \text{ have modinv !} \end{cases}$

- The euclidean algorithm → finds $GCD(a, b)$

1. $\begin{cases} \text{if } a == 0 \Rightarrow GCD(a,b) = b \\ \text{if } b == 0 \Rightarrow GCD(a,b) = a \end{cases}$
2. $A = B \cdot Q + R \Leftrightarrow$ calc $A \bmod B = R$
3. $GCD(B, R) = GCD(A, B)$

More properties

$\left.\begin{array}{l} \text{if } a \equiv b \bmod n \\ c \equiv d \bmod n \end{array}\right\} \Rightarrow \begin{cases} a+c \equiv b+d \bmod n \\ ac \equiv bd \bmod n \end{cases}$

if $a \equiv b \bmod n \Rightarrow -a \equiv -b \bmod n$

if $gcd(k, n) = 1$ and $ka \equiv kb \bmod n \Rightarrow a \equiv b \bmod n$

if $a_1 \equiv b_1 \bmod n$; $a_2 \equiv b_2 \bmod n$

$a_1 + a_2 \equiv b_1 + b_2 \bmod n$

$a_1 a_2 \equiv b_1 b_2 \bmod n$

$p(a) \equiv p(b) \bmod (n)$; p = polynomial

T Fermat's little theorem : p = prime ; $p \nmid a \Rightarrow a^{p-1} \equiv 1 \bmod p$

$\Rightarrow a^{-1} \equiv a^{p-2} \bmod p$

T Wilson's theorem p = prime $\Leftrightarrow (p-1)! \equiv p-1 \bmod p$

Quadratic residual : $a = QR$ if $\exists\, x \in \mathbb{Z}$ s.t. $x^2 \equiv a \bmod n$.

if p = odd prime $\Rightarrow a = QR \Leftrightarrow a^{(p-1)/2} \equiv 1 \bmod p$

An Introduction to mathematical cryptography

Chapter 1 – Intro to crypto

1.1. Simple substitution cyphers

$A, \mathbb{A} \Rightarrow f: A \to B$, f = substitution function

Cryptanalysis : Given A = alphabet $\Rightarrow 26! > 10^{26}$ different substit cyphers

Hard to break? No → Letters are not random ⇒ probability breaks it

1.2 Divisibility & GCD

$$\begin{cases} a|b,\ b|c \Rightarrow a|c \\ a|b,\ b|a \Rightarrow a = \pm b \\ a|b,\ a|c \Rightarrow a|(b+c);\ a|(b-c) \end{cases}$$

$$a = b \cdot q + r;\ 0 \le r < b$$
$$\text{if } d|a, d|b \Rightarrow d|r \\ e|b,\ e|r \Rightarrow e|a \Big\} \Rightarrow \gcd(a,b) = \gcd($$

Euclidean algo ⇕

! Euclidean algo has $O(2\log_2 b + 2)$ iterations

Extended Euclidean algorithm $\gcd(a,b) = au + bv$ → lin comb of a

if (u_0, v_0) is a solution ⇒ $u = u_0 + \frac{b \cdot k}{\gcd(a,b)}$; $V = v_0 - \frac{a \cdot k}{\gcd(a,b)}$

Def $a, b \in \mathbb{Z}$; a, b are relatively prime $\Leftrightarrow \gcd(a,b) = 1$

!obs Any equation $Au + Bv = \gcd(A,B)$ can be reduced to a case of relatively prime ns: $\frac{A}{\gcd(A,B)} \cdot u + \frac{B}{\gcd(A,B)} V = 1$

1.3 Modular Arithmetic $a \equiv b \bmod m \iff m \mid (a-b)$

Prop

$$\left.\begin{array}{l} a_1 \equiv a_2 \bmod m \\ b_1 \equiv b_2 \bmod m \end{array}\right\} \Rightarrow \begin{array}{l} a_1 \pm b_1 \equiv a_2 \pm b_2 \bmod m \\ a_1 b_1 \equiv a_2 b_2 \bmod m \end{array}$$

; $a \cdot b \equiv 1 \bmod m \iff \gcd(a, m) = 1$ (2) → mod inv - Unique

Proof for (2)

a) Suppose $\gcd(a, m) = 1 \Rightarrow \exists u, v$ s.t. $au + mv = 1 \iff au - 1 = -mv \Rightarrow$

$m \mid au - 1 \Rightarrow au \equiv 1 \bmod m$; take $b = u$

b) Suppose $\exists\, b$ s.t. $a \cdot b \equiv 1 \bmod m \Rightarrow ab - 1 = c \cdot m$; $c \in \mathbb{Z} \Rightarrow \gcd(a, m) \mid ab - c$

$\Rightarrow \gcd(a, m) = 1$

Suppose $a \cdot b_1 \equiv a \cdot b_2 \equiv 1 \bmod m \Rightarrow b_1 \equiv b_1 \cdot 1 \equiv b_1 \cdot a \cdot b_2 \equiv b_1 \cdot a \cdot b_2 \equiv 1 \cdot b_2 \equiv b_2 \bmod m$

$\Rightarrow b$ is unique

Def $\mathbb{Z}/m\mathbb{Z} = \{0, 1, \dots, m-1\}$ = ring of integers modulo m

$(\mathbb{Z}/m\mathbb{Z})^* = \{a \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a, m) = 1\}$

Euler's totient fct = How many ms have inverses

Not $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$; if m is prime $\Rightarrow \varphi(m) = m - 1$

1.4 Prime numbers, factorization & fields

T Let $a \geq 2 \Rightarrow a = \prod_i p_i^{e_i}$ ← Unique ; we call $e_i = \text{ord}_{p_i}(a)$; $\text{ord}_p(1) = 0$ for all primes

Obs Ext GCD helps us calculate $a^{-1} \bmod p$:

Solve $au + pv = 1$; $u = a^{-1} \bmod p$

Def Field = commutative ring where every elem has a mult. inv.

Ex: $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$

↳ Finite $\Rightarrow$ Not $\mathbb{F}_p$

1.5 Powers and primitive roots in finite fields

T Fermat's Little theorem: p = prime, a = any int $\Rightarrow a^{p-1} \equiv \begin{cases} 1 \bmod p & \text{if } p \nmid a \\ 0 \bmod p & \text{if } p \mid a \end{cases}$

$\Rightarrow a^{-1} \equiv a^{p-2} \bmod p$

T Primitive Root Theorem: p = prime $\Rightarrow \exists\, g \in \mathbb{F}_p^*$ s.t. $\mathbb{F}_p^* = \{1, g^1 \dots g^{p-2}\}$

- g = primitive roots of $\mathbb{F}_p^*$ or generators
- order$(g) = p-1$ where order(g) = smallest k s.t. $g^k \equiv 1 \bmod p$

1.7 Symmetric & Asymmetric Ciphers

encryption: $e: \mathcal{K} \times \mathcal{M} \to \mathcal{C}$
decryption: $d: \mathcal{K} \times \mathcal{C} \to \mathcal{M}$
$\Rightarrow d(k, e(k, m)) = m$

- Kerckhoffs' principle: cryptosystem depends on secrecy of key, not algorithm

1. $\forall k, m \in \mathcal{K}, \mathcal{M} \Rightarrow e_k(m)$ = easy
2. $\forall k, dec \in \mathcal{K}, c \Rightarrow d_k(c)$ = easy
3. Given $c_1 \dots c_n \in C \Rightarrow$ diff to compute $d_k(c_1) \dots d_k(c_n)$ w/o $k \in \mathcal{K}$
4. Given $(m_1, c_1) \dots (m_n, c_n) \Rightarrow$ diff to decrypt (m, c) w/o $k \in \mathcal{K}$
5. Any $m_1 \dots m_n \in \mathcal{M}$, $e_k(m_1) \dots e_k(m_n)$ CHOSEN $\Rightarrow$ diff to decrypt c that is not chosen w/ k

! Obs If we view elems of $\mathcal{M}$ as consisting of blocks $\Rightarrow$ we can decrypt blo

$\mathcal{K} = \{k \in \mathbb{Z} \mid 0 \le k \le 2^{Bk}\}$

$\mathcal{M} = \{m \in \mathbb{Z} \mid 0 \le m \le 2^{Bm}\}$

C - ——

- Sym Ciphers

① $e_k(m) = k\,m \bmod p$
$d_k(c) = k' \cdot c \bmod p$
$\Rightarrow$ Given c and $m \Rightarrow \exists\, k$ s.t. $e_k(m) = c$
$k = m^{-1} c \bmod p \Rightarrow (m, c)$ gets $k \Rightarrow$
$\Rightarrow$ BAD

② $e_k(m) = m + k \bmod p$

$d_k(c) = c - k \bmod p$

③ $e_k(m) = k_1 m + k_2 \bmod p$

$d_k(m) = k_1' \cdot (c - k_2) \bmod p$

④ $e_k(m) = k \oplus m$

$d_k(c) = k \oplus c$

if k is used more than once =>

$c \oplus c' = (k \oplus m) \oplus (k \oplus m') = m \oplus m' \Rightarrow$ BAD

- **Random bit Sequences**

Let $R: \mathbb{Z}_2 \times \mathbb{Z} \to \{0,1\}$

⇓

turn k into a sequence of bits $R(k_1)$...

⇓

use sequence as a one time pad

1. $\forall k \in \mathbb{Z}, \forall j \in \mathbb{Z} \Rightarrow R(k,j)$ = easy
2. Given arbitrarily long seq $j_1 \dots j_n$ and all $R(k j_1) \dots R(k j_n) \Rightarrow$ hard to det k
3. Given any $(j_1 \dots j_n)$ and $R \dots R \Rightarrow$ hard to guess $R(k_j)$

- **Asymmetric ciphers** $k = (k_{priv}, k_{pub})$; $d_{k_{priv}}(e_{k_{pub}}(m)) = m$

Exercices:

1.19 $g^a \equiv 1 \bmod m$

$g^b \equiv 1 \bmod m$

Prove $g^{gcd(a,b)} \equiv 1 \bmod m$

$gcd(a,b) = ua + vb \Rightarrow (g^a)^u (g^b)^v = 1^u \cdot 1^v \equiv 1 \bmod p$

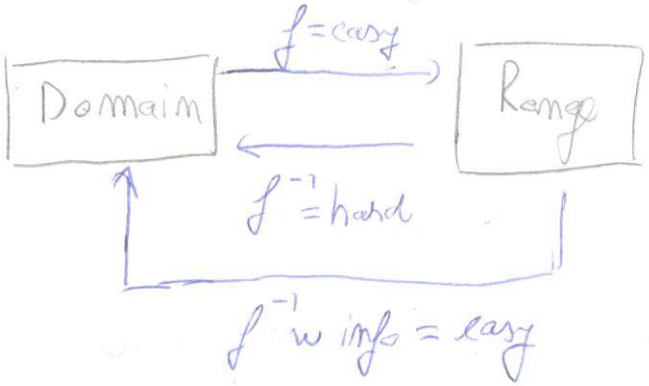
1.22 $m \in \mathbb{Z}$

$m \equiv 1 \bmod b \Rightarrow \frac{m-1}{b} \in \mathbb{Z} \Rightarrow b \frac{m-1}{b} = m - 1 \equiv -1 \bmod m \;/ \cdot(-1) \Rightarrow b \frac{1-m}{b} \equiv 1 \bmod m$

