Number Theory and RSA Problem

Yu Zhang

HIT/CST/NIS

Cryptography, Spring, 2012

Outline

1. Arithmetic and Basic Group Theory

2. Primes and Factoring

3. RSA Assumption

Content

1. Arithmetic and Basic Group Theory
2. Primes and Factoring
3. RSA Assumption

Primes and Divisibility

- The set of **integers** $\mathbb{Z}$, $a, b, c \in \mathbb{Z}$.
- a **divides** b: $a \mid b$ if $\exists c, ac = b$ (otherwise $a \nmid b$).
  b is a **multiple** of a. If $a \notin \{1, b\}$, then a is a **factor** of b.
- $p > 1$ is **prime** if it has no factors.
- An integer > 1 which is not prime is **composite**.
- $\forall a, b$, $\exists$ **quotient** q, **remainder** r: $a = qb + r$, and $0 \leq r < b$.
- **Greatest common divisor** $\gcd(a, b)$ is the largest integer c such that $c \mid a$ and $c \mid b$. $\gcd(0, b) = b$, $\gcd(0, 0)$ undefined.
- a and b are **relatively prime (coprime)** if $\gcd(a, b) = 1$.
- **Euclid's theorem**: there are infinitely many prime numbers.

Fundamental Theorem of Arithmetic

- **Bézout's lemma**: $\forall a, b,\ \exists\ X, Y:\ Xa + Yb = \gcd(a, b)$. $\gcd(a, b)$ is the smallest positive integer that can be expressed in this way.
- **Euclid's lemma**: If $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$. If p is prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$.
- **Fundamental theorem of arithmetic**: $\forall N > 1,\ N = \prod_i p_i^{e_i}$, $\{p_i\}$ are distinct primes and $e_i \geq 1$. This expression is unique.

Modular Arithmetic

- Remainder $r = [a \bmod N] = a - b\lfloor a/b \rfloor$ and $r < N$. N is called **modulus**.
- **Reduction modulo** N: mapping a to $[a \bmod N]$.
- $\mathbb{Z}_N = \{0, 1, \ldots, N-1\} = \{a \bmod N | a \in \mathbb{Z}\}$.
- a and b are **congruent modulo** N: $a \equiv b \pmod{N}$ if $[a \bmod N] = [b \bmod N]$.
- a is **invertible modulo** $N \iff \gcd(a, N) = 1$. If $ab \equiv 1 \pmod{N}$, then $b = a^{-1}$ is **multiple inverse** of a **modulo** N.
- **Cancellation law**: If $\gcd(a, N) = 1$ and $ab \equiv ac \pmod{N}$, then $b \equiv c \pmod{N}$.
- **Euclidean algorithm**: $\gcd(a, b) = \gcd(b, [a \bmod b])$.
- **Extended Euclidean algorithm**: Given a, N, find X, Y with $Xa + YN = \gcd(a, N)$.

Examples of Modular Arithmetic

"Reduce and then add/multiply" instead of "add/multiply and then reduce".

Compute $193028 \cdot 190301 \bmod 100$

$193028 \cdot 190301 = [193028 \bmod 100] \cdot [190301 \bmod 100] \bmod 100$
$= 28 \cdot 1 \equiv 28 \bmod 100.$

$ab \equiv cb \pmod N$ does *not necessarily* imply $a \equiv c \pmod N$.

$a = 3, c = 15, b = 2, N = 24$

$3 \cdot 2 = 6 \equiv 15 \cdot 2 \pmod{24}$, but $3 \not\equiv 15 \pmod{24}$.

Use extended Euclidean algorithm to ...

Find the inverse of $11 \pmod{17}$

$(-3) \cdot 11 + 2 \cdot 17 = 1$, so 14 is the inverse of 11.

