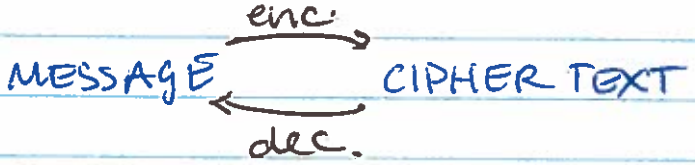
Cryptography (Chpt 6)

Defn: A PRIVATE KEY CRYPTOSYSTEM consists of:

An ENCODER algorithm $E(M,X)$ which takes a MESSAGE M, and a PRIVATE KEY X, and produces a CIPHER TEXT $C = E(M,X)$

A DECODER algorithm $D(C,X)$ which gives $M = D(C,X)$



Ex (Caesar cipher) consider the alphabet as a list of numbers:

0	1	2	.....	25
↕	↕	↕		↕
A	B	C		Z

To encode the letter m with private key x:
output $m+x \bmod 26$

To decode the cipher text c with private key x:
output $c-x \bmod 26$.

Ex: HELLO WORLD $\xrightarrow{+3}$ KHOOR ZRUOG

THIS IS VERY HARD $\xrightarrow{+7}$ AOPZ PZ CLYF OHYK

Thm: The Caesar Cipher satisfies:

$$M = D(E(M, X), X)$$

Every message decodes to itself

Pf: $(m+x) - x \bmod 26$
$= m \bmod 26$

Ex (Rot 13 Encoding)

To encode a letter m output $m+13 \bmod 26$
To decode a letter m output $m+13 \bmod 26$.

Thm: The Rot 13 encoding satisfies:

$$M = E(E(M, X), X)$$ # encoding = decoding

Pf: $(m+13)+13 \bmod 26$
$= m+26 \bmod 26$
$= m \bmod 26$

Ex (one Time Pad) # The strongest possible cryptosystem
It is hard to transmit keys.

To encode a bit m with bit x ouput $x+m \bmod 2$
To decode a bit c with bit x output $c+m \bmod 2$.

$M = 01011$
$X = 11010$

$E(M, X) = 10001$

Real coin tosses!

$M = 10000$
$X = 10111$

$E(M, X) = 00111$

The RSA Algorithm

Defn: A PUBLIC KEY CRYPTOSYSTEM consists of:

→ PRIVATE-PUBLIC KEY PAIR (X, Y)
→ An PUBLIC KEY ENCODER $E(M, Y)$
→ A PRIVATE KEY DECODER $D(C, X)$

Such that: $M = D(E(M, Y), X)$

NB: The key Y can be made publically available with compromising security.

The RSA crypto-system

- Pick two large primes p and q.
- Calculate $N = pq$
- Calculate $\phi(N) = (p-1)(q-1)$

- Choose e so that $\gcd(e, \phi(N)) = 1$
- Solve $de \equiv 1 \bmod \phi(N)$

The public key is (N, e)
The private key is d

To encrypt M calculate $C \equiv M^e \bmod N$

To decrypt C calculate $M = C^d \bmod N$.

Thm: For the RSA cryptosystem

$$M = D(E(M,e),d)$$

Pf: $D(E(M,e),d)$

$$\equiv D(M^e, d) \bmod N$$

$$\equiv (M^e)^d \equiv M^{ed}$$

However, $ed \equiv 1 \bmod \phi(N)$.

$$\Rightarrow \phi(N) \mid (ed-1)$$

$$\Rightarrow ed - 1 = k\phi(N)$$

Thus, $D(E(M,e),d) \equiv M^{ed} \bmod N$

$$\equiv M^{ed-1+1}$$

$$\equiv M^{k\phi(N)+1}$$

\# By Euler's Thm $\equiv M \cdot (M^{\phi(N)})^k$

$$\equiv M \cdot 1^k \equiv M.$$

Thus, $D(E(M,e),d) = M$.

Rational Numbers (chpt 8)

Def^n A **RATIONAL NUMBER** is $\frac{a}{b}$ where: $a, b \in \mathbb{Z}$ and $b \neq 0$.

