Introduction to Cryptography CS 355

Lecture 6

Elementary Number Theory (2)

Lecture Outline

- The Extended Euclidian Algorithm
- Solving Linear Congruence
- The Affine Cipher
- The Chinese Remainder Theorem

Towards Extended Euclidian Algorithm

- **Theorem:** Given integers a, b > 0 and a < b, then d = gcd(a,b) is the least positive integer that can be represented as ax + by, x, y integer numbers.
- How to find such x and y?

The Extended Euclidian Algorithm

First computes	Then computes	And
$b = q_1 a + r_1$	$x_0 = 0$	$y_0 = 1$
$a = q_2 r_1 + r_2$	$x_1 = 1$	$y_1 = 0$
$r_1 = q_3 r_2 + r_3$	$x_2 = -q_1 x_1 + x_0$	$y_2 = -q_1 y_1 + y_0$
…	…	…
$r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$	$x_k = -q_{k-1} x_{k-1} + x_{k-2}$	$y_k = -q_{k-1} y_{k-1} + y_{k-2}$
$r_{k-2} = q_k r_{k-1}$		

We have $ax_k + by_k = r_{k-1} = \gcd(a,b)$

Extended Euclidian Algorithm

```
x=1;  y=0;  d=a;  r=0;  s=1;  t=b;
while (t>0) {
        q = ⌊d/t⌋
        u=x-qr;  v=y-qs;  w=d-qt
        x=r;      y=s;      d=t
        r=u;      s=v;      t=w
}
return (d, x, y)
```

Invariants:

$ax + by = d$

$ar + bs = t$

Another Way

Find gcd(143, 111)

$$143 = 1 \times 111 + 32$$
$$111 = 3 \times 32 + 15$$
$$32 = 2 \times 15 + 2$$
$$15 = 7 \times 2 + 1$$

$$\gcd(143, 111) = 1$$

$$32 = 143 - 1 \times 111$$
$$15 = 111 - 3 \times 32$$
$$= 4 \times 111 - 3 \times 143$$
$$2 = 32 - 2 \times 15$$
$$= 7 \times 143 - 9 \times 111$$
$$1 = 15 - 7 \times 2$$
$$= 67 \times 111 - 52 \times 143$$

Linear Equation Modulo n

If gcd(a, n) = 1, the equation

$$ax \equiv 1 \bmod n$$

has a unique solution, 0< x < n. This solution is often represented as a^{-1} mod n

Proof: if $ax_1 \equiv 1 \pmod n$ and $ax_2 \equiv 1 \pmod n$,
then $a(x_1-x_2) \equiv 0 \pmod n$, then $n \mid a(x_1-x_2)$,
then $n \mid (x_1-x_2)$, then $x_1-x_2=0$

How to compute a^{-1} mod n?

Linear Equation Modulo (cont.)

To solve the equation

$$ax \equiv b \bmod n$$

When gcd(a,n)=1, compute $x = a^{-1} b \bmod n$.
When gcd(a,n) = d >1, do the following

- If d does not divide b, there is no solution.
- Assume d|b. Solve the new congruence, get x_0

$$(a/d)x \equiv b/d \ (\bmod n/d)$$

- The solutions of the original congruence are
  x_0, $x_0+(n/d)$, $x_0+2(n/d)$, …, $x_0+(d-1)(n/d)$ (mod n).

The Affine Cipher

- A special case of monoalphabetical substitution cipher that strengthen the shift cipher slightly
- A key consists of two integers α and β in [0..25] such that gcd(α,26)=1.
- $E_{\alpha,\beta}[x] = \alpha x + \beta \pmod{26}$
- What is the key size?
- How to decrypt?
- How to do ciphertext only, known plaintext, chosen plaintext attack?

Chinese Reminder Theorem (CRT)

Theorem

Let $n_1, n_2, ,,, n_k$ be integers s.t. $\gcd(n_i, n_j) = 1$ for any $i \neq j$.

$$x \equiv a_1 \bmod n_1$$

$$x \equiv a_2 \bmod n_2$$

...

$$x \equiv a_k \bmod n_k$$

There exists a unique solution modulo $n = n_1 n_2 \ldots n_k$

Proof of CRT

- Consider the function χ: $Z_n \rightarrow Z_{n1} \times Z_{n2} \times \ldots \times Z_{nk}$
  $\chi(x) = (x \bmod n_1, \ldots, x \bmod n_k)$
- We need to prove that χ is a bijection.
- For $1 \le i \le k$, define $m_i = n / n_i$, then $\gcd(m_i, n_i) = 1$
- For $1 \le i \le k$, define $y_i = m_i^{-1} \bmod n_i$
- Define function $\rho(a1,a2,\ldots,ak) = \sum a_i m_i y_i \bmod n$, this function inverts χ
  - $a_i m_i y_i \equiv a_i \pmod{n_i}$
  - $a_i m_i y_i \equiv 0 \pmod{n_j}$ where $i \neq j$

