SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

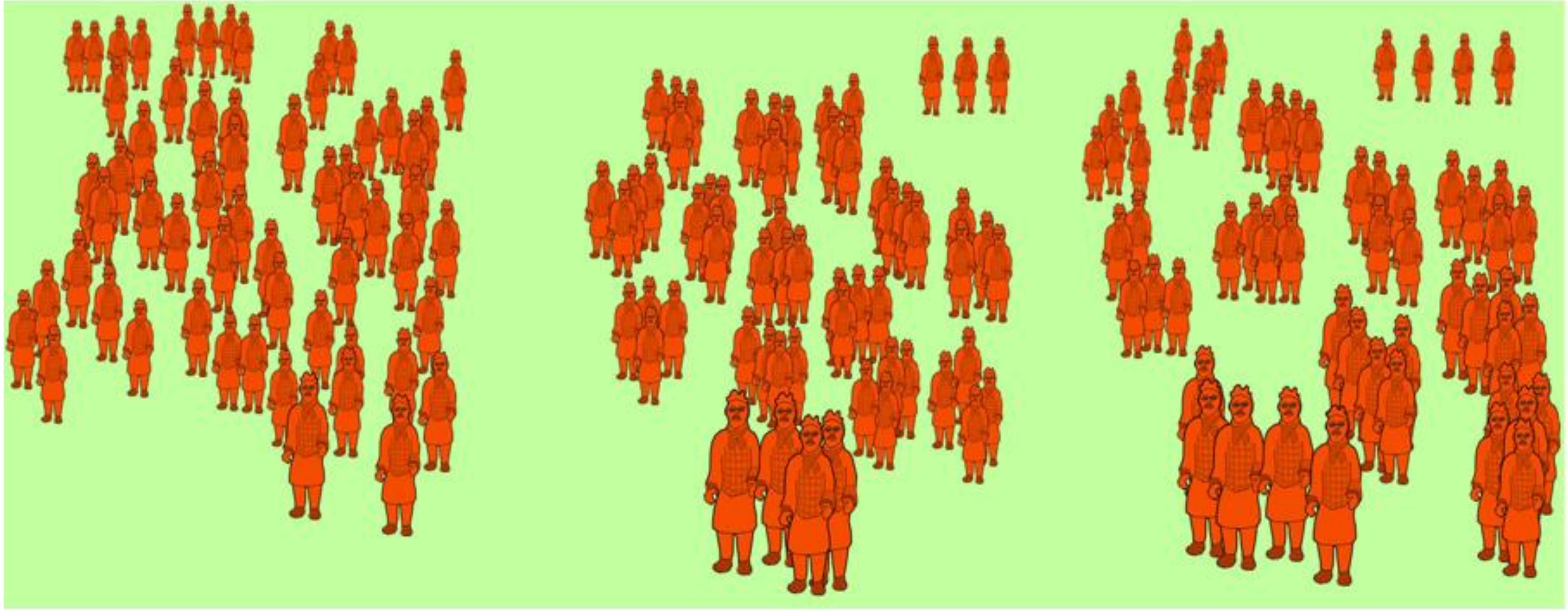
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE NAME : 19CS503 Cryptography and Network Security

III YEAR /V SEMESTER

Unit 3- Public Key Cryptography

Topic : The Chinese remainder theorem- Exponentiation and Logarithms



How many people
What is x?

Divided into 4s: remainder 3
$x \equiv 3 \pmod 4$

Divided into 5s: remainder 4
$x \equiv 4 \pmod 5$

Chinese Remainder Theorem

- used to speed up modulo computations
- if working modulo a product of numbers
  - eg. mod $M = m_1 m_2 .. m_k$
- Chinese Remainder - each moduli m_i works separately
- since computational cost is proportional to size, this is faster than working in the full modulus M

Chinese Remainder Theorem

- can implement CRT in several ways
- to compute A(mod M)
  - first compute all a_i = A mod m_i separately
  - determine constants c_i below, where $M_i = M/m_i$
  - then combine results to get answer using

$$A \equiv \left(\sum_{i=1}^{k} a_i c_i\right) (\bmod M)$$

$$c_i = M_i \times (M_i^{-1} \bmod m_i) \quad \text{for } 1 \leq i \leq k$$

Theorem: If $m_1, m_2, \ldots, m_k$ are relatively prime and $a_1, a_2, \ldots, a_k$ are integers, then

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

$$x \equiv a_k \pmod{m_k}$$

have a **unique** solution modulo m, where $m = m_1 m_2 \ldots m_k$. *(That is, there is a solution x with* $0 \le x < m$ and all other solutions are congruent modulo *m to this solution.)*

(1) Compute $m = m_1 m_2 \ldots m_n$.