Groups

A **group** is a set $\mathbb{G}$ with a binary operation $\circ$:

- (**Closure**:) $\forall g, h \in \mathbb{G}$, $g \circ h \in \mathbb{G}$.
- (**Existence of an Identity**:) $\exists$ **identity** $e \in \mathbb{G}$ such that $\forall g \in \mathbb{G}, e \circ g = g = g \circ e$.
- (**Existence of Inverses**:) $\forall g \in G$, $\exists\ h \in \mathbb{G}$ such that $g \circ h = e = h \circ g$. h is an **inverse** of g.
- (**Associativity**:) $\forall g_1, g_2, g_3 \in \mathbb{G}$, $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.

$\mathbb{G}$ with $\circ$ is **abelian** if

- (**Commutativity**:) $\forall g, h \in \mathbb{G}, g \circ h = h \circ g$.

Existence of inverses implies **cancellation law**.
When $\mathbb{G}$ is a **finite group** and $|\mathbb{G}|$ is the **order** of group.

Group Exponentiation

$$g^m \stackrel{\text{def}}{=} \underbrace{g \circ g \circ \cdots \circ g}_{m \text{ times}}.$$

Theorem 1

$\mathbb{G}$ *is a finite group. Then* $\forall g \in \mathbb{G}, g^{|\mathbb{G}|} = 1$.

Corollary 2

$\forall g \in \mathbb{G}$ *and* i, $g^i = g^{[i \bmod |\mathbb{G}|]}$.

Corollary 3

Define function $f_e : \mathbb{G} \to \mathbb{G}$ *by* $f_e(g) = g^e$.
If $\gcd(e, |\mathbb{G}|) = 1$, *then* f_e *is a permutation.*
Let $d = [e^{-1} \bmod |\mathbb{G}|]$, *then* f_d *is the inverse of* f_e. *(*$f_d(f_e(g)) = g$*)*
e***'th root of*** c: $g^e = c$, $g = c^{1/e} = c^d$.

The Group $\mathbb{Z}_N^*$

$$\mathbb{Z}_N^* \stackrel{\text{def}}{=} \{a \in \{1, \ldots, N-1\} \,|\, \gcd(a, N) = 1\}$$

Euler's phi function: $\phi(N) \stackrel{\text{def}}{=} |\mathbb{Z}_N^*|$.

Theorem 4

$N = \prod_i p_i^{e_i}$, $\{p_i\}$ are distinct primes, $\phi(N) = \prod_i p_i^{e_i - 1}(p_i - 1)$.

Corollary 5 (Euler's theorem & Fermat's little theorem)

$a \in \mathbb{Z}_N^*$. $a^{\phi(N)} \equiv 1 \pmod{N}$.
If p is prime and $a \in \{1, \ldots, p-1\}$, then $a^{p-1} \equiv 1 \pmod{p}$.

Corollary 6

Define function $f_e : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ by $f_e(x) = [x^e \bmod N]$.
If $\gcd(e, \phi(N)) = 1$, then f_e is a permutation.
Let $d = [e^{-1} \bmod \phi(N)]$, then f_d is the inverse of f_e.
*e**'th root of** c: $g^e = c$, $g = c^{1/e} = c^d$.*

Subgroups

If $\mathbb{G}$ is a group, a set $\mathbb{H} \subseteq \mathbb{G}$ is a **subgroup** of $\mathbb{G}$ if $\mathbb{H}$ itself forms a group under the same operation associated with $\mathbb{G}$. $\mathbb{H}$ is a **strict subgroup** if $\mathbb{H} \neq \mathbb{G}$.

- If $\mathbb{H} \subseteq \mathbb{G}$, $\mathbb{H}$ contains the identity element of $\mathbb{G}$, and $\mathbb{H}$ is closed, then $\mathbb{H}$ is a subgroup of $\mathbb{G}$.
- **Lagrange's theorem**: For a finite group $\mathbb{G}$ and its subgroup $\mathbb{H}$, $|\mathbb{H}| \mid |\mathbb{G}|$.
- $\mathbb{H}$ is a strict subgroup of a finite group $\mathbb{G}$, then $|\mathbb{H}| \leq |\mathbb{G}|/2$.