? $x \in \overline{1, m-1}$, $x = b^{-1} \bmod m$? $/ \Rightarrow \frac{1-m}{b} + m = \frac{1 + b - 1m}{b} \in \mathbb{Z} \Rightarrow$ ($\frac{1-m}{b} < 0$)

$\Rightarrow b \underbrace{\frac{1+(b-1)m}{b}}_{b^{-1}} = 1 \bmod m$

Chapter 2 Diffie-Hellman



→ PKC

Discrete Log Problem find x s.t. $g^x \equiv h \bmod p$ where $\begin{cases} g = \text{primitive root} \\ h = \text{non-zero} \end{cases}$

$x = \log_g(h)$

Obs. • if there is a solution ⇒ there are infinite: $g^{p-1} \equiv 1 \bmod p$ ⇒

$\Rightarrow g^{x+k(p-1)} = g^x \cdot g^{k(p-1)} \equiv h \cdot 1^k \equiv h \bmod p \Rightarrow$

⇒ $\log_g(h)$ is defined by adding or subtracting $k(p-1)$ ⇒

$\Rightarrow \log_g : \mathbb{F}_p^* \to \mathbb{Z}/(p-1)\mathbb{Z}$

• $\log_g(ab) = \log_g(a) + \log_g(b)$; $\forall a, b \in \mathbb{F}_p^*$

Diffie-Hellman key exchange

Problem: key exchange when communication is insecure

Algorithm

1. public: choose large prime p
   -11- g with large prime order
2. private:
   A: secret a ⇒ $A \equiv g^a \bmod p$
   B: -11- b ⇒ $B \equiv g^b \bmod p$

3. public: exchange A & B
4. $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \bmod p$

BUT g^{ab} = shared info ⇒

⇒ the DH Problem is: ~~Given~~ Given $\left.\begin{matrix} g^a \bmod p \\ g^b \bmod p \\ p, g \end{matrix}\right\}$ Find $g^{ab} \bmod p$

The Elgamal PKC

Let $\begin{cases} p = \text{big prime} \\ g \in \mathbb{F}_p^* \text{ with large order} \end{cases}$

① Let a = secret key $\Rightarrow A \equiv g^a \bmod p$

A = public key

② Let Bob's message be $m \in (2, p)$, Let k = random $\Rightarrow \begin{cases} c_1 = g^k \bmod p \\ c_2 = m \cdot A^k \bmod p \end{cases}$ send (c_1, c_2)

③ $(c_1^a)^{-1} \cdot c_2 \equiv (g^{ak})^{-1} \cdot m A^k \equiv (g^{ak})^{-1} \cdot m (g^{ak}) \equiv m \bmod p$

Group Theory

Def: smallest d s.t. $a^d = e$ is called **order of a**

Prop: Let G be finite $\Rightarrow \forall a \in G$, $\text{ord}(a)$ is finite.

If $a^k = e \Leftrightarrow \text{ord}(a) \mid k$

T Lagrange: G = fin group, $a \in G \Rightarrow$ Order of G : $\text{ord}(a) \mid |G|$

~~Let~~ Collision Algo for DLP $g^x = h \to O(N)$ with multiplication by g.

Shanks baby-step-giant-step $O(\sqrt{N} \log N)$ time, $O(\sqrt{N})$ storage; $N = \text{ord}(g)$ ~~$|G|$~~

1. Let $n = 1 + \lfloor \sqrt{N} \rfloor$
2. List 1 $= e, g \dots g^n$

   List 2 $= h, h \cdot g^{-n} \dots h \cdot g^{-n^2}$
3. Find a match $g^i = h g^{-jn}$
4. $x = i + jn$ solution

Chinese remainder theorem

T Let $m_1 .. m_k$ be a collection of pairwise coprime integers ($\Leftrightarrow$)

$\Leftrightarrow \gcd(m_i, m_j) = 1 \quad \forall i, j = \overline{1,k} \; ; \; i \neq j$

Let $a_1 .. a_k$ be arbitrary integers

Then $\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \vdots \\ x \equiv a_k \bmod m_k \end{cases}$ has a solution $x = c$.

If c and c' are both solutions $\Rightarrow$

$\Rightarrow c \equiv c' \bmod (m_1 \cdot \ldots \cdot m_k)$

Ex: $x \equiv 2 \bmod 3 \quad (1)$

$x \equiv 3 \bmod 7 \quad (2)$

$x \equiv 4 \bmod 16 \quad (3)$

Let $x = 2$ for $x \equiv 2 \bmod 3 \Rightarrow x = 2 + 3y$

(2) $2 + 3y \equiv 3 \bmod 7 \Leftrightarrow 3y \equiv 1 \bmod 7 \;\Big|\; 3^{-1} = 5 \Leftrightarrow y \equiv 5 \bmod 7 \Big\} \Leftrightarrow$

$\Rightarrow x = 2 + 3y = 2 + 3 \cdot 5 = 17 \overset{(1)\&(2)}{\Rightarrow} x = 17 + 21z$

$3 \cdot 7$

3 $17 + 21z \equiv 4 \bmod 16 \Leftrightarrow 5z \equiv 3 \bmod 16 \Leftrightarrow z = 3 \cdot 13 \equiv 39 \equiv 7 \bmod 16$

$\Rightarrow x = 17 + 21 \cdot 7 = 164$

Composite moduli

1. if p = prime; $p \equiv 3 \bmod 4$; Let $a \in \mathbb{Z}_p$ s.t. $x^2 \equiv a \bmod p$ has a solution

$\Rightarrow b \equiv a^{(p+1)/4}$ with $b^2 \equiv a \bmod p$

2 If m is a composite module $\rightarrow$ factorize it.

Ex: $x^2 \equiv 197 \bmod 437$; $437 = 19 \cdot 23 \Rightarrow \begin{matrix} y^2 \equiv 197 \equiv 7 \bmod 19 \\ z^2 \equiv 197 \equiv 13 \bmod 23 \end{matrix} \Big\} \Leftrightarrow$

$\Rightarrow \begin{matrix} y \equiv \pm 8 \bmod 19 \\ z \equiv \pm 6 \bmod 13 \end{matrix} \Big\} \Leftrightarrow \begin{cases} x \equiv 8 \bmod 19 \\ x \equiv 6 \bmod 23 \end{cases} \Big\} \Rightarrow x \equiv 236 \bmod 437$

Pohlig-Hellman Algorithm

- In DLP $\rightarrow g^x \equiv h \bmod p$; if $x \in \mathbb{Z}_{p-1} \Rightarrow$ factorization of $p-1$ may matter
- Generally if $g \in G$; $\text{ord}|g| = N \Rightarrow g^x = h$ are determined mod $N \Rightarrow$ $\Rightarrow$ factoring may matter
- Suppose we have an algo that can solve $g^x = h$ when g and $|g| = q^l$; q prime

  Let G, $g \in G$ with $\text{ord}(g) = N = q_1^{e_1} \dots q_t^{e_t}$

  1) $1 \le i \le t$ let $\left\{ \begin{array}{l} g_i = g^{N/q_i^{e_i}} \\ h_i = h^{N/q_i^{e_i}} \end{array} \right\} \Rightarrow g_i^y = h_i \Rightarrow y = y_i = \text{solution}$

  2) CRT $\quad x \equiv y_1 \bmod q_1^{e_1}$
  $\vdots$
  $x \equiv y_t \bmod q_t^{e_t}$

- Now we solve for g and $g = q^s \Rightarrow g^{q^{e-1}}$ has order q

  ~~If~~ Let G be a group, q = prime, we know an algo that solves $g^x = h$ whenever g and $\text{ord}(g) = q$ in S_q steps

  Now let $g \in G$ with $\text{ord}(g) = q^l \Rightarrow g^x = h$ in $O(e \cdot S_q)$ steps

- $x = x_0 + x_1 q_1 + \dots + x_{e-1} q^{e-1} \Rightarrow$ ~~deter~~ find $x_0 \dots x_{e-1}$

$$h^{q^{e-1}} = (g^x)^{q^{e-1}} = \left(g^{x_0 + \dots + x_{e-1} q^{e-1}}\right)^{q^{e-1}} = (g^{x_0})^{q^{e-1}} \left(g^{q^e}\right)^{x_1 \dots x_{e-1} q^{e-2}} = (g^{q^{e-1}})^{x_0}$$

$\Rightarrow$ solve with the algorithm

Rings, Quotient rings, Poly rings

Ring: $+$ → Identity, Inverse, Associative, Commutative
$*$ → — " — — " — — " —
$+, *$ → distributive

Field = Ring and $*$ has commutative law

Def R = ring → $a, b \in R$, $b \neq 0 \Rightarrow b \mid a \Leftrightarrow \exists\, c \in R$ s.t. $a = b * c$

→ u = unit $\Leftrightarrow \exists\, v \in R$ s.t. $u * v = 1$

→ $a \equiv b \bmod m \Leftrightarrow m \mid (a - b)$

→ $m \in R$. $\bar{a} = \{a' \in R \mid a' \equiv a \bmod m\}$ $\forall a \in R$ $\Big\}$ $R/mR = \{\bar{a} \mid a \in$

= congruence class of a

= quotient

Polynomial rings

Def $R[x] = \{a_0 + \dots + a_n x^n \mid n \geq 0,\ a_1 \dots a_n \in R\}$; $\deg(a) = n$

if $a_n = 1 \Rightarrow a(x)$ = monic polynomial

Let $\mathbb{F}$ = field, $a, b \in \mathbb{F}[x]$ with $b \neq 0 \Rightarrow a = b \cdot k + r$ $\Big\{$ $k, r \in \mathbb{F}[x]$, $\deg(r) < \deg(b)$

(k: quotient, r: remainder)

Def common divisor: $d \in \mathbb{F}[x]$; $d \mid a$, $d \mid b$

GCD: $d \in \mathbb{F}[x]$; $d \mid a$, $d \mid b$, $\forall d'$, $d' \mid a$, $d' \mid b$, $d' \mid d$

Quotients of polynomial rings

- F = field, $m \in \mathbb{F}[x]$ is a non-zero polynomial $\Rightarrow \forall\, \bar{a} \in \mathbb{F}[x]/(m)$ has a unique representative r: $\Big\{$ $\deg r < \deg m$, $a \equiv r \bmod m$ $\Big\} \Leftrightarrow a = m \cdot k + r$

- Let $\mathbb{F}_p$ be a finite field, $m \in \mathbb{F}_p[x]$ be a non-zero poly of degree $d \geq 1$

Then $|\mathbb{F}_p[x]/(m)| = p^d$

- Let $\mathbb{F}$ = field, $a, m \in \mathbb{F}[x]$, $m \neq 0$. Then $\bar{a}$ is unit in $\mathbb{F}[x]/m \Leftrightarrow \gcd(a, m) = 1$

- $\mathbb{F}_p$ = field. $m \in \mathbb{F}_p[x]$, m = irreducible $\Rightarrow |\mathbb{F}_p[x]/(m)| = p^d$

$\Rightarrow \mathbb{F}_p[x]/(m)$ = field

!obs · we usually work in $\mathbb{F}_{2^d}$ rather then $\mathbb{F}_p$.

