Cryptology **8th august 2015**

Lecture 2: Classical Ciphers II: Some number theoretic results on GCD

Instructor: Goutam Paul *Scribe: Arup Biswas*

2.1 GCD

Theorem 2.1 $gcd\,(a,b) = min\,\{ax + by : ax + by > 0, x, y \in \mathbb{Z}\}$

Proof: let $g = gcd\,(a,b)$.
let $m = min\{ax + by : ax + by > 0\}$
Need to show $g = m$.
Let $S = \{ax + by : ax + by > 0\}$.
Since$g = gcd\,(a,b)$,
$therefore g \mid a$ and $g \mid b$.
$\Rightarrow g \mid ax$ and $g \mid by$, $\forall x, \forall y \in \mathbb{Z}$.
$\Rightarrow g \mid ax + by$, $\forall x, \forall y \in \mathbb{Z}$.
$\Rightarrow g \mid ax^\star + by^\star$, where $m{=}ax^\star + by^\star$
$\Rightarrow g \mid m$.
$\Rightarrow g \leq m$. .....(1)

claim $m \mid a$ suppose $a = mq + r$, $0 \leq r < m$.
$\Rightarrow r = a - mq = a - (ax^\star + by^\star)q$
$\Rightarrow r = a(1 - qx^\star) + b(-qy^\star) = ax' + by'$.

Further, if $r > 0$,
$r = ax' + by' \in S$
which contradicts the minimality of $m \in S$
$\Rightarrow r$ has to be 0.
$\Rightarrow m \mid a$
Similar argument gives $m \mid b$.
$\therefore m$ is a common divisor of a and b.
$\Rightarrow m \leq g$.....(2)
(1) and (2) $\Rightarrow m = g$.
■

2.1.1 Extended Euclid's Algorithm

Given a and b how to find x,y s.t. $gcd(a,b) = ax + by$.
From extended euclid's algorithm we can calculate the x and y.

w.l.g. assume $a > b$.
$a = r_{-1}$

$b = r_0$
$b \mid a$ we get quotient q_1 and remainder r_1

$r_{-1} = r_0 q_1 + r_1$
$r_0 = r_1 q_2 + r_2$
.
.
.
$r_{n-2} = r_{n-1} q_n + r_n$
$r_{n-1} = r_n q_{n+1} + 0$
From Euclid's algorithm we get
gcd(a,b)=$r_n = r_{n-2} - r_{n-1} q_n$
$= r_{n-2} - q_n(r_{n-3} - r_{n-2} q_{n-1})$
$= r_{n-2}(1 + q_n q_{n-1}) + r_{n-3}(-q_n)$
$= (r_{n-4} - r_{n-3} q_{n-2})(1 + q_n q_{n-1}) + r_{n-3}(-q_n)$
from this derivation we can show that the $gcd(a, b)$=r_n is the linear combination of r_{-1} and r_0 that is linear combination of a and b. From that linear combination we get the x and y. such that $gcd(a, b) = ax + by$.

Example 1
$a = 65$ and $b = 40$
Step 1:The Euclidean algorithm:
$65 = 1x40 + 25$
$40 = 1x25 + 15$
$25 = 1x15 + 10$
$15 = 1x10 + 5$
$10 = 2x5 + 0$
therefore $gcd(65, 40) = 5$
Step 2:Using the method of back-substitution:
$5 = 15 - 10$
$= 15 - (25 - 15)$
$= 2 * 15 - 25$
$= 2 * (40 - 25) - 25$
$= 2 * 40 - 3 * 25$
$= 2 * 40 - 3 * (65 - 40)$
$= 5 * 40 - 3 * 65$
$= 65 * (-3) + 40 * 5$
so $x = -3$ and $y = 5$.

Theorem 2.2 *a^{-1} mod n exists iif $gcd(a, n) = 1$.*

Proof: Suppose a^{-1} mod n exists, and is equal to x.
therefore $ax = 1$ mod n by defination.
$\Rightarrow ax = nq + 1$, for some q.
$\Rightarrow ax + n(-q) = 1$
$\Rightarrow 1 = min\{ax + ny : ax + ny > 0\} = gcd(a, n)$ by Theorem 2.1

Suppose $gcd(a, n) = 1$
By Theorem 2.1,$\exists x^\star, y^\star$ s.t.

$ax^\star + ny^\star = 1$
$\Rightarrow ax^\star = 1 \bmod n$
$\Rightarrow x^\star = a^{-1} \bmod n$, by definition.

■

(1) Given a and n s.t. $gcd(a, n) = 1$, how to find a^{-1} mod n.
Ans. Use extended Euclid's Algorithm

2.2 Affine cipher

$e_k(x) = (ax + b) \bmod n$; $k = (a, b)$ s.t. $gcd(a, n) = 1$.
$d_k(y)$=$a^{-1}(y - b) \bmod n$, $k = (a, b)$ s.t. $gcd(a, n) = 1$.
$\mid Keyspace \mid$= (number of $b's$) * (the number that is less than n and relatively prime to n). $= n * \phi(n)$.
$\phi(n)$ is the euler's totient function. $\phi(n)$=$\mid \{1 \leq x < n : gcd(a, n) = 1\} \mid$

2.3 Hill cipher

Hill cipher message encryption done block by block. Say block size m. plaitext message $x_1, x_2, ..., x_m, x_{m+1}, x_{m+2}, ..., x_{2m}$,. and ciphertext $y_1, y_2, ..., y_m, y_{m+1}, y_{m+2}, ..., y_{2m}$,...

$$\begin{bmatrix} y_1 \\ y_2 \\ . \\ . \\ . \\ y_m \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & . & . & . & k_{1m} \\ k_{21} & k_{22} & . & . & . & k_{2m} \\ . & & & & & \\ . & & & & & \\ . & & & & & \\ k_{m1} & k_{m2} & . & . & . & k_{mm} \end{bmatrix} \times \begin{bmatrix} x_1 \\ x_2 \\ . \\ . \\ . \\ x_m \end{bmatrix}$$

Hill cipher decryption done by multiply invertible matrix. $X_{m\times 1} = K^{-1}_{m\times m} \times Y_{m\times 1}$. Key space of the Hill cipher is the number of $m * m$ invertable matrix if the block size is m.

2.4 Substitution cipher

In substitution cipher one symbol in the plain text substitute by another letter in the alphabet.
Key space in the subtitution cipher is the all possible permutation of the alphbet set. In english apbhabet key space is $26! \approx 4 * 10^{26}$

2.5 Models of attack

(1) **Ciphertext only**
In this model of attack adversary has access only to the ciphertext, and has no access to the plaintext. This type of attack is the most likely case encountered in real life cryptanalysis, but is the weakest attack because of the advarsary's lack of information.

(2) **Known plaintext**
In this model of attack adversary has access to at list a limited number of pairs of plaintext and the corresponding ciphered text.
(3) **Chosen plaintext**
In this model attack the adversary is able to choose a number of plaintexts to be enciphered and have access to the resulting ciphertext. This allows him to explore whatever areas of the plaintext state space he wishes and may allow him to exploit vulnerabilities and nonrandom behavior which appear only with certain plaintexts. In the widely used public-key cryptosystems, the key used to encrypt the plaintext is publicly distributed and anyone may use it, allowing the cryptanalyst to create ciphertext of any plaintext he wants. So public-key algorithms must be resistant to all chosen-plaintext attacks.
(4) **chosen ciphertext**
In this model attack the adversary can choose arbitrary ciphertext and have access to plaintext decrypted from it