Examples on Groups

- $\mathbb{Z}$ is an abelian group under '$+$', not a group under '$\cdot$'.
- The set of real numbers $\mathbb{R}$ is not a group under '$\cdot$'.
- $\mathbb{R} \setminus \{0\}$ is an abelian group under '$\cdot$'.
- $\mathbb{Z}_N$ is an abelian group under '$+$' modulo N.
- If p is prime, then $\mathbb{Z}_p^*$ is an abelian group under '$\cdot$' modulo p.
- $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$, $|\mathbb{Z}_{15}^*| = 8$.
- $\mathbb{Z}_3^*$ is a subgroup of $\mathbb{Z}_{15}^*$, but $\mathbb{Z}_5^*$ is not.
- $2^{1/3} \bmod 5 = 2^3 \bmod 5 = 3$. $(3^{-1} = 3 \pmod 4)$
- g^3 is a permutation on $\mathbb{Z}_{15}^*$, but g^2 is not (e.g., $8^2 \equiv 2^2 \equiv 4$).

$N = pq$ where p, q are distinct primes. $\phi(N) =?$

$\phi(N) = (N-1) - (q-1) - (p-1) = (p-1)(q-1)$.

Isomorphism and Cross Product

A bijection function $f : \mathbb{G} \to \mathbb{H}$ is an **isomorphism from $\mathbb{G}$ to $\mathbb{H}$**:

$$\forall g_1, g_2 \in \mathbb{G}, f(g_1 \circ_{\mathbb{G}} g_2) = f(g_1) \circ_{\mathbb{H}} f(g_2).$$

If $\exists$ such f, $\mathbb{G} \simeq \mathbb{H}$.

The **cross product** of $\mathbb{G}$ and $\mathbb{H}$: $\mathbb{G} \times \mathbb{H}$. The elements are (g, h) with $g \in \mathbb{G}$ and $h \in \mathbb{H}$, the operation $\circ$,

$$(g, h) \circ (g', h') \stackrel{\mathsf{def}}{=} (g \circ_{\mathbb{G}} g', h \circ_{\mathbb{H}} h')$$

Chinese Remainder Theorem

Theorem 7 (Chinese remainder theorem)

$N = pq$ *where* $\gcd(p, q) = 1$.

$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q \text{ and } \mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*.$$

f *maps* $x \in \{0, \ldots, N-1\}$ *to pairs* (x_p, x_q) :

$$f(x) \stackrel{\text{def}}{=} ([x \bmod p], [x \bmod q]).$$

f *is an isomorphism from* $\mathbb{Z}_N$ *to* $\mathbb{Z}_p \times \mathbb{Z}_q$ *and* $\mathbb{Z}_N^*$ *to* $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

If $f(x) = (x_p, x_q)$, $x \leftrightarrow (x_p, x_q) = ([x \bmod p], [x \bmod q])$.

Using the Chinese Remainder Theorem

Compute $g = g_1 \circ_{\mathbb{G}} g_2$ [$g \equiv g_1 \times g_2 \pmod N$]:

1. Compute $h_1 = f(g_1)$ and $h_2 = f(g_2)$;
2. Compute $h = h_1 \circ_{\mathbb{H}} h_2$;
3. Compute $g = f^{-1}(h)$.

Compute $14 \cdot 13 \bmod 15$

$[14 \cdot 13 \bmod 15] \leftrightarrow (4, 2) \cdot (3, 1) = ([4 \cdot 3 \bmod 5], [2 \cdot 1 \bmod 3])$
$= (2, 2) \leftrightarrow 2.$

Using the Chinese Remainder Theorem (Cont.)

Convert (x_p, x_q) to its representation modulo N:

1. Compute X, Y such that $Xp + Yq = 1$.
2. $1_p = [Yq \bmod N]$ and $1_q = [Xp \bmod N]$.
3. Compute $x = [(x_p \cdot 1_p + x_q \cdot 1_q) \bmod N]$.

Find the representation of $([4 \bmod 5], [3 \bmod 7])$ modulo 35.

Use extended Euclidean algorithm, $3 \cdot 5 - 2 \cdot 7 = 1$.
$1_p = [(-2 \cdot 7) \bmod 35] = 21$ and $1_q = [3 \cdot 5 \bmod 35] = 15$.
$(4, 3) \leftrightarrow [4 \cdot 1_p + 3 \cdot 1_q \bmod 35] = 24$.