· For $\mathbb{F}_{2^d}$, $\forall \mathbb{F}_{2^e}$ with $e|d$ is a subfield of $\mathbb{F}_{p^d}$

· $\mathbb{F}$ = finite field with q elems. $\forall a \in \mathbb{F}$, $a \neq 0$; $\exists a^{-1} \Rightarrow |\mathbb{F}^*| = q - 1$

Lagrange theorem $\Rightarrow \forall a \in \mathbb{F}^*$, $\text{ord}(a) \mid q-1 \Rightarrow a^{q-1} \equiv 1 \ \forall a \in \mathbb{F}$

Chapter 3 RSA & Int factorization

Euler's formula and Rats mod pq

Ex: $m = 15 = pq$

observe $a^4 \equiv 1 \bmod 15$ for $a = \{1, 2, 4, 7, 8, 11, 13, 14\} = \{a \in \mathbb{Z}_{15} \mid \gcd(a, m)$

$a^1 \not\equiv \bmod 15$ for the rest

$a^4 = (a^2)^2 = (a^{3-1})^2 \equiv 1^2 \equiv 1 \bmod 3$ $\Rightarrow a^4 \equiv 1 \bmod 15$

$a^4 = a^{5-1} \equiv 1 \bmod 5$

I Let p, q = primes, $g = \gcd(p-1, q-1)$ $\Rightarrow a^{(p-1)(q-1)/g} \equiv 1 \bmod pq$ $\forall a, \gcd(a, pq)$

If gcd are odd primes $\Rightarrow g = 2$

RSA solves the eq $x^e \equiv c \bmod N$, e, c, N - known. But is this hard?

Prop p = prime, $e \geq 1$ s.t. $\gcd(e, p-1) = 1$ $\Rightarrow \exists d$ with $de \equiv 1 \pmod{p-1} \Rightarrow x \equiv c^d \bmod$

Proof $c \equiv 0 \bmod p$ is trivial

$c \neq 0 \bmod p \Rightarrow \exists k$ s.t. $de = 1 + k(p-1) \Rightarrow (c^d)^e \equiv c^{de} \equiv c^{1+k(p-1)} = c \cdot \underbrace{c^{(p-1)^k}}_{1} \equiv c \bmod$

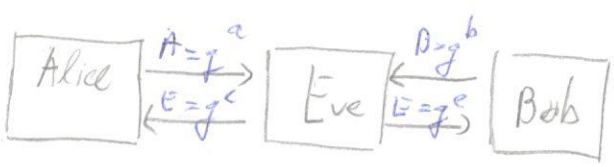
Prop p,q = distinct primes
$e \geq 1$, $\gcd(e, (p-1)(q-1)) = 1$ $\Big\}$ $\rightarrow \exists\, d$ s.t. $de \equiv 1 \bmod (p-1)(q-1) \Rightarrow$
$\Rightarrow x \equiv c^d \bmod pq$ is solution for $x^e = c \bmod pq$

RSA

Setup: p,q = primes ; $N = pq$; e, c = integers
Problem: solve $x^e = c \bmod N$
encrypt $c = m^e \bmod N$
decrypt $d \equiv e^{-1} \bmod (p-1)(q-1)$
$m = c^d \bmod N$

!obs $\rightarrow$ $d < N^{1/4} \Rightarrow$ insecure
$\rightarrow (p-1)(q-1) = N - (p+q) + 1 \Rightarrow$ if Eve finds $(p+q) \Rightarrow$ finds $(p-1)(q-1) \Rightarrow$
$\Rightarrow$ she can decrypt
$\rightarrow x^2 - (p+q)x + pq \Rightarrow$ find p & q

Man in the middle



DH key exchange

Primality testing

Def n = int ; a = witness for n if $a^n \not\equiv a \bmod n$. if $\exists$ an $a \Rightarrow n$ is not prime

Read: Miller-Rabin test

Distribution of primes : Let $\pi(x) = (\#$ of primes p, $2 \leq p \leq x)$

T Prime number Theorem $\lim_{x \to \infty} \frac{\pi(x)}{x / \ln(x)} = 1$

Pollard's p-1

Task $N = p \cdot q$, ~~det~~ $p, q = ?$
Let $L \in \mathbb{Z}$ s.t. $p-1 \mid L$, $q-1 \nmid L$
$\Rightarrow \exists\, i, j, k$ s.t.
$L = i(p-1)$
$L = j(p-1) + k$

Choose a. $a^L = a^{i(p-1)} \equiv 1 \bmod p$
$a^L = a^{j(q-1)+k} = a^k \bmod q$
$\Rightarrow k \neq 0 \Rightarrow$ ~~big~~ unlikely $a^k \equiv 1 \bmod q$
$\Rightarrow p \mid a^L - 1$, $q \nmid a^L - 1 \Rightarrow$
$\Rightarrow p = \gcd(a^L - 1, N)$

How to find L? if p^{-1} = product of many small primes $\Rightarrow p-1 \mid n! \Rightarrow$

$\Rightarrow$ For each $n = 2, 3, \ldots$ choose a and compute $\gcd(a^{n!}-1, N)$

if $\gcd(a^{n!}-1, N) \neq e \Rightarrow$ we found a non-trivial factor of N

Smooth nr's, Sieves

Def • n is called B-smooth if $\forall p$ = prime factor $\Rightarrow p \leq B$

• $\psi(x, B)$ = nr of B-smooth ~~nr~~ n s.t $1 \leq n \leq x$

I Canfield Erdös Pomerance)

Fix ~~δ~~ $0 < \varepsilon < \frac{1}{2}$, x and B increase together satisfying $(\ln x)^{\varepsilon} < \ln B < (\ln x)^{1-\varepsilon}$

Let $u = \frac{\ln x}{\ln B}$

$\Rightarrow$ $\psi(x, B) = x \cdot u^{-u(1+o(1))}$ where $f(x) = o\,g(x)$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$

How should we choose B in terms of x?

let $L(x) = e^{\sqrt{(\ln x)(\ln\ln x)}} \Rightarrow$

$\Rightarrow \forall$ fixed $0 < c < 1 \Rightarrow \psi(x\, L(x)^{c}) = x \cdot L(x)^{-(1/2c)(1+o(1))}$ as $x \to \infty$

?????

Prop let N = large int, $B = L(N)^{\frac{1}{\sqrt{2}}} \Rightarrow$ we expect to check

a) $\simeq L(N)^{\sqrt{2}}$ random nr modulo N to find $\pi(B)$ nr that are B-smooth

b) ——— of the form $a^2 \bmod N$ to find B-smooth nr to factor N

Read = Number field Sieve

Factorization via difference of squares

$x^2 - y^2 = (x+y)(x-y)$

$N = a^2 - b^2 = (a+b)(a-b) \Rightarrow$ we search for b^2 s.t $N + b^2 = a^2$

obs $k\ N = (a+b)(a-b) \Rightarrow$ probably N has ~~gcd~~ $\gcd(N, a-b) \neq 0$ or $\gcd(N, a+b) \neq 0$

Algorithm

1. Relation building → Find many $a_1 \dots a_2$ s.t $c_i = a_i^2 \bmod N$ factors as a product of small primes
2. Elimination → $c_i \cdots c_s \Rightarrow \forall p$ in product appears at an even power $= b^2$
3. $a = a_{i_1} \cdots a_{i_s} \Rightarrow \gcd(N, a-b) = d$

$a^2 = (a_{i_1} \cdots a_{i_s})^2 = c_{i_1} \cdots c_{i_s} = b^2 \bmod N \Rightarrow d \mid N \ ; d > 1$

The index calculus method for computing discrete log in $\mathbb{F}_p$

- Solve $g^x = h \bmod p$, g = primitive root in $\mathbb{F}_p$
- Rather than solving $g^x \equiv h \bmod p$ we choose B and solve

$$g^x = \ell \bmod p \text{ for all } \ell \leq B$$

- look through $h \cdot g^{-k} \bmod p$, $k = 1, 2 \dots$ until we find k s.t. $h g^{-k} \bmod p$ is B smooth $\Rightarrow$

$$h \cdot g^{-k} = \prod_{\ell \leq B} \ell^{e_\ell} \bmod p \text{ for certain } e_\ell$$

$$\Rightarrow \log_g(h) = k + \sum_{\ell \leq B} e_\ell \cdot \log_g(\ell) \pmod{p-1} \quad *$$

already done $\Rightarrow$ we have $\log_g(h)$

How to find $\log_g(\ell)$?

for random $i \Rightarrow g_i \equiv g^i \bmod p$

if g_i is B-smooth $\Rightarrow g_i = \prod_{\ell \leq B} \ell^{a_\ell(i)} \Rightarrow i = \log_g(g_i) \equiv \sum a_\ell(i) \cdot \log_g(\ell) \pmod{p-1}$ (+)

$\Rightarrow$ find $\pi(B)$ equations (+) $\Rightarrow$ solve with CRT for each $q \mid p$, q = prime

Quadratic Residues & Quadratic Reciprocity

Problem: How can we tell $a \equiv x^2 \bmod p$?

Def p = prime, $p \nmid a$, a = quadratic residue $\Leftrightarrow \exists\, c \in \mathbb{Z}_p$ s.t. $a \equiv c^2 \bmod p$

Props (*):
- QR · QR = QR
- QR · NQR = NQR
- NQR · NQR = QR

Proof: let g = generator; let $m = 2k \Rightarrow g^m \equiv$ QR

let $m = 2k+1 \Rightarrow g^m = c^2 \bmod p$?

$c^{p-1} \equiv 1 \bmod p \Leftrightarrow c^{p-1} \equiv (c^2)^{\frac{p-1}{2}} \equiv g^{m\left(\frac{p-1}{2}\right)} \equiv g^{2k+1\left(\frac{p-1}{2}\right)} \equiv g^{k(p-1)} \cdot g^{\frac{p-1}{2}} \bmod p$

$\Rightarrow g^{\frac{p-1}{2}} \equiv 1 \bmod p$ FALSE since g = generator (the left side $\equiv 1$)

$\Rightarrow g^m = \begin{cases} \text{QR if } m \text{ even} \\ \text{NQR if } m \text{ odd} \end{cases} \Rightarrow (*)$

$\Rightarrow \left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a = \text{QR} \\ -1 & \text{if } a = \text{NQR} \\ 0 & \text{if } p \mid a \end{cases}$ Legendre symbol

Let p, q = odd primes

$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4 \end{cases} \quad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \bmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \bmod 8 \end{cases}$

$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \bmod 4 \text{ or } q \equiv 1 \bmod 4 \\ \left(\frac{q}{p}\right) & \text{if } p \equiv 3 \bmod 4 \text{ or } q \equiv 1 \bmod 4 \end{cases} \Rightarrow$ Tells us if $x^2 \equiv p \bmod q$ is square modulo q

Jacobi symbol

$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_t}\right)^{e_t}$ where $b = p_1^{e_1} \cdots p_t^{e_t}$

Goldwasser-Micali Cryptosystem

$e(m_1, r) = c_1$ = cyphertext for m_1 with a random r

Algorithm

1. Key choose p, q
   a with $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$
   $N = pq$
2. Encryption: $m \in \{0,1\}$
   r ~~with~~ $1 < r < N$

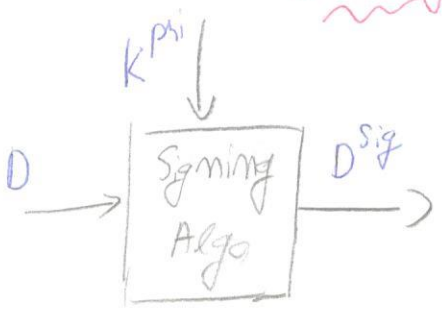
$$c = \begin{cases} r^2 \% N & \text{if } m = 0 \\ a\, r^2 \% N & \text{if } m = 1 \end{cases}$$

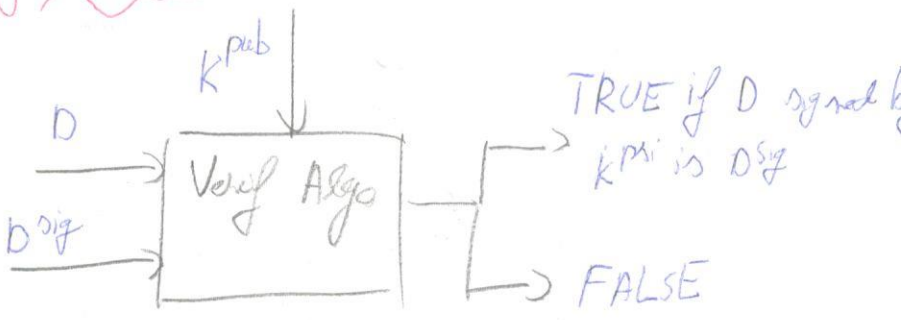
3. Decrypt: $m = \begin{cases} 0 \text{ if } \left(\frac{c}{p}\right) = 1 \\ 1 \text{ if } \left(\frac{c}{p}\right) = -1 \end{cases}$

$$\left(\frac{c}{p}\right) \begin{cases} \left(\frac{r^2}{p}\right) = \left(\frac{r}{p}\right)^2 = 1 & \text{if } m = 0 \\ \left(\frac{a r^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{r}{p}\right)^2 = \left(\frac{a}{p}\right) = -1 & \text{if } m = 1 \end{cases}$$

---

4. Digital signatures





!dss. verif algo doesn't have K^{pri} !