Two rational numbers are equal if:

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc$$

Ex: $\frac{1}{2} = \frac{2}{4}$ since $1 \cdot 4 = 2 \cdot 2$

$\frac{5}{7} = \frac{10}{14}$ since $5 \cdot 14 = 7 \cdot 10$

$\frac{1}{3} \neq \frac{1}{2}$ since $1 \cdot 2 \neq 1 \cdot 3$

Nota: The **RATIONALS** are the set of rational numbers

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}$$

Thm

- $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$
- $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$
- $n = \frac{n}{1}$
- $\frac{a}{b} \neq 0 \Rightarrow \frac{b}{a} \cdot \frac{a}{b} = 1$

Lemma: For any rational number $\frac{a}{b}$ we may find $\frac{p}{q}$ such that:

- $\gcd(p,q) = 1$
- $\frac{a}{b} = \frac{p}{q}$

Pf: If $d|a$ and $d|b$ then we write:

$$a = pd \quad \text{and} \quad b = qd$$

We get $\frac{a}{b} = \frac{pd}{qd} = \frac{p}{q}$. ▪

Taking $d = \gcd(a,b)$ gives $\gcd(p,q) = 1$.

Thm (Rational Roots)

If $\frac{m}{n}$ is a rational root of

$$a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$$

where $a_i \in \mathbb{Z}$ and $\gcd(m,n) = 1$ then

$m|a_0$ and $n|a_k$

Pf (Rational Roots)

If $\frac{m}{n}$ is a root then we have:

$$a_k\left(\frac{m}{n}\right)^k + a_{k-1}\left(\frac{m}{n}\right)^{k-1} + \dots + a_1\left(\frac{m}{n}\right) + a_0 = 0$$

$$\Rightarrow a_k m^k + a_{k-1} m^{k-1} n + \dots + a_1 m n^{k-1} + a_0 n^k = 0$$

We get:

$$a_k m^k = n\left(-a_{k-1} m^{k-1} - \dots - a_0 n^{k-1}\right)$$

Thus, $n \mid a_k m^k$ and so $n \mid a_k$ ✓

$$a_0 n^k = m\left(-a_k m^{k-1} - \dots - a_1 n^{k-1}\right)$$

Thus, $m \mid a_0 n^k$ and so $m \mid a_0$ ✓

Thm: The polynomial $p(x) = x^2 - 2$ has no rational roots.

Pf: If $\frac{m}{n}$ was a root of $p(x)$ we would get:

$$m \mid (-2) \quad \text{and} \quad n \mid (1)$$

Thus, $\frac{m}{n} = \frac{\pm 2}{1}, \frac{\pm 1}{1} = -2, 2, -1, 1.$

None of these are roots, and thus $p(x)$ has no rational roots.

Defn: A real number x is IRRATIONAL if $x \neq \frac{a}{b}$ for any $a, b \in \mathbb{Z}$ with $b \neq 0$.

Ex: $\sqrt{2}$ is irrational.

Pf: Recall $p(x) = x^2 - 2$ has no rational roots.
But $p(\sqrt{2}) = (\sqrt{2})^2 - 2 = 2 - 2 = 0$.
Thus, $\sqrt{2}$ is a root of $p(x)$.

Pf: Suppose $\left(\frac{m}{n}\right)^2 = 2$. We get $m^2 = 2n^2$.

We may choose $\frac{m}{n}$ so that $\gcd(m,n) = 1$.

$2n^2 = m^2 \Rightarrow 2 \mid m^2 \Rightarrow 2 \mid m$ since 2 is prime

We get $m = 2k$ and thus

$$(2k)^2 = 2n^2 \Rightarrow 4k^2 = 2n^2$$
$$\Rightarrow 2k^2 = n^2$$
$$\Rightarrow 2 \mid n$$

Thus, $2 \mid m$ and $2 \mid n$. We get $\gcd(m,n) \neq 2$.

Pf: We have $\underbrace{m^2}_{\text{Exponent of two must be even}} = \underbrace{2n^2}_{\text{Exponent of two is odd.}}$

By the Fundamental Theorem of Arithmetic, the exponent of two is unique.

Thm: If N is a natural number and $\sqrt{N}$ is rational then $\sqrt{N}$ is an integer

Pf: Consider the polynomial $p(x) = x^2 - N$.
We have that $p(\sqrt{N}) = (\sqrt{N})^2 - N = 0$.