Compute $[29^{100} \bmod 35]$

$29 \leftrightarrow ([1 \bmod 5], [-1 \bmod 7])$,
$[29^{100} \bmod 35] \leftrightarrow (1, -1)^{100} = (1, 1) \leftrightarrow 1$.

Arithmetic algorithms

- **Addition/subtraction**: linear time $O(n)$.
- **Mulplication**: naively $O(n^2)$. Karatsuba (1960): $O(n^{\log_2 3})$
  Basic idea: $(2^b x_1 + x_0) \times (2^b y_1 + y_0)$ with 3 mults.
  Best (asymptotic) algorithm: about $O(n \log n)$.
- **Division with remainder**: $O(n^2)$.
- **Exponentiation**: $O(n^3)$.

Algorithm 1: Exponentiating by Squaring

input : $g \in G$; exponent $x = [x_n x_{n-1} \ldots x_2 x_1 x_0]_2$

output: g^x

$y \leftarrow g; z \leftarrow 1$

for $i = 0$ **to** n **do**

  if $x_i == 1$ **then** $z \leftarrow z \times y$

  $y \leftarrow y^2$

return z

Content

1 Arithmetic and Basic Group Theory

2 Primes and Factoring

3 RSA Assumption

Integer Factorization/Factoring

"The problem of distinguishing prime numbers from composite numbers and of resolving the later into their prime factors is known to be one of the most important and useful in arithmetic." – Gauss (1805)

The "hardest" numbers to factor seem to be those having only large prime factors.

- The best-known algorithm is the **general number field sieve** [Pollard] with time $\mathcal{O}(\exp(n^{1/3} \cdot (\log n)^{2/3}))$.
- RSA Factoring Challenge: RSA-768 (232 digits)
  - Two years on hundreds of machines (2.2GHz/2GB, 1500 years)
  - Factoring a 1024-bit integer: about 1000 times harder.

Generating Random Primes

Algorithm 2: Generating a random prime

input : Length n; parameter t

output: A random n-bit prime

for $i = 1$ **to** t **do**
  $p' \leftarrow \{0,1\}^{n-1}$
  $p := 1 \| p'$
  if p *is prime* **then return** p
return fail

To show its efficiency, we need understand two issues:

- the probability that a randomly-selected n-bit integer is prime.
- how to efficiently test whether a given integer p is prime.

The Distribution of Prime

Theorem 8 (Prime number theorem)

$\exists$ a constant c such that, $\forall n > 1$, a randomly selected n-bit number is prime with probability at least c/n.

The probability that a prime is *not* chosen in $t = n^2/c$ iterations is

$$\left(1 - \frac{c}{n}\right)^t = \left(\left(1 - \frac{c}{n}\right)^{n/c}\right)^n \le \left(e^{-1}\right)^n = e^{-n}.$$

The algorithm will fail with a negligible probability.

Testing Primality

- **Trial division**: Divide N by $a = 2, 3, \ldots, \sqrt{N}$.
- **Probabilistic algorithm for approximately computing**:
  - Atlantic City algorithm with two-sided error.
  - Monte Carlo algorithm with one-sided error.
  - Las Vegas algorithm with zero-sided error.
- **Fermat primality test**: $a^{N-1} \equiv 1 \pmod{N}$.
- a is a **witness** that N is composite if $a^{N-1} \not\equiv 1 \pmod{N}$.
- a is a **liar** if N is composite and $a^{N-1} \equiv 1 \pmod{N}$.
- **Carmichael numbers**: composite numbers without witnesses.

Theorem 9

If $\exists$ a witness, then at least half the elements of $\mathbb{Z}_N^*$ are witnesses.

The Miller-Rabin Primality Test

$N-1 = 2^r u$, u is odd. $a \in \mathbb{Z}_N^*$ is a **strong witness** if

1. $a^u \neq \pm 1$, and
2. $a^{2^i u} \neq -1$ for $i \in \{1, \ldots, r-1\}$.