- Given K^{pub} an attacker can't det K^{pri} nor can she det any other private key that produces the same sign
- Given K^{pub} and a list of $D_1 .. D_n$ with $D_1^{sig} .. D_n^{sig}$ an attacker can't det a valid sign on a document ~~except them~~ that is not in $D .. D_n$

RSA DS

Algorithms

- Key creation: p, q primes
  Verif exp e
  $\gcd(e, (p-1)(q-1))$
  let: $N = pq$, e
- Signing: compute d, $de \equiv e \bmod (p-1)(q-1)$
  Sign $S \equiv D^d \bmod N$
- Verif $S^e \bmod N = D$

$$S^e \equiv D^{de} \equiv D \bmod N$$

Efficient if $de \equiv 1 \bmod \frac{(p-1)(q-1)}{\gcd(p-1)(q-1)}$

Elgamal Sign

- key creation: $1 \le a \le p-1$, a = sign key
  $A = g^a \bmod p$
  return A
- Signing: doc $D \bmod p$
  random $1 < k < p$
  $\gcd k(p-1) = 1$
  return $\begin{cases} S_1 \equiv g^k \bmod p \\ S_2 \equiv (D - aS_1) k^{-1} \bmod p-1 \end{cases}$
- Verif: $A^{S_1} S_1^{S_2} \bmod p = g^D \bmod p$

Proof

$$A^{S_1} S_1^{S_2} = g^{aS_1} g^{kS_2} = g^{aS_1 + kS_2} =$$
$$= g^{aS_1 + k(D-aS_1)k^{-1}} \equiv g^D \bmod p$$

DSA -> works in $\mathbb{F}_p^*$, $|\mathbb{F}_p^*| = q$

Choose p, q, $p \equiv 1 \bmod q$, g of order $q \bmod p$

- Key creation: choose $1 \le a \le q-1$, a = secret key
  return: $A = g^a \bmod p$
- Signing choose $D \bmod q$
  random $1 < k < q$
  compute $S_1 \equiv g^k \pmod p \bmod q$
  $S_2 \equiv (D + aS_1) k^{-1} \bmod q$
- Verif $V_1 \equiv DS_2^{-1} \bmod q$
  $V_2 \equiv S_1 S_2^{-1} \bmod q$
  Verif $g^{V_1} A^{V_2} \pmod p \bmod q = S_1$

Proof

$$g^{V_1} A^{V_2} \equiv g^{DS_2^{-1}} g^{aS_1 S_2^{-1}} \equiv g^{(D+aS_1)S_2^{-1}} \equiv g^k \bmod$$
$$\Rightarrow g^k \bmod p \bmod q = S_1$$

5. Combinatorics, prob & information Theory

Counting

- Permutations: S = set, $|S| = n \Rightarrow n!$ permutations
- Combinations of: k $\binom{n}{k} = \frac{n!}{k!(n-k)!} \Rightarrow$ binomial Theorem, $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

Vigenere cipher

- message, key, set of characters
- apply the key as a positional shift

Probability Theory

$[0,1]$

$Pr : \Omega \to \mathbb{R}$, Ω = sample space

- Let ω = ~~event~~ sample $\Rightarrow 0 \le Pr(\omega) \le 1 \ \forall \omega \in \Omega$; $\sum_{\omega \in \Omega} Pr(\omega) = 1$

  E = event $\subset \Omega \Rightarrow Pr(E) = \sum_{\omega = E} Pr(\omega)$
- $E \cap F \neq \emptyset \iff E$ & F are disjoint $\Rightarrow Pr(E \cup F) = Pr(E) + Pr(F)$
- if E & F are NOT disjoint $\Rightarrow Pr(E \cup F) = Pr(E) + Pr(F) - Pr(E \cap F)$
- E^c = complement $(E) \Rightarrow Pr(E^c) = 1 - P(E)$ — don't count twice
- E, F = independent $\iff Pr(E \cap F) = Pr(E) \cdot Pr(F)$
- Bayes Formula $\boxed{Pr(F|E) = \frac{Pr(F \cap E)}{Pr(E)}} \Rightarrow \boxed{Pr(F|E) = \frac{Pr(E|F) \cdot Pr(F)}{Pr(E)}}$

Monte Carlo Algorithms

Let S = set, $m \in S$, A = a property

1. $Pr(m \text{ has } A \mid \text{algo returns Yes}) = 1$
2. $Pr(\text{algo returns Yes} \mid m \text{ has prop}) \ge \frac{1}{2}$

We know ≈ how many m have A

We want to find if a fixed m has A

$Pr(m \text{ has } A \mid \text{algo returns No } N \text{ times}) \xrightarrow[N \to \infty]{} 1$

Proof Let $E = \{ m \in S \text{ doesn't have } A \}$; $P_r(E) = 0{,}01$
$F = \{$ the algo returns No N times in a row $\}$ $\Rightarrow P_r(E|F) = ?$

$$P_r(E|F) = \frac{P_r(F|E)\cdot P_r(E)}{P_r(F)} = \frac{P_r(F|E)\cdot P_r E}{P_r(F|E)P_r(E) + P_r(F|E^c)P_r(E^c)} =$$

$P_r(F|E) = ?$

$P_r(m \text{ has } A \mid YES) = P_r(No \mid m \text{ doesn't have } A) = 1 \Rightarrow P_r(F|E) = 1$

$P_r(F|E^c) = P_r(No \mid m \text{ has } A)^N = 1 - P_r(YES \mid m \text{ has } A)^n \le \left(1 - \frac{1}{2}\right)^N = \frac{1}{2^N}$

$$P_r(E) \ge \frac{1\cdot 0{,}01}{1\cdot 0{,}01 + 2^{-N}\cdot 0{,}99} = 1 - \frac{99}{2^N + 99} \xrightarrow{N\to\infty} 1$$

Random Variables

$X : \Omega \to \mathbb{R}$

- Prob density function $= f_X(x) = P_r(X = x)$
- Prob distribution fct $= F_X(x) = P_r(X \le x)$

Ex: uniform distrib: $f_X(j) = P_r(X = j) = \begin{cases} \frac{1}{N} & \text{if } j \in S \\ 0 & \text{if } j \notin S \end{cases}$

2. Binomial distrib: $f_X(k) = \binom{n}{k} p^k (1-p)^{n-k}$ → k successes

3. Hypergeometric distrib
   N balls, m red, $N-m$ blue
   n balls chosen w/o replacement
   X = number of red balls chosen

$$\Rightarrow f_X(i) = P_r(X = i) = \frac{\binom{m}{i}\binom{N-m}{n-i}}{\binom{N}{n}}$$

4 Geometric distribution
$X(\omega) = X(b_1 \dots b_i) =$ smallest i s.t. $b_i = 1$

$$\Rightarrow f_X(n) = (1-p)^{n-1} p$$

$\{X = n\} = \{\underbrace{000\dots}_{n-1} 1 b_{n+1} \dots\}$

→ # n failures until 1 success

Def: Joint density function $= f_{X,Y}(x,y) = P_r(X=x, Y=y)$

Conditional — " — $= f_{X|Y}(x|y) = P_r(X=x, Y=y)$

- X, Y independent $\Leftrightarrow f_{X,Y}(x,y) = f_X(x) \cdot f_Y(y)$
- Bayes formula $\boxed{f_{X|Y}(x,y) = \frac{f_X(x) \cdot f_{Y|X}(y|x)}{f_Y(y)}}$, if X, Y indep $\Rightarrow$ $\Rightarrow f_{X|Y}(x|y) = f_X(x)$

Expected Value (mean)

$$E(X) = \sum_{i=1}^{n} x_i \cdot f_X(x_i) = \sum x_i \cdot P(X=x_i) \rightarrow \text{Check for every distribution}$$

Collision Algorithms & MitM

The birthday paradox

$N = 40$

→ (1) what is the P_r (someone has your bday)?

→ (2) P_r (at least 2 ppl have the same bday) = ?

$$P_r(1) = 1 - P_r(\overline{1}) = 1 - \prod_{i=1}^{40} P_r(\text{i doesn't share bday}) = 1 - \left(\frac{364}{365}\right)^{40} \approx 10\%$$

$$P_r(2) = 1 - P_r(\overline{2}) = 1 - \prod_{i=1}^{40} P_r\left(\begin{matrix}\text{i does not have}\\ \text{the same bday}\\ \text{as the } i-1 \text{ ppl}\end{matrix}\right) = 1 - \prod_{i=1}^{40} \frac{365-(i-1)}{365} =$$

$$= 1 - \frac{365}{365}\cdot\frac{364}{365}\cdots\frac{326}{365} \approx 90\%$$

A Collision Theorem

T Urn has N balls → n red, $N-n$ blue

Bob samples w replacement m balls

$\Rightarrow P_r(\text{at least one red}) = 1 - \left(1 - \frac{n}{N}\right)^m \geq 1 - e^{-m \cdot n / N}$

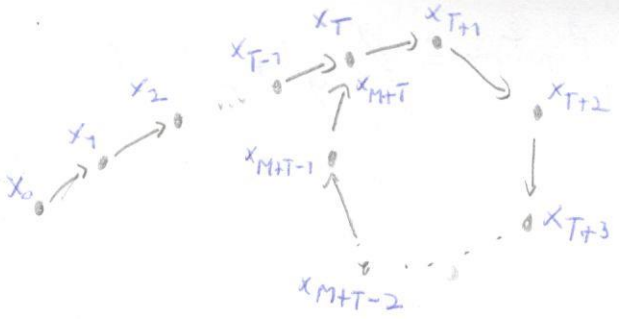
Ex: $P_r(\text{match}) \approx 99,99\%$; $n = ?$

$= 1 - 10^{-4} = 1 - e^{-n^2/N} \Rightarrow \frac{n^2}{N} = \ln 10^{-4} \Rightarrow n = \sqrt{N \ln 10^4} \approx 3\sqrt{N}$