(2) Determine $M_1 = m/m_1$; $M_2 = m/m_2$; … ; $M_n = m/m_n$

(3) Find the inverse of M_1 mod m_1, M_2 mod m_2 , …, M_n mod m_n which are y_1 , y_2 ,…, y_n ,

$$M_k y_k \equiv 1 \pmod{m_k}.$$

(4) Compute $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n$

(5) Solve $x \equiv y \pmod{m}$

Example : Solve the system of congruences

$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$

Solution:

(1) $m = 3 \cdot 5 \cdot 7 = 105$

(2) $M_1 = m/m_1 = 105/3 = 35$, $M_2 = 21$; $M_3 = 15$

(3) $y_1 = 2$ is an inverse of 35 mod 3 because $35 \equiv 2 \pmod 3$

$y_2 = 1$ is an inverse of 21 mod 5 because $21 \equiv 1 \pmod 5$

$y_3 = 1$ is an inverse of 15 mod 7 because $15 \equiv 1 \pmod 7$

(4) $x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$

(5) $233 \equiv$ **23** (mod 105)

$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$

a	2	3	2	
m	3	5	7	105
M	35	21	15	
	$2.y_1$	$1.y_2$	$1.y_3$	
y	2	1	1	
	2.35.2	3.21.1	2.15.1	233

$233 \equiv \mathbf{23} \pmod{105}$

We conclude that 23 is the smallest positive integer that:

$$23 \bmod 3 = 2$$
$$23 \bmod 5 = 3$$
$$23 \bmod 7 = 2$$

Power of integer modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Problems

- consider the powers of 7, modulo 19:
  - $7^1 = 7 \pmod{19}$
  - $7^2 = 49 = 11 \pmod{19}$
  - $7^3 = 343 = 1 \pmod{19}$
  - $7^4 = 2401 = 7 \pmod{19}$
  - $7^5 = 16807 = 11 \pmod{19}$

Activity

Discrete Logarithms

- Let g be the generator of the group Z_n^* . Given an element $y = g^x$ (mod n) the discrete logarithm is defined as $dlog_{n,g}(y) = x$.

Properties of logarithms

- $\log_a 1 = 0$
- $\log_a a = 1$
- $\log_a xy = \log_a x + \log_a y$
- $\log_a x^n = n\log_a x$

Properties of Discrete Logarithms

- $dlog_{n,g}(1) = 0$ $g^0 = 1 (\mathrm{mod}\ n)$
- $dlog_{n,g}(g) = 1$ $g^1 = g (\mathrm{mod}\ n)$
- $dlog_{n,g}(xy) = (dlog_{n,g}(x) + dlog_{n,g}(y)) \ (\mathrm{mod}(\Phi(n))$
- $dlog_{n,g}\ x^r = r\ dlog_{n,g}(x)\ (\mathrm{mod}\ \Phi(n))$

Assessment 1

1. The solution of the linear congruence 4x = 5(mod
   a) 6(mod 9)
   b) 8(mod 9)
   c) 9(mod 9)
   d) 10(mod 9)

2. The linear combination of gcd(252, 198) = 18 is?
   a) 252*4 – 198*5
   b) 252*5 – 198*4
   c) 252*5 – 198*2
   d) 252*4 – 198*4

REFERENCES

1. William Stallings, Cryptography and Network Security, 6 th Edition, Pearson Education, March 2013.
2. http://nptel.ac.in/courses/106103015/11
3. http://nptel.ac.in/courses/106103015/17

THANK YOU