Lemma 10

*$x \in \mathbb{Z}^*$ is a **square root of 1 modulo** N if $x^2 \equiv 1 \pmod N$. If N is an odd prime then the only x are $[\pm 1 \bmod N]$.*

Theorem 11

N is an odd, composite number that is not a prime power. Then at least half the elements of $\mathbb{Z}_N^*$ are strong witnesses.

Theorem 12

If N is prime, then the Miller-Rabin test always outputs "prime". If N is composite, then the algorithm outputs "prime" with probability at most 2^{-t}[1].

[1] Actually, it is at most 4^{-t}.

Describing The Algorithm

Algorithm 3: The Miller-Rabin primality test

input : Integer $N > 2$ and parameter t

output: A decision as to wether N is prime or composite

if N *is a perfect power* **then return** "composite"
compute $r \geq 1$ and u odd such that $N - 1 = 2^r u$
LOOP: **for** $s = 1$ **to** t **do**
    $a \leftarrow \{2, \ldots, N-2\}$
    $x = a^u \bmod N$
    if $x = \pm 1$ **then** do next **LOOP**
    for $i = 1$ **to** r **do**
        $x = x^2 \bmod N$
        if $x = -1$ **then** do next **LOOP**
    return "composite"
return "prime"

Examples of Primality Tests

Liars in Fermat primality test

$2^{340} \equiv 1 \pmod{341}$, but $341 = 11 \cdot 31$.
$5^{560} \equiv 1 \pmod{561}$, but $561 = 3 \cdot 11 \cdot 17$.
Carmichael numbers < 10000:
561, 1105, 1729, 2465, 2821, 6601, 8911.

Examples of Miller-Rabin test

Carmichael number $1729 = 7 \cdot 13 \cdot 19$.
$1729 - 1 = 1728 = 2^6 \cdot 27$. So $r = 6, u = 27$. $a = 671$.

$$671^{27} \equiv 1084 \pmod{1729}$$
$$671^{27\cdot 2} \equiv 1065 \pmod{1729}$$
$$671^{27\cdot 2^2} \equiv 1 \pmod{1729}$$

The Factoring Assumption

Let $\mathsf{GenModulus}(1^n)$ be a polynomial-time algorithm that, on input 1^n, outputs (N, p, q) where $N = pq$, and p, q are n-bit primes except with probability negligible in n.

The factoring experiment $\mathsf{Factor}_{\mathcal{A},\mathsf{GenModulus}}(n)$:

1. Run $\mathsf{GenModulus}(1^n)$ to obtain (N, p, q).
2. $\mathcal{A}$ is given N, and outputs $p', q' > 1$.
3. $\mathsf{Factor}_{\mathcal{A},\mathsf{GenModulus}}(n) = 1$ if $p' \cdot q' = N$, and 0 otherwise.

Definition 13

Factoring is hard relative to GenModulus if $\forall$ PPT algorithms $\mathcal{A}$, $\exists$ negl such that

$$\Pr[\mathsf{Factor}_{\mathcal{A},\mathsf{GenModulus}}(n) = 1] \leq \mathsf{negl}(n).$$

Algorithms for Factoring

- **Factoring** $N = pq$. p, q are of the same length n.
- **Trial division**: $\mathcal{O}(\sqrt{N} \cdot \text{polylog}(N))$.
- **Pollard's** $p-1$ method: effective when $p-1$ has "small" prime factors.
- **Pollard's rho** method: $\mathcal{O}(N^{1/4} \cdot \text{polylog}(N))$.
- **Quadratic sieve** algorithm [Carl Pomerance]: sub-exponential time $\mathcal{O}(\exp(\sqrt{n \cdot \log n}))$.
- The best-known algorithm is the **general number field sieve** [Pollard] with time $\mathcal{O}(\exp(n^{1/3} \cdot (\log n)^{2/3}))$.