$\Rightarrow$ $\sqrt{N}$ small time

$\sqrt{N}$ storage might be big

Pollard's ρ Method



T = tail length
M = loop length

$f: S \to S$

$x_0 = x$, $x_i = \underbrace{f \circ \cdots \circ f}_{i}(x)$

$x_0, x_1, \ldots$ = forward orbit $= O_f^+(x)$; S finite $\Rightarrow$ must be a duplicate

T = largest int s.t. x_{T-1} appears only once in $O_f^+(x)$

M = smallest int s.t. $x_{T+M} = x_T$

$\Rightarrow x_{2i} = x_i$ for some $1 \le i < T+M$

DLP $g^t = h$ in $\mathbb{F}_p^+$; let $f(x) = \begin{cases} gx & 0 \le x \le p/3 \\ x^2 & p/3 \le x < 2p/3 \\ hx & 2p/3 \le x < p \end{cases}$

$x_i = g^{\alpha_i} \cdot h^{\beta_i}$; $\alpha_{i+1} = \begin{cases} \alpha_i + 1 \ \% (p-1) \\ 2\alpha_i \ \% (p-1) \\ \alpha_i \ \% (p-1) \end{cases}$ $\beta_{i+1} = \begin{cases} \beta_i \ \% (p-1) \cup \\ 2\beta_i \ \% (p-1) \\ \beta_i + 1 \ \% (p-1) \end{cases}$

$x_{2i} = g^{\alpha_{2i}} \cdot h^{\beta_{2i}}$

$x_i = x_{2i} \Rightarrow g^{\alpha_i} h^{\beta_i} = g^{\alpha_{2i}} h^{\beta_{2i}} \Rightarrow \left.\begin{array}{l} u \equiv \alpha_i - \alpha_{2i} \ \% \ p-1 \\ v \equiv \beta_{2i} - \beta_i \ \% \ p-1 \end{array}\right\} \Rightarrow v \log_g(h) = u \ \% (p-1)$ (*)

if $\gcd(v, p-1) = 1 \Rightarrow (*) \cdot v^{-1} \Rightarrow \log_g(h) = v^{-1} u$

else let $d = \gcd(v, p-1) \Rightarrow$ use EGcd to find s s.t. $s \cdot v \equiv d \ \% (p-1)$

$(*) \cdot s \Leftrightarrow d \log_g(h) = u \cdot s \ \% (p-1) \Rightarrow$

$\Rightarrow \log_g(h) = \left\{ \frac{u \cdot s}{d} + k \cdot \frac{p-1}{d} \mid k = \overline{0 \ldots d-1} \right\}$

$d \mid p-1 \Rightarrow d \mid u \cdot s$ ~~$\Rightarrow \log_g$~~

Information Theory

Perfect secrecy: Let M, C, K be random variables, f_M, f_C, f_K = their density fct

↳ $f(m|c) = f(m)$ $\forall m \in \mathcal{M}, c \in C$

↳ *Intuition*: ciphertext gives no info about the msg

↳ Bayes $\Rightarrow f(m|c) f(c) = f(c|m) f(m) \Leftrightarrow f(c|m) = f(c)$ $\forall c \in C, m \in \mathcal{M}$, $f(m) \neq 0$

Total prob $f_C(c) = \sum_{k \in \mathcal{K} \text{ s.t. } c = e_k(m) \text{ for some } m \in \mathcal{M}} f_K(k)\, f_M(d_k(c))$

Prop if a system has perfect secrecy $\Rightarrow |\mathcal{K}| \geq |C^+|$ where $C^+ = \{m \in \mathcal{M} \mid f(m) > 0\}$ is a set of plaintexts that have a positive probability of being selected.

T $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$; The system has perf secrecy $\Leftrightarrow$

1. $\forall k \in \mathcal{K}$, k is used with equal prob.
2. For a given $m \in \mathcal{M}$ and $c \in \mathcal{C}$, $\exists!\, k \in \mathcal{K}$ that encrypts m to c

Entropy = measure of uncertainty in a system

- *Intuition*: $f_X(x) = P_r(X = x) \Rightarrow$ Entropy of X will be small if a single outcome of an experiment reveals a significant amount of information about X
- X = random var with $\{x_1 \dots x_n\}$, $\{p_1 \dots p_n\}$; $p_i = f_X(x_i) = P_r(X = x_i)$

Entropy $H(X) = H(p_1 \dots p_n)$

Properties

H1. H should be continuous in p_i (a small change in $p_i \Rightarrow$ small change in information revealed by X)

H2. X_n = uniform distrib $\left(\frac{1}{n}\right) \Rightarrow H(X_{n+1}) > H(X_n)$ $\forall n \geq 1$
(if outcomes are equally likely $\Rightarrow$ uncertainty ↑ if n ↑)

H3 If the outcome is a choice $\Rightarrow$ broken down to 2 consecutive choices

$X: \to \{x_{ij} \mid 1 < i < n;\ 1 < j < m_i\}$
$Y: \to \{z_1 \dots z_n\}$
$Z_i: \to \{x_{ij} \mid 1 < j < m_i\}$
$\Rightarrow H(X) = H(Y) + \sum_{i=1}^{n} P_r(Y = z_i) \cdot H(Z_i)$

Ex: ① Let X_n be unif distrib $\Rightarrow H(X_{n^2}) = 2H(X_n)$

View X_{n^2} as choosing an elem from $\{x_{ij} \mid 1 \le i,j \le n\} \Rightarrow$ 2 choices

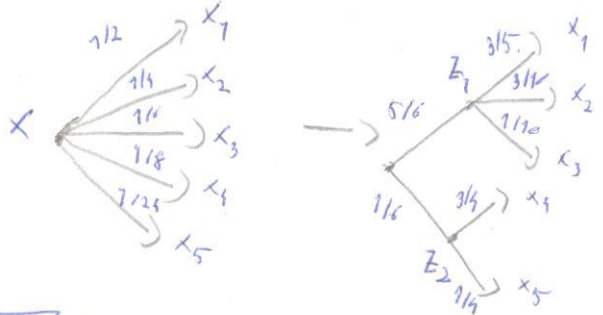
$\Rightarrow H(X_{n^2}) \overset{H_3}{=} H(X) + \sum_{i=1}^{n} \frac{1}{n} H(X_n) = 2H(X_n)$

② $X = \{x_1 \dots x_5\}$; $f_X(x_1) = \frac{1}{2}$, $f_X(x_2) = \frac{1}{4}$; $f_X(x_3) = \frac{1}{12}$, $f_X(x_4) = \frac{1}{8}$, $f_X(x_5) = \frac{1}{24}$

Let $X = \{\underbrace{x_1, x_2, x_3}_{Z_1}\} \cup \{\underbrace{x_4, x_5}_{Z_2}\} \Rightarrow f_Y(Z_1) = \frac{5}{6}$, $f_Y(Z_2) = \frac{1}{6}$

and $f_{Z_1}(x_1) = \frac{3}{5}$, $f_{Z_1}(x_2) = \frac{3}{10}$, $f_{Z_1}(x_3) = \frac{1}{10}$, $f_{Z_2}(x_4) = \frac{3}{4}$, $f_{Z_2}(x_5) = \frac{1}{4}$ $\Rightarrow$

$\overset{H_3}{\Rightarrow} H\left(\frac{1}{2}, \frac{1}{4}, \dots \frac{1}{24}\right) = H\left(\frac{5}{6}, \frac{1}{6}\right) + \frac{5}{6} H\left(\frac{3}{5}, \frac{3}{10}, \frac{1}{10}\right) + \frac{1}{6} H\left(\frac{3}{4}, \frac{1}{4}\right)$



T ∀ f having props H_1, H_2, H_3 is a constant multiple of the function

$$H(p_1 \dots p_n) = -\sum_{i=1}^{n} p_i \log_2(p_i)$$

- Intuition → if $\exists\ p_i = 1$, rest are $0 \Rightarrow H(p_1 \dots p_n) = 0 \Rightarrow$ we know for certain the outcomes
  → maximal uncertainty when all $p_i = \frac{1}{n}$ or equal

$$\Rightarrow \begin{cases} H(X) \le \log_2 n \\ H(X) = \log_2 n \iff \forall\ X = x_i \Rightarrow p_i = 1/n \end{cases} \Big| \text{ for } X = \text{finite random var}$$

Conditional entropy

$$H(X|Y) = -\sum_{i=1}^{n} \sum_{j=1}^{m} f_Y(y_j) \cdot f_{X|Y}(x_i|y_j) \log_2 f_{X|Y}(x_i|y_j)$$

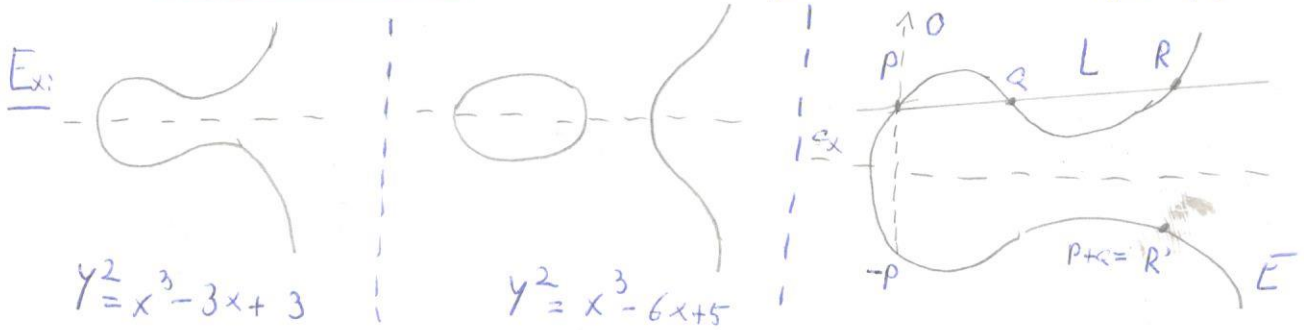
- Intuition: signal —noisy channel→ received signal
- if $X = k$, $Y = C \Rightarrow H(k|C)$ = total amount of info about the key revealed by C
- $H(K|C) = H(K) + H(M) - H(C)$

Chapter 6. Elliptic Curves Cryptography

Elliptic curves = set of solutions to an equation of the form

$y^2 = x^3 + Ax + B$ → Weierstrass equations; $4A^3 + 27B^2 \neq 0$

Ex:



$y^2 = x^3 - 3x + 3$ $\qquad$ $y^2 = x^3 - 6x + 5$

"Addition" Let E = elliptic curve; O lies on every vertical line $\qquad$ Reflection across X

Let $P \& Q \in E$; Let L = line(P,Q) $\Rightarrow E \cap L = \{P, Q, R\}$; if $R=(a,b) \Rightarrow$ sum$(P,Q) = R' = (a,-b)$

Notation: $P+Q=R$; $P=(a,b) \Rightarrow -P=(a,-b)$; $nP = \underbrace{P+\dots+P}_{n \text{ times}}$; $P+O=P$ → the zero in addition

Props

1. $P+O = O+P = P$
2. $P+(-P)=O$
3. $(P+Q)+R = P+(Q+R)$
4. $P+Q = Q+P$

$\Rightarrow (E,+)$ = abelian group

Addition algorithm: $E: y^2 = x^3 + Ax + B$; $P_1, P_2 \in E$

1. $P_1 = O \Rightarrow P_1 + P_2 = P_2$
2. $P_2 = O \Rightarrow P_2 + P_1 = P_1$
3. $P_1 = (x_1, y_1)$; $P_2 = (x_2, y_2)$
4. $x_1 = x_2$; $y_1 = -y_2 \Rightarrow P_1 + P_2 = O$
5. define $\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \frac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2 \end{cases} \Rightarrow$

