Euclidean Algorithm

Let $r_0 > r_1$ ①

r_2 positive int

then $r_0 = q_1 r_1 + r_2 \quad 0 < r_2 < r_1$

$r_1 = q_2 r_2 + r_3 \quad 0 < r_3 < r_2$

$r_{m-2} = q_{m-1} r_{m-1} + r_m \quad 0 < r_m < r_{m-1}$

$r_{m-1} = q_m r_m$

Then it is not hard to show that $GCD(r_0, r_1) = GCD(r_1, r_2) = \dots GCD(r_{m-1}, r_m) = r_m$ ②

Extended

Now suppose we define a sequence of numbers $t_0, t_1, \dots t_m$ according to the following recurrence relation $t_0 = 0$

$t_1 = 1 \quad t_j = (t_{j-2} - q_{j-1} * t_{j-1}) \bmod r_0 \quad \text{if } j \geq 2$

where the q_j is defined as above.

Corollary: if $GCD(r_0, r_1) = 1$ then $t_m = r_1^{-1} \bmod r_0$

Extended Algorithm

$r_0 = n$

$b_0 = b$

$t_0 = 0$

$t = 1$

$q = \lfloor \frac{r_0}{b_0} \rfloor$

$r = (r_0 - q) * b_0$

while $(r > 0)$

{ temp $= (t_0 - q) * t$

if (temp ≥ 0)

temp = temp mod n

if (temp < 0)

temp $= n - \{(-\text{temp}) \bmod n\}$

$t_0 = t$

$t =$ temp

$r_0 = b_0$

$b_0 = r$

$q = \lfloor r_0 / b_0 \rfloor$

$r = r_0 - q * b_0$

}

if $(b \neq 1)$

b has no inverse of modulo n

else

$b^{-1} = b \bmod n$

Let a and b are two positive integer $\in$ a strictly less than b, and a and b are relatively prime that is a and b doesn't have any common factor.

Then, a^{-1} is another integer less than b such that $a * a^{-1} = 1 \bmod b$ This positive integer a^{-1} is called multiplicative inverse of a in mod b.

Let $r_0 > r_1$ are two positive integers.

Then $r_0 = q_1 r_1 + r_2 \quad 0 < r_2 < r_1$

$r_1 = q_2 r_2 + r_3 \quad 0 < r_3 < r_2$

$\vdots$

$r_{m-2} = q_{m-1} r_{m-1} + r_m \quad 0 < r_m < r_{m-1}$

$r_{m-1} = q_m \times r_m$

Then it is not hard to show that $GCD(r_0, r_1) = GCD(r_1, r_2)$

$= \dots\dots = GCD(r_{m-1}, r_m)$

$= r_m$

Now suppose we define a sequence of number according to the following recurrence relation. $t_0 = 0$ $t_1 = 1 \ldots t_j = t_{j-2} - q_{j-1} * t_{j-1}$ if $j \geq 2$

Where q_j are defined as above

(Prove)

Cokollary → if $GCD(r_0, r_1) = 1$ then $t_n = (r_1^{-1}) \bmod r_0$

Extended Euclidean Algorithm

$n_0 = n$

$b_0 = b$

$t_0 = 0$

$t = 1$

$q = \lfloor n_0 / b_0 \rfloor$

$r = n_0 - q \times b_0$

```
while (r > 0)
{
 temp = (t0 - q) * t
 if (temp > 0)
   tem = temp mod n
 if (tem < 0)
   temp = n - {(-temp) mod n}
 t0 = t
 t = temp
 n0 = b0
 b0 = r
  q = ⌊n0/b0⌋
  r = n0 - q * b0
}
1 =
if (b ≠ 1)
  then b has no inverse in mod n
else
  b-1 = t mod n
```

Info Sec

A crypto system is a 5 tuple (P, C, K, E, D) where the following conditions are satisfied

1) P is a finite set of possible plain texts
2) C is a finite set of possible cipher text
3) K, the keyspace is the finite set of possible keys
4) For each $k \in K$ there is a encryption rule $e_k \in E$ and a corresponding decryption rule $d_k \in D$. Each $e_k : P \to C$ are functions such that $d_k(e_k(x)) = k$.

For every plain text belongs to P

Sythe Cipher

Let $P = C = K = Z_{26}$, for $0 \geq k \geq 25$ define $0 > k > 25$

define $e(k(x)) = x + k[26]$ and the subscript $k(x)$

$y - k[26]$ where $x, y \in Z_{26}$

Definition of multiplicative inverse

suppose $a \in Z_m$

The multiplicative inverse of a is an a^{-1} such that $a \cdot a^{-1} \equiv 1 \pmod{m}$

to Z_m multiplicative inverse of

1) What is a crypto system ?

A crypto system is a five tuple (P, C, K, E, D) where the following conditions are satisfied.

→ P is a finite set of possible plain text

→ C is a finite set of possible cipher text

→ K(k), the keyspace, is a finite set of possible keys.

→ E, for each $k \in K$, there is a encryption rule $e_k \in E$ and a corresponding decryption rule $d_k \in D$ such that each $e_k : P \to C$ such that for each and $d_k : C \to P$ are functions and $d_k(e_k(x)) = x$ for every plain text $x \in P$.

2) Definition of congruency

Suppose a and b are integers and m is a positive integer then we write $a \equiv b \pmod m$ if m devides $b-a$.

The integer m is called modulus.

3) Sieve Cipher

Let $P = C = K = Z_{26}$

We define $e_k(x) = x + k \bmod 26$ and $d_k = y - k \bmod 26$

Possible Questions

Plain text to cipher text (with given small text)

Write down code for sieve cipher when $k = 4$

4) Definition of Multiplicative inverse

Multiplicative inverse of $a \in Z_m$ is an element $a^{-1} \in Z_m$ such that $a \cdot a^{-1} \equiv 1 \bmod m$

Corrollary

The multiplicative inverse of small a in mod m exists if a and m are relatively prime that is a and m doesn't have any common factor.

Substitution | Sieve → caesar cipher (k=3) | affine cipher | RSA and related math | Knapsak

Stream Cipher

In the cryptosystem we have studied to this point successive plaintext element are encrypted using the same key that is the cipher text string y is obtained as follows. $y = y_1 y_2 \ldots = e_K(x_1) e_K(x_2) \ldots$. Cryptosystem of this type are often called block cipher. An alternative approach is to what are called stream ciphers. The basic idea is to generate a key stream $z = z_1 z_2 \ldots$ and use it encrypt a plain text string. $x = x_1 x_2 \ldots$ according to the rule of stream cipher $y = y_1 y_2 \ldots = e_{z_1}(x_1) \times e_{z_2}(x_2) \ldots$

Public key Cryptosystem and Private key cryptosystem

In the classical model of cryptography we have been studied so far we use same key k for encryption and decryption or the decryption key can be derived from encryption key. For example (DES Cryptosystem). The cryptosystem of this type known as private key cryptosystem since the exposure of e_k rendered the system insecure.

The idea behind public key system is that it might be possible to find a cryptosystem where is it computationally infeasible to determine d_K given e_K. Then the encryption rule e_K could be made public by publishing it in a directory. The decryption rule d_K will be kept private.

RSA Algo — show that RSA decryption is inverse of encryption

Extended Euclidean algo

set of super increasing number

Subset Problem — Knapsack