Pollard's $p-1$ Method

Idea: Fermat's little theorem: $y = x^{(p-1)\cdot k} \equiv 1 \pmod{p}$. Then $(y-1) \equiv 0 \pmod{p}$ and $p \mid (y-1)$. So $p = \gcd(y-1, N)$. To make the exponent a large multiple of $(p-1)$:

$$M = lcm(\{i|i \leq B\}) = \prod_{\text{prime } i \leq B} i^{\lfloor \log_i B \rfloor}.$$

If $p-1$ has only "small" factors, then the bound B will be small.

Algorithm 4: Pollard's $p-1$ algorithm for factoring

input : Integer N

output: A non-trivial factor of N

$x \leftarrow \mathbb{Z}_N^*$

$y := [x^M \bmod N]$

$p := \gcd(y-1, N)$

if $p \notin \{1, N\}$ **then return** p

Pollard's Rho (ρ) Method

Idea: Using the improved birthday attack[2] to find x, x' such that $x \neq x' \wedge x \equiv x' \pmod{p}$. Then $p \mid (x - x')$, $p = \gcd(x - x', N)$.
$F(x) = x^2 + b$, where $b \not\equiv 0, -2 \pmod{N}$.

Algorithm 5: Pollard's rho algorithm for factoring

---

input : Integer N

output: A non-trivial factor of N

$x_0 \leftarrow \mathbb{Z}_N^*$

for $i = 1$ **to** $2^{n/2}$ **do**

  $x_i := [F(x_{i-1}) \bmod N]$

  $x_{2i} := [F(F(x_{2i-2})) \bmod N]$

  $p := \gcd(x_{2i} - x_i, N)$

  if $p \notin \{1, N\}$ **then return** p

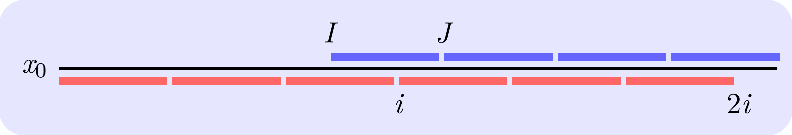
---

[2] Floyd's cycle-finding algorithm (the "tortoise and the hare" algorithm).

Proof of Pollard's ρ Method

Lemma 14

Let $x_1, \ldots$ be a sequence with $x_m \equiv F(x_{m-1}) \pmod N$. F satisfies that $x \equiv x' \pmod N \implies F(x) \equiv F(x') \pmod N$. If $x_I \equiv x_J \pmod p$ with $I < J$, then $\exists\ i < J$ such that $x_i \equiv x_{2i} \pmod p$.



Proof.

See the proof of improved birthday attack. □

According to the lemma of birthday problem, given a sequence of length $O(N^{1/4})$, find such pair with probability $1/4$.

Example of Pollard's $p-1$ and ρ methods

Factorizing $N = 5917$ with Pollard's $p-1$ method

Choose $B = 5$, $M = lcm(1,2,3,4,5) = 60$.
For $x = 2$, $y \equiv x^M \equiv 2^{60} \equiv 3417 \pmod{5917}$.
$p = gcd(y-1, N) = \gcd(3416, 5917) = 61$.

Factorizing $N = 8051$ with Pollard's ρ method

$f(x) = x^2 + 1$, $x_0 = 2$.

i	x_i	x_{2i}	$\gcd(x_{2i} - x_i, N)$
1	5	26	1
2	26	7474	1
3	677	871	97

The Quadratic Sieve Algorithm

Idea: Find x, y with $x^2 \equiv y^2 \pmod{N}$ and $x \not\equiv \pm y \pmod{N}$.
$x^2 - y^2 \equiv 0 \pmod{N} \implies (x+y)(x-y) \equiv 0 \pmod{N}$.
$\gcd(x+y, N)$ and $\gcd(x-y, N)$ will give p.
Finding congruence of squares:

1. Choose a factor base $B = \{p_1, \ldots, p_k\}$ of prime numbers.
2. Use '**sieve theory**' to find $\ell = k + 1$ distinct $x_1, \ldots, x_\ell$ for which $[x_i^2 \bmod N]$ decompose into the elements of B: $x_i^2 \equiv \prod_{j=1}^{k} p_j^{e_j} \pmod{N}$.
3. Write x_i^2 as an exponent vector $\langle e_{i,1}, \ldots, e_{i,k} \rangle \pmod{2}$.
4. Find the addition of vectors = the zero vector $\pmod{2}$. $X = \{x_{\ell_1}, \ldots, x_{\ell_n}\}$. $\forall i$, $E_i = \sum_{j=1}^{n} e_{\ell_j,i} \equiv 0 \pmod{2}$.
5. Find a pair: $x = \prod_{i=1}^{n} x_{\ell_i} \not\equiv y = \prod_{i=1}^{k} p_i^{E_i/2} \pmod{N}$.