λ = slope of L

$\begin{cases} y = \lambda x + v \\ v = y_1 - \lambda x_1 \end{cases}$

$\Rightarrow x_3 = \lambda^2 - x_1 - x_2$; $y_3 = \lambda(x_1 - x_3) - y_1$

Elliptic curves over finite fields

Def Let $p \geq 3 \Rightarrow$ Elliptic curve over $\mathbb{F}_p$ is $E: y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{F}_p$ and $4A^3 + 27B^2 \neq 0$

$E(\mathbb{F}_p) = \{(x,y) \mid x, y \in \mathbb{F}_p \text{ and } y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$

$(E(\mathbb{F}_p), +)$ = addition finite group

T Hasse

$|E(\mathbb{F}_p)| = p + 1 - t_p$ where $|t_p| \leq 2\sqrt{p}$; t_p = trace of Frobenius

= trace of a matrix 2×2 that acts as a linear transformation on a certain vector space associated with $E/\mathbb{F}_p$

Elliptic curve DLP

Let $E(\mathbb{F}_p)$, $P, Q \in E(\mathbb{F}_p) \Rightarrow$ ECDLP = find n s.t $\boxed{Q = nP}$

Notation: $n = \log_P(Q)$

!Obs
- $\log_P(Q)$ is not defined for all Q, P
- But in practice $Q = nP \Rightarrow$ we choose n

Def order of P is the smallest number s s.t $sP = \mathcal{O}$; $s \mid |E(\mathbb{F}_p)|$

- if n_0 = integer s.t $Q = n_0 P \Rightarrow$ solutions for $Q = nP$ are $n = n_0 + is$, $i \in \mathbb{Z} \Rightarrow$
$\Rightarrow n \in \mathbb{Z}/s\mathbb{Z}$, n is integer modulo s

Props

$\log_P(Q_1 + Q_2) = \log_P(Q_1) + \log_P(Q_2)$

!Obs $\log_P : E(\mathbb{F}_p) \to \mathbb{Z}/s\mathbb{Z}$ (group homomorphism)

Double and add algorithm

Input $P \in E(\mathbb{F}_p)$, $n \geq 1$
1. Set $Q = P$; $R = \mathcal{O}$
2. while $n > 0$
   if $n \equiv 1 \bmod 2$: $R = R + Q$
   $Q = 2Q$; $n = \lfloor n/2 \rfloor$
3. return R

$n = n_0 + 2n_1 + \dots + 2^k n_k$; $n_i \in \{0, 1\}$

$Q_i = 2^i P$

$nP = n_0 Q_0 + n_1 Q_1 + \dots + n_k Q_k$

Elliptic DH KE

- Public param creation
  Large prime p, $E(\mathbb{F}_p)$, $P \in E(\mathbb{F}_p)$
- Private
  A: $n_A \Rightarrow Q_{nA} = n_A P$
  B $n_B \Rightarrow Q_B = n_B P$
- Exchange Q_A, Q_B
- Shared secret
  $n_A Q_B = n_A n_B P = n_B Q_A$

Obs • they can exchange only the x coord
• y can be calculated (especially if $p \equiv 3 \bmod 4$)

Elliptic Elgamal KE

—— " ——

- key creation (A)
  A: $n_A \Rightarrow P n_A = Q_A \rightarrow B$
- Encryption (B)
  Choose plaintext M } $C_1 = kP \in E(\mathbb{F}_p)$
  — " — random k } $C_2 = M + k Q_A \in E(\mathbb{F}_p)$
  $(C_1, C_2) \rightarrow A$
- Decryption (A)

$M = C_2 - n_A C_1 \in E(\mathbb{F}_p)$

Obs • 4-1 message expansion (C_1, C_2 with coords)
• only $\approx p$ points on $E(\mathbb{F}_p)$
$\Rightarrow$ Limited

Lenstra's Elliptic Curve factorization algo

- Similar to Pollard's $p-1$
- Intuition → I work on mod N $\Rightarrow$ $\exists$ k s.t. $k \cdot P = \mathcal{O}$ $\Rightarrow$ line between $(k-1)P$ & P has undefined slope

→ Why? Slope $= \frac{y_2 - y_1}{x_2 - x_1} \Rightarrow (y_2 - y_1)(x_2 - x_1)^{-1}$
$= \frac{3x_1^2 + a}{2y} \Rightarrow (3x_1^2 + a) \cdot (2y)^{-1}$
undefined if it has common factors with N $\Rightarrow$
$\Rightarrow$ returns gcd(denom, N)

Algorithm

- Input: N

1. Choose random A, x, y mod N
2. $P = (x, y)$; $B \equiv y^2 - x^3 - Ax \bmod N$
   $E: Y^2 = x^3 + Ax + B$
3. for $j = 2, 3, \ldots$
   $Q = j \cdot P$; $P = Q$
   if $Q = jP$ fails:
   gcd(d, N)
   if $d < N$: return d
   else go to 1

Elliptic curves over $\mathbb{F}_2$ and $\mathbb{F}_{2^k}$

Reminder: $\forall p^k$, p = prime; $\exists!$ $\mathbb{F}_{p^k}$ with p^k elements

Ex: $f(x) = a_n x^{n-1} + \dots + a_1 x + a_0$; Each $a_i \in \mathbb{Z}_p$ $\Big\}$ $\Rightarrow p^n$ polynomials

Let m be an irreductible poly of degree m; $\mathbb{F}[x]/m$ = finite field

- So we can map $\mathbb{F}_{p^k}$ to $\mathbb{F}[x]/m$ with m irr of degree k
- All finite fields of a given order (size) are isomorphic
- Obviously $p=0$

Generalized Weierstrass equation

E: $Y^2 + a_1 x Y + a_3 Y = x^3 + a_2 x^2 + a_4 X + a_6$; $\Delta \neq 0$

$\Delta = -b_2^2 \cdot b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6$ where $b_2 = a_1^2 + a_2$; $b_4 = 2a_4 + a_1 \cdot a_3$

$b_6 = a_3^2 + 4a_6$; $b_8 = a_1^2 a_6 + 4 a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$

Reflection $(x,y) \to (x, -y - a_1 x - a_3)$

$x(P_1 + P_2) = \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2$

$x(2P) = \dfrac{x^4 - b_4 x^2 - 2 b_6 x - b_8}{4x^3 + b_2 x^2 + 2 b_4 x + b_6}$

Frobenius map $\tau : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$; $\tau(x) = x^p$ $\Big\{ \to \tau(x+y) = \tau(x) + \tau(y)$; $\to \tau(x \cdot y) = \tau(x) \cdot \tau(y)$

- Let ~~$E(\mathbb{F}_2)$~~ E defined over $\mathbb{F}_2$; $P = (x,y) \in E(\mathbb{F}_{2^k})$ $\Big\} \Rightarrow \tau(P) = (\tau(x), \tau(y)) \in E(\mathbb{F}_{2^k})$; $\Rightarrow \tau(P+Q) = \tau(P) + \tau(Q)$

[T] Hasse $E(\mathbb{F}_{p^k}) = p^k + 1 - t_{p^k}$ where $|t_{p^k}| \leq 2 p^{k/2}$

[T] Let $E(\mathbb{F}_p)$; $t = p + 1 - |E(\mathbb{F}_p)|$ $\Big\} \Rightarrow$ (a) α, β = complex roots of $Z^2 - tZ + p$ $\Rightarrow |\alpha| = |\beta| = \sqrt{p}$; $\forall k \geq 1 \Rightarrow |E(\mathbb{F}_{p^k})| = p^k + 1 - \alpha^k - \beta^k$

(b) Let $\tau : E(\mathbb{F}_{p^k}) \to E(\mathbb{F}_{p^k})$; $(x,y) \to (x^p, y^p) \Rightarrow \forall Q \in E(\mathbb{F}_{p^k}) \Rightarrow \tau^2(Q) - t \cdot \tau Q + p \cdot Q = O$

$\Rightarrow \tau^2 = -2 - \tau \Rightarrow$ (Let) $n \in \mathbb{Z}$; $n = v_0 + v_1 \tau + \dots + v_\ell \tau^\ell$; $v_i \in \{-1, 0, 1\} \Rightarrow$

$\Rightarrow$ we can compute nP faster ($\tau^i(P)$ is easier than $2^i P$)

Bilinear pairings on EC

- Ex: dot product $\beta(v,w) = v \cdot w = v_1 w_1 + \dots + v_n w_n$
  determinant on $\mathbb{R}^2$ $\det\begin{pmatrix} v_1 & v_2 \\ w_1 & w_2 \end{pmatrix} = v_{w_2} - v_2 w_1$
- Intuition: take a pair of vectors → a number

Points of finite orders

$E[m] = \{P \in E \mid mP = \mathcal{O}\}$; P = point of order m

Prop: $P, Q \in E[m] \Rightarrow P+Q, -P \in E[m] \Rightarrow E[m]$ is a subgroup of E

Prop 1. $E(\mathbb{C})[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

2 $p \nmid m$; $\exists k$ s.t $E(\mathbb{F}_{p^{jk}}) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ $\forall j \geq 1$

product of 2 cyclic groups of order m

Rational functions & divisors on EC

$$f(x) = \frac{a_0 + \dots + a_m x^m}{b_0 + \dots + b_n x^n} = \frac{a(x-\alpha_1)^{e_1} \dots (x-\alpha_k)^{e_k}}{b(x-\beta_1)^{d_1} \dots (x-\beta_s)^{d_s}}$$ where $\begin{cases} \alpha_1 \dots \alpha_k = \text{zeroes} \\ \beta_1 \dots \beta_s = \text{poles} \end{cases}$ distinct

$\operatorname{div}(f(x)) = e_1[\alpha_1] + \dots + e_k[\alpha_k] - d_1[\beta_1] - \dots - d_k[\beta_k]$ $\begin{cases} e_1 \dots e_k \\ d_1 \dots d_s \end{cases}$ = multiplicities

Let $E = EC$ $E: y^2 = x^3 + Ax + B \Rightarrow f(P) = f(x,y) \Rightarrow \operatorname{div}(f) = \sum_{P \in E} n_P [P]$

$n_P \in \mathbb{Z}$, finite amount are non zero

1. E, f, g ; if $\operatorname{div}(f) = \operatorname{div}(g) \Rightarrow \exists\, c \neq 0$ constant s.t $f = cg$
2. $D = \sum_{P \in E} n_P [P]$ = divisors on E. D is a div of a rational fct $\iff \begin{cases} \deg(D) = 0 \\ \text{Sum}(D) = 0 \end{cases}$

The Weil Pairing

→ takes a pair of points $P, Q \in E[m]$
↳ outputs an mth root of unity $e_m(P,Q)$

Let f_P and f_Q be rational fct with $\begin{cases} \operatorname{div}(f_P) = m[P] - m[\mathcal{O}] \\ \operatorname{div}(f_Q) = m[Q] - m[\mathcal{O}] \end{cases}$

$$e_m(P,Q) = \frac{f_P(Q+S)}{f_P(S)} \Big/ \frac{f_Q(P-S)}{f_Q(-S)}$$ where $S \in E$; $S \neq \{\mathcal{O}, P, -Q, P-Q\}$