If $\sqrt{N}$ is rational then it is a rational root of $p(x)$. We obtain that $\sqrt{N} = \frac{m}{n}$ implies

$$m \mid (-N) \text{ and } n \mid 1$$

Thus, $\frac{m}{n} = \frac{m}{\pm 1}$ and we obtain $\frac{m}{n} = \pm m$.

It follows that $\sqrt{N} = \frac{m}{n} = \pm m$ is an integer.

Corollary: If $\sqrt{N}$ is rational then N is a square.

Pf: If $\sqrt{N}$ is rational, then it is an integer.
We get $\sqrt{N} = m$ and thus $N = m^2$.

Ex: $\sqrt{15}$ is irrational since 15 is not a square.

$\sqrt{42}$ is irrational since 42 is not a square.

Ex: $\sqrt{3}+\sqrt{5}$ is irrational

Suppose $x = \sqrt{3}+\sqrt{5}$. We get:

$$\Rightarrow x^2 = 3 + 2\sqrt{3}\sqrt{5} + 5$$
$$\Rightarrow x^2 - 8 = 2\sqrt{3}\sqrt{5}$$
$$\Rightarrow x^4 - 16x^2 + 64 = 4 \cdot 3 \cdot 5 = 60$$
$$\Rightarrow x^4 - 16x^2 - 4 = 0$$

Thus, x is a root of $p(x) = x^4 - 16x^2 - 4$.

If $p(x)$ has a rational root $\frac{m}{n}$ then:

$$m \mid (-4) \text{ and } n \mid (1)$$

Thus, $\frac{m}{n} = -4, -2, -1, 1, 2, 4$

We note $p(x) = p(-x)$ and so we check:

$$p(1) = -19$$
$$p(2) = -52$$
$$p(4) = -4$$

Thus, $p(x)$ has no rational roots and

$x = \sqrt{3}+\sqrt{5}$ is irrational.

Review

Topics:
- naturals
- primes / composites
- divisibility
- induction
- modular arithmetic
- Fermat's Theorem
- Wilson's Thm
- Fund Thm of Arithmetic
- Euclidean Algorithm

Memorize the Following:

- induction
- well ordering
- generalized induction $\{n, n+1, \dots\}$
- complete induction
- generalized complete
- Fermat
- division $a = qb + r$
- Fundamental Thm of Arithmetic (and canonical factorizations)

Bits and Pieces

Ex: Determine if 103 is prime.

if $n=ab$ then $a \le \sqrt{n}$ or $b \le \sqrt{n}$

We test by dividing by all primes $\le \sqrt{103} \approx 10$.

divide by 2

$103 = 2 \cdot 51 + 1$

divide by 3

$103 = 34 \cdot 3 + 1$

divide by 5

$103 = 20 \cdot 5 + 3$

divide by 7

$103 = 14 \cdot 7 + 5$

Thus, 103 has no prime divisors $\le \sqrt{103}$
It follows that 103 is prime.

Ex: Show that $x^2+y^2 = 103$ has no integer solution.

(!) Work in modular arithmetic.

n	n^2 mod 4
0	0
1	1
2	0
3	1

Thus, $x^2+y^2 \equiv 0+0 \equiv 0 \mod 4$.
$\equiv 0+1 \equiv 1$
$\equiv 1+1 \equiv 2$

It follows that $x^2+y^2 = 103$ has no solu.

Ex: Show that the congruence $x^4+3x^2 \equiv 1 \pmod 5$ has no solutions.

$x^4 \equiv 1 \pmod 5$ by Fermat

$x \equiv 1 \Rightarrow x^4+3x^2 \equiv 1+3 \equiv 4 \pmod 5$

$x \equiv 2 \Rightarrow \equiv 1+1 \equiv 2$

$x \equiv 3 \Rightarrow \equiv 1+2 \equiv 3$

$x \equiv 4 \Rightarrow \equiv 1+3 \equiv 4$

$x \equiv 0 \Rightarrow \equiv 0+0 \equiv 0$

Thus, $x^4+3x^2 \equiv 1$ has no solutions.