Example of Quadratic Sieve Algorithm

Factorizing $N = 377753$ with quadratic sieve algorithm

$B = \{2, 13, 17, 23, 29\}$.

$$620^2 \equiv 17^2 \cdot 23 \pmod N$$
$$621^2 \equiv 2^4 \cdot 17 \cdot 29 \pmod N$$
$$645^2 \equiv 2^7 \cdot 13 \cdot 23 \pmod N$$
$$655^2 \equiv 2^3 \cdot 13 \cdot 17 \cdot 29 \pmod N$$

$$[620 \cdot 621 \cdot 645 \cdot 655 \bmod N]^2 \equiv [2^7 \cdot 13 \cdot 17^2 \cdot 23 \cdot 29 \bmod N]^2$$
$$\implies 127194^2 \equiv 45335^2 \pmod N,$$

Computing $\gcd(127194 - 45335, 377753) = 751$.

Content

1 Arithmetic and Basic Group Theory

2 Primes and Factoring

3 RSA Assumption

The RSA Problem

Recall group exponentiation on $\mathbb{Z}_N^*$

Define function $f_e : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ by $f_e(x) = [x^e \bmod N]$.
If $\gcd(e, \phi(N)) = 1$, then f_e is a permutation.
If $d = [e^{-1} \bmod \phi(N)]$, then f_d is the inverse of f_e.
e**'th root of** c: $g^e = c$, $g = c^{1/e} = c^d$.

Idea: factoring is hard
$\implies$ for $N = pq$, finding p, q is hard
$\implies$ computing $\phi(N) = (p-1)(q-1)$ is hard
$\implies$ computations modulo $\phi(N)$ is not available
There is a gap.
$\implies$ **RSA problem** [Rivest, Shamir, and Adleman] is hard:
Given $y \in \mathbb{Z}_N^*$, compute y^{-e}, e^{th}-root of y modulo N.

Open problem

RSA problem is easier than factoring?

Generating RSA Problem

Algorithm 6: GenRSA

input : Security parameter 1^n

output: N, e, d

$(N, p, q) \leftarrow \mathsf{GenModulus}(1^n)$

$\phi(N) := (p-1)(q-1)$

find e such that $\gcd(e, \phi(N)) = 1$

compute $d := [e^{-1} \bmod \phi(N)]$

return N, e, d

The RSA Assumption

The RSA experiment $\mathsf{RSAinv}_{\mathcal{A},\mathsf{GenRSA}}(n)$:

1. Run $\mathsf{GenRSA}(1^n)$ to obtain (N, e, d).
2. Choose $y \leftarrow \mathbb{Z}_N^*$.
3. $\mathcal{A}$ is given N, e, y, and outputs $x \in \mathbb{Z}_N^*$.
4. $\mathsf{RSAinv}_{\mathcal{A},\mathsf{GenRSA}}(n) = 1$ if $x^e \equiv y \pmod{N}$, and 0 otherwise.

Definition 15

RSA problem is hard relative to GenRSA if $\forall$ PPT algorithms $\mathcal{A}$, $\exists$ negl such that

$$\Pr[\mathsf{RSAinv}_{\mathcal{A},\mathsf{GenRSA}}(n) = 1] \leq \mathsf{negl}(n).$$

Summary

- Primes, modular arithmetic.
- Miller-Rabin primality testing.
- Factoring, Pollard's $p-1$ and ρ methods.
- e^{th}-root modulo N, RSA.

Textbook

"*A Computational Introduction to Number Theory and Algebra*" (Version 2) by Victor Shoup