An Example Illustrating Proof of CRT

- Example of the mappings:
  - $n_1=3$, $n_2=5$, $n=15$
  - $m_1=5$, $y_1=m_1^{-1} \bmod n_1=2$, $\quad 5¢2 \bmod 3 = 1$
  - $m_2=3$, $y_2=m_2^{-1} \bmod n_2=2$, $\quad 3¢2 \bmod 5 = 1$

  - $\rho(2,4) = (2 ¢ 5 ¢ 2 + 4 ¢ 3 ¢ 2) \bmod 15$
    $= 44 \bmod 15 = 14$
  - $14 \bmod 3 = 2$, $14 \bmod 5 = 4$

Example of CRT:

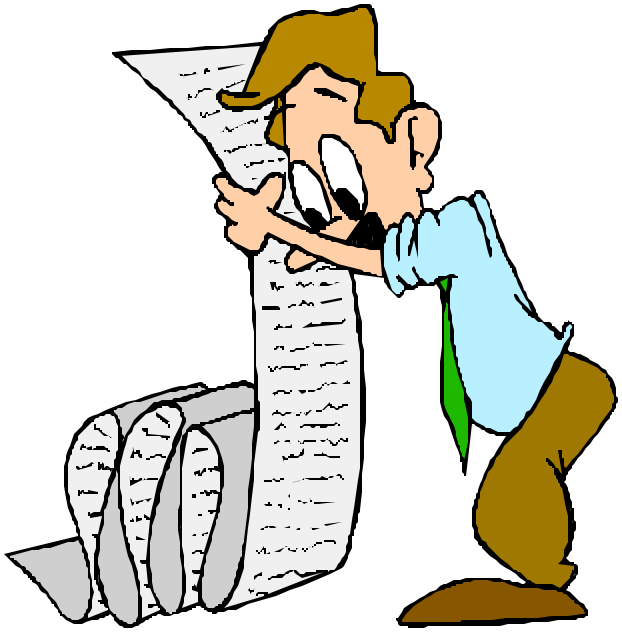
$x \equiv 5 \pmod 7$
$x \equiv 3 \pmod{11}$
$x \equiv 10 \pmod{13}$

- $n_1=7,\ n_2=11,\ n_3=13,\ n=1001$
- $m_1=143,\ m_2=91,\ m_3=77$
- $y_1=143^{-1} \bmod 7 = 3^{-1} \bmod 7 = 5$
- $y_2=91^{-1} \bmod 11 = 3^{-1} \bmod 11 = 4$
- $y_3=77^{-1} \bmod 13 = 12^{-1} \bmod 13 = 12$

- $x = (5\times143\times5 + 3\times91\times4 + 10\times77\times12) \bmod 1001$
  $= 13907 \bmod 1001 = 894$

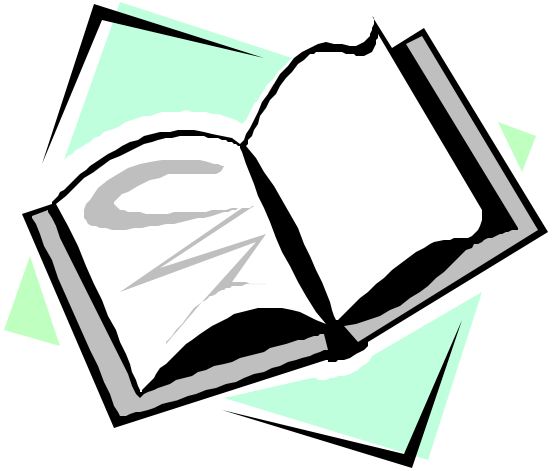
Summary

- Extended Euclidian Algorithm
- Solving linear congruence
- Affine Cipher
- Chinese Remainder Theorem



Summary of Recommended Readings up to This Lecture

- Trappe & Washington
  - Section 1
  - Section 2.1, 2.2, 2.3, 2.4, 2.12
  - Section 3.1, 3.2, 3.3, 3.4
- The Code Book
  - Chapters 1, 2, 3, 4



Coming Attractions …

- More on Attacking Enigma Machine
- Recommended reading for next lecture:
  - Facts and myths of Enigma: breaking stereotypes. By Kris Gaj and Arkadiusz Orlowski. In EuroCrypt 2003.