Th 1. $e_m(P,Q)^m = 1 \quad \forall P,Q \in E[m]$

2. $e_m(P_1+P_2, Q) = e_m(P_1,Q) \cdot e_m(P_2,Q)$
   $e_m(P, Q_1+Q_2) = e_m(P,Q_1) \cdot e_m(P,Q_2)$
   $\Big\} \Leftrightarrow e_m$ is bilinear

3. $e_m(P,P) = 1 \quad \forall P \in E[m] \Leftrightarrow e_m$ is alternating $\Rightarrow e_m(P,Q) = e_m(P,Q)^{-1}$

4. if $e_m(P,Q) = 1 \quad \forall Q \in E[m] \Rightarrow P = \mathcal{O} \Leftrightarrow e_m$ is non degenerate

! For an algorithm read Miller's Weil Pairing algo

The Tate pairing → more efficient than Weil

Let $E(\mathbb{F}_q)$, l = prime, $P \in E(\mathbb{F}_q)[l]$, $Q \in E(\mathbb{F}_q)$. choose f_P, $\operatorname{div}(f_P) = l[P] - l[\mathcal{O}]$

$$\tau(P,Q) = \frac{f_P(Q+S)}{f_P(S)} \in \mathbb{F}_q^*$$; where $S \in E(\mathbb{F}_q)$ s.t. $f_P(Q+S), f_P(S) \neq 0$

Modified: $\hat{\tau}(P,Q) = \tau(P,Q)^{(q-1)/l}$ when $q \equiv 1 \bmod l$

The Weil pairing over $\mathbb{F}_{p^k}$

Def Embedding degree of E with respect to m = smallest k s.t.

$$E(\mathbb{F}_{p^k})[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \text{ where } p \nmid m$$

- The Weil pairing embeds E DLP $E(\mathbb{F}_p)$ into DLP in $\mathbb{F}_{p^k}$ → MOV ALGO

Modified Weil pairing

if $P_1 = aP$, $P_2 = bP \Rightarrow e_m(P_1,P_2) = e_m(aP, bP) = e_m(P,P)^{ab} = 1^{ab} = 1$ → Problem!

- Solution: we choose $\phi : E \to E$; let $P \in E[l]$

  1. $\phi(nP) = n\phi P \quad \forall n \geq 1$
  2. $e_l(P, \phi(P))^k = 1 \Leftrightarrow l \mid k$

  $\Big\} \Rightarrow \phi$ = distortion map

Prop view $E[l] = \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$ as a 2 dim vector space over $\mathbb{Z}/l\mathbb{Z}$

1. P & Q form a basis for $E[l]$
2. $P \neq \mathcal{O}$, Q is not a multiple of P
3. $e_l(P,Q)$ is a primitive lth root of unity
4. $e_l(P,Q) \neq 1$

$\Big\}$ equivalent

MOV Algorithm
↓
to read

Chapter 7 Lattices and Cryptography

A congruential public key cryptosystem

1.
- Public q
- Secret $f < \sqrt{q/2}$; $\sqrt{q/4} < g < \sqrt{q/2}$; $\gcd(f, 2g) = 1$
- Public $h = f^{-1} g \bmod q$

2. Encryption
- Choose $m < \sqrt{q/4}$
- Choose $r < \sqrt{q/2}$
- return $e = (rh + m) \bmod q$

3. Decryption
- $a = fe \bmod q$
- $b = f^{-1} a \bmod g$

$\Rightarrow m = b$

Size restrictions $\Rightarrow rg + fm < \sqrt{\frac{q}{2}}\sqrt{\frac{q}{2}} + \sqrt{\frac{q}{2}}\sqrt{\frac{q}{4}} < q$

$\Rightarrow$ when $a \equiv (fe) \bmod q \Rightarrow a = rg + fm \Rightarrow$

$\Rightarrow b \equiv f^{-1} a \equiv f^{-1}(rg + fm) \equiv m \bmod g$

($rg + fm \equiv 0 \bmod g$)

How to break? $\rightarrow$ try to find (f, g) from (q, h)

$\Rightarrow$ Find (F, G): $Fh \equiv G \bmod q$; $F, G = \mathcal{O}(\sqrt{q})$

$\Leftrightarrow Fh = G + qR \Leftrightarrow F\begin{pmatrix}1\\ h\end{pmatrix} - R\begin{pmatrix}0\\ q\end{pmatrix} = \begin{pmatrix}F\\ G\end{pmatrix} \Rightarrow$

(v_1, v_2, w)

$\Rightarrow$ find $w = a_1 v_1 + a_2 v_2$ where $\begin{cases} v_1, v_2 = \mathcal{O}(q) \\ w = \mathcal{O}(\sqrt{q}) \end{cases} \Leftrightarrow$

$\Leftrightarrow$ find a sort vector in $L = \{a_1 v_1 + a_2 v_2 \mid a_1, a_2 \in \mathbb{Z}\}$

Subset Sum Problems & knapsack crypto

- Subset-Sum Problem = Given $(M_1 \dots M_n)$, find a subset where the sum is S $\rightarrow$ Not(M, S)

Prop $\forall I \subset \{i \mid 1 \le i \le \frac{1}{2}n\}$; $J \subset \{j \mid \frac{1}{2}n < j \le n\}$ list of $A_I = \sum_{i \in I} M_i$; $B_J = S - \sum_{j \in J} M_j$

Then these lists contain (I_0, J_0) with $A_{I_0} = B_{J_0} \Rightarrow S = \sum_{i \in I_0} M_i + \sum_{j \in J_0} M_j \rightarrow$ solu

Obs $2^{n/2}$ entries at most $\Rightarrow \mathcal{O}(2^{n/2 + \varepsilon})$

$\Rightarrow$ We can make a cryptosystem out of this!

Def superincreasing sequence $r = (r_1 \dots r_n)$ with $r_{i+1} > 2r_i$ $\forall 1 \le i \le n-1$

$\Rightarrow$ if M = superincreasing $\Rightarrow$ we have an ~~cryptosystem~~ algo for solving (M, S)

Algorithm

for $i = n \to 1$:
  if $S \geq M_i$:
    $S -= M_i$
    $x_i = 1$
  else:
    $x_i = 0$

Merkle-Hellman

- Key creation
  $h = (h_1 \dots h_n)$ super-increasing
  A, B with $B \geq 2h_n$, $\gcd(A, B) = 1$
  $M_i = A h_i$
  return M
- Encryption
  Choose x
  $S = x \cdot M$
  return S
- Decryption
  $S' = A^{-1} S \bmod B$
  Solve$(S', h) \Rightarrow x$

Proof: $S' = A^{-1}S = A^{-1} \sum_{i=1}^{n} x A h_i \equiv \sum_{i=1}^{n} x_i h_i \bmod B$; $B \geq 2h_n \Rightarrow \sum_{i=1}^{n} x_i h_i < \sum_{i=1}^{n} h_i < 2h_n <$

Obs.
- $\exists$ collision algo in $O(2^{n/2}) \Rightarrow n > 2k$ for 2^k security
- $h_1 > 2^n \Rightarrow h_n > 2^{2n} \Rightarrow B > 2h_n = 2^{2n+1} \Rightarrow M_i = O(2^{2n})$; $S = O(2^{2n})$

$\Rightarrow$ Big public key $\Rightarrow$ impractical

- Where is the lattice?

$$\begin{matrix} v_1 \\ v_2 \\ \vdots \\ v_n \\ v_{n+1} \end{matrix} \begin{pmatrix} 2 & 0 & \dots & 0 & m_1 \\ 0 & 2 & \dots & 0 & m_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 2 & m_2 \\ 1 & 1 & \dots & 1 & S \end{pmatrix} \Rightarrow L = \{ a_1 v_1 + \dots + a_{n+1} v_{n+1} \mid a_1, \dots a_{n+1} \in \mathbb{Z} \}$$

$\Rightarrow S = x_1 m_1 + \dots + x_n m_n$

Let x = solution $\Rightarrow t = \sum_{i=1}^{n} x_i v_i - v_{n+1} = (2x_1 - 1, 2x_2 - 1, \dots 0)$

Since $x_i \in \{0, 1\} \Rightarrow t_i \in \{-1, 1\} \Rightarrow \|t\| = \sqrt{n} = \text{short}$

$m_i = O(2^{2n})$; $S = O(2^{2n})$

$\Rightarrow$ likely that t is the shortest $\Rightarrow$ LLL to solve

Vector spaces review

Lattices

Def Let $v_1 \dots v_n \in \mathbb{R}^m$ be a set of l.i. vectors $\Rightarrow$

$\Rightarrow L = \{ a_1 v_1 + \dots + a_n v_n \mid a_1 \dots a_n \in \mathbb{Z} \}$; $\dim L = n$

- Suppose $v_1 \dots v_n$ is a basis in L; $w_1 \dots w_n \in L \Rightarrow \begin{cases} w_1 = \alpha_{11} v_1 + \dots + \alpha_{1n} v_n \\ \vdots \\ w_n = \alpha_{n1} v_1 + \dots + \alpha_{nn} v_n \end{cases}$; $\alpha_{ij} \in \mathbb{Z}$

$\Rightarrow A = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{n1} & \dots & \alpha_{nn} \end{pmatrix}$; if we want to express v_i in terms of $w_j \Rightarrow A^{-1}$

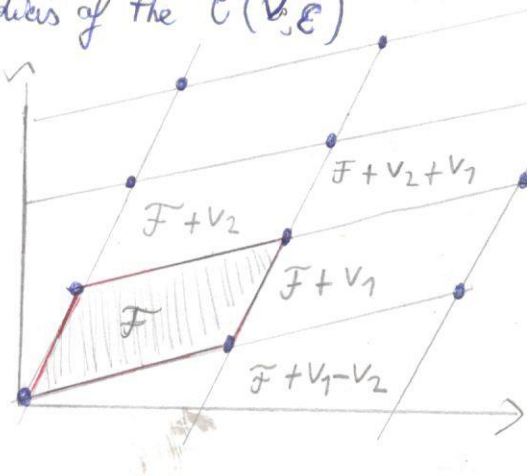
BUT $1 = \det(I) = \det(AA^{-1}) = \det A \det A^{-1} \Rightarrow \det(A), \det(A^{-1}) \in \{-1, 1\}$

$\det A \in \mathbb{Z}$, $\det A^{-1} \in \mathbb{Z}$

Lattices as discrete additive subgroup

1. $\exists \varepsilon > 0$ s.t. $\forall v \neq w, v, w \in L, \|v - w\| \geq \varepsilon$
2. $\forall v, w \in L \Rightarrow v - w \in L$

Intuition: $\exists \varepsilon$ s.t. $\nexists w$ ~~in~~ near v in the vertices of the $\mathcal{C}(v, \varepsilon)$



Fundamental domain

$$\mathcal{F}(v_1 \dots v_n) = \{ t_1 v_1 + \dots + t_n v_n \mid 0 \leq t_i < 1 \}$$

Prop

Let $L \subset \mathbb{R}^n$; $\mathcal{F}$ = fundamental domain for $L \Rightarrow$

$\Rightarrow \forall w \in \mathbb{R}^n \Rightarrow w = t + v$ for a unique $t \in \mathcal{F}$, unique $v \in L \Rightarrow \mathcal{F} + v = \{ t + v \mid t \in \mathcal{F} \}$

Def $\det(L)$ = n-dim volume of $\mathcal{F}$ = $\det(F)$ where F = $\mathcal{F}$ coord matrix $= \mathbb{R}^n$

Hadamard Inequality: $\det L = \mathrm{Vol}(\mathcal{F}) \leq \|v_1\| \cdot \dots \cdot \|v_n\|$

Intuition: the orthogonal the basis vectors are $\Rightarrow$ the closer this is to ~~max~~ equality is

!obs! $\forall \mathcal{F}$ for $L \Rightarrow$ ~~det~~ Vol$(\mathcal{F})$ = const !

Short vectors in lattices

- Shortest vector problem (SVP) = find $v \in L, v \neq 0$ that minimizes $\|v\|$
- Closest vector problem (CVP) = Given $w \in \mathbb{R}^m$; $w \notin L$, find $v \in L$ ~~s.t.~~ that minimizes $\|w - v\|$

!Obs SVP & CVP $\simeq$ NP-hard $\Rightarrow$ nice for crypto

- Shortest basis problem (SBP): Given L, find a basis $\{v_1 \dots v_n\}$ that is "shortest" in some sense

Ex: $\max_{i \leq n} \|v_i\|$ or $\sum_{i=1}^{n} \|v\|^2$

- Appr SVP Let $\psi(n)$ = function; $\dim L = n$. Find $\|v\| \leq \psi(n) \|v_{shortest}\|$

  Ex: $\|v\| \leq 3\sqrt{n} \|v_{shortest}\|$

- Appr CVP: same idea

T Hermite's theorem $\forall L$, $\dim L = n$, $\exists\, v \in L, v \neq 0$ with $\|v\| \leq \sqrt{n}\, \det(L)^{\frac{1}{n}}$

Obs • for n, γ_n = smallest const s.t. $\forall L$, $\dim L = n$ $\exists\, v \in L$ s.t.

$$\|v\|^2 \leq \gamma_n^2 \det(L)^{2/n}$$

• for large $n \Rightarrow$ $\boxed{\frac{n}{2\pi e} \leq \gamma_n \leq \frac{n}{\pi e}}$

$\forall a \in \mathbb{R}^n$, $\forall R > 0$, the closed ball of radius R centered in a is

$$B_R(a) = \{ x \in \mathbb{R}^n \mid \|x - a\| \leq R \}$$

T Minkowski's theorem: Let $L \subset \mathbb{R}^n$, $\dim L = n$; $S \subset \mathbb{R}^n$, S = bounded sym convex set whose volume satisfies $Vol(S) > 2^n \det(L)$

$\Rightarrow$ $\exists$ nonzero lattice vector in S

Babai's algorithm → solving approx CVP using a "good" basis

if L's basis is orthogonal $\Rightarrow$ SVP is found in the basis set

For CVP $\left.\begin{matrix} w = t_1 v_1 + \dots + t_n v_n \\ v = a_1 v_1 + \dots + a_n v_n \end{matrix}\right\} \Rightarrow \|v - w\|^2 = (a_1 - t_1)^2 \|v_1\| + \dots + (a_n - t_n)^2 \|v_n\|^2 \Rightarrow$

$\Rightarrow$ take a_i closest int to t_i

Intuition: • Find a translation of $\mathcal{F}$ that contains w $(\mathcal{F} + v)$

• $w = v + \varepsilon_1 v_1 + \dots + \varepsilon_n v_n$ where $\varepsilon_i = \{0, 1\}$

Algorithm

$w = t_1 v_1 + \dots + t_n w_n$, $t_1 \dots t_n \in \mathbb{R}$

$a_i = \lfloor t_i \rceil$ for $i = 1 \dots n$

return $v = a_1 v_1 + \dots + a_n v_n$

Hadamard's ratio

$$\mathcal{H}(B) = \left(\frac{\det L}{\|v_1\| \cdot \dots \cdot \|v_n\|} \right)^{1/n} \in (0, 1]$$

→ the closer to 1 $\Rightarrow$ the more orth the are the vectors

GGH Cryptosystem

- **Key creation**
  - good $V = \{v_1 \dots v_m\}$
  - U with $\det(U) = \pm 1$
  - bad $W = UV$,
  - return W
- **Encryption**
  - m, r
  - $e = mW + r$
  - return e
- **Decryption**
  - find closest $v \in L$ to e using Babai
  - $m = V \cdot W^{-1}$

Convolutional Polynomial Rings

Def Fix $N \in \mathbb{Z}_+$. The ring of conv poly of rank N

$$R = \frac{\mathbb{Z}[x]}{(x^N - 1)}$$

Ring of conv poly modulo q $R_q = \dfrac{\mathbb{Z}/q\mathbb{Z}[x]}{(x^N - 1)}$

$\Rightarrow \forall$ element $= a_0 + \dots + a_{N-1} x^{N-1}$ representation (unique) with coeff $\in \mathbb{Z}$ or $\mathbb{Z}/q\mathbb{Z}$

Intuition When we mod $x^N - 1$ we require $x^N = 1 \Rightarrow$ when we see $x^N \to$ we replace with 1

Let $a(x) = (a_0 \dots a_{N-1})$ ← Notation

- Addition $a(x) + b(x) = (a_0 + b_0 + \dots + a_{N-1} + b_{N-1})$
- Product $a(x) \cdot b(x) = c(x)$ where $c_k = \sum_{i+j \equiv k \bmod N} a_i b_{k-i}$

Def Let $a(x) \in R_q$. The **center lift of $a(x)$**: $a'(x) \bmod q = a(x)$ with $a'(x) \in R$, coeff $(a'(x)) \in \left(-\frac{q}{2}, \frac{q}{2}\right]$; $a'(x)$ is unique

Prop Let q = prime $\Rightarrow \exists\, a(x)^{-1} \in R_q \Leftrightarrow \gcd(a(x), x^N - 1) = 1$ in $\mathbb{Z}/q\mathbb{Z}[$

E GCD $\Rightarrow a(x)u(x) + (x^N - 1)v(x) = \gcd(a(x), x^N - 1) \Rightarrow a(x)^{-1} = u(x)$

NTRU

$$R = \frac{\mathbb{Z}[x]}{(x^N - 1)} \; ; \; R_p = \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^N - 1)} \; ; \; R_q = \mathbb{Z}/q\mathbb{Z}[x]$$

with N = prime ; $\gcd(N, q) = \gcd(p, q) = 1$

Def $\forall d_1, d_2 \in \mathbb{Z}_+ \quad \mathcal{T}(d_1, d_2) = \{ a(x) \in R \mid a(x) \text{ has } d_1 \text{ coeff} = 1,\ a(x) \text{ has } d_2 \text{ coeff} = -1,\ a(x) \text{ has all other} = 0 \}$

= ternary polynomials

Algorithm

- **Public parameters**
  - N = prime ; $\gcd(N, q) = \gcd(p, q) = 1$
  - $q > (6d+1)p$
- **Key creation**
  - Choose private $f \in \mathcal{T}(d+1, d)$ with inv in R_p & R_q ; $f(d, d)$
  - $F_p = f^{-1}$ in R_p ; $F_q = f^{-1}$ in R_q
  - return $h = F_q * f$
- **Encryption**
  - $m \in R_p$, $r \in \mathcal{T}(d, d)$
  - return $e = (p\, r * h + m) \% q$
- **Decryption**
  - $f * e = (p\, g * r + f * m) \% q$
  - Center-lift a to $a \in R$
  - Compute $m \equiv (F_p * a) \bmod p$

- $m \in R$ where coeff satisfy $-\frac{1}{2}p < m_i < \frac{1}{2}p$
  $\Rightarrow m$ is a center-lift of a poly in R_p
- $e \in R_q$

Proof $F_p * e \equiv m \bmod q$

$a = f * e \bmod q$

$= f * (p\, h * r + m) = p\, f * F_q * g * r + m f \bmod q$

$= p\, g * r + m f \bmod q$ [1]

1. Since $g, r \in \mathcal{T}(d, d) \Rightarrow g * r$ all the 1's and -1's match up $\Rightarrow$ larges possible coeff $= 2d$
2. $f \in \mathcal{T}(d+1, d)$, $m_i \in \left(-\frac{p}{2}, \frac{p}{2}\right] \Rightarrow$ largest coeff $= (2d+1)\frac{p}{2}$

1, 2 $\Rightarrow$ if the coeff's coincide $\Rightarrow$

$\Rightarrow p \cdot 2d + (2d+1)\frac{p}{2} = \left(3d + \frac{1}{2}\right)p = \text{max coeff} < \frac{q}{2}$ $\Rightarrow$

$\Rightarrow$ you lift it to $R \Rightarrow h = F_p(p\, g * r + f * m) \bmod p$

$= F_p * f * m \bmod p$

$= m$

NTRU Problems

→ Given $h(x)$, find ternary $f(x), g(x)$ s.t $f(x) \cdot h(x) \equiv g(x) \bmod q$

How hard is it?

→ not a unique solution $\Rightarrow (x^k f, x^k g)$ is a solution $\forall\ 0 \le k \le N$

→ Any pair with small coeffs that can satisfies $f \cdot h = g \bmod q$ is a key

- Brute force

$$|\mathcal{T}(d_1, d_2)| = \binom{N}{d_1}\binom{N-d_1}{d_2} = \frac{N!}{d_1!\, d_2!\, (N-d_1-d_2)!}$$ max = when $d_1, d_2 \approx N/3$

↳ big

- Collision
  - → needs space
  - → $\mathcal{O}(3^{N/2}/\sqrt{N})$ steps

NTRU Lattice cryptosystem

- Let $h(x) = h_0 + \dots + h_{N-1} x^{N-1} \Rightarrow$ Let $\boxed{M_h^{NTRU} = \begin{pmatrix} I_N & P_N(h) \\ 0_N & q \cdot I_N \end{pmatrix}}$

where $P_N = \begin{pmatrix} h_0 & h_1 & \dots & h_{N-1} \\ h_{N-1} & h_0 & \dots & h_{N-2} \\ \vdots & & & \\ h_1 & h_2 & \dots & h_0 \end{pmatrix}$ = permutation Matrix

Let $L_H^{NTRU} =$ ~~the lattice~~ $Span(M_h^{NTRU})$

Prop Let $f \cdot h = g \bmod q$; $u \in R$ s.t $f \cdot h = g + q u$

Then $(f, -u)\, M_h^{NTRU} = (f, g) \iff (f, -u)\begin{pmatrix} I_N & P_N(h) \\ 0_N & qI_N \end{pmatrix} = (f, g)$

Prop

$$\det(L_h^{NTRU}) = q^N$$

T Let L = lattice, $\dim(L) = n$. Any LLL-reduced basis has:

1. $\prod_{i=1}^{n} \|v_i\| \le 2^{n(n-1)/4} \det L$
2. $\|v_j\| \le 2^{(i-1)/2} \|v_i^*\| \quad \forall\ 1 \le j \le i \le n$

$\|v_1\| \le 2^{n-1/4} |\det L|^{1/n}$

$\|v_1\| \le 2^{(n-1)/2} \min_{0 \neq v \in L} \|v\| \Rightarrow$

$\Rightarrow$ LLL solves approx SVP within $2^{(n-1)/2}$

Algorithm

Intuition - we form a basis satisfy size cond
- we check Lovasz condition
- LLL tries to minimise the volumes of $L_1 \dots L_n$

→ wikipedia for algorithm

Using LLL to solve approx CVP

T $\exists$ C = const s.t. $\forall L$, $\dim L = n$, the following algo solves approx CVP within C^n

1. Apply LLL to $\{v_1 \dots v_n\}$
2. Apply Babai's using the reduced basis

Applications

1. Congruential