SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

Course Code and Name : 19IT602– CRYPTOGRAPHY AND CYBER SECURITY

III YEAR / VI SEMESTER

Unit 3: ASYMMETRIC KEY CRYPTOGRAPHY

Topic : Chinese Remainder Theorem

Chinese Remainder Theorem

- used to speed up modulo computations
- if working modulo a product of numbers
  - eg. mod $M = m_1m_2..m_k$
- 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 $a_i = A \bmod m_i$ separately
  - determine constants c_i below, where $M_i = M/m_i$
  - then combine results to get answer using:

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

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

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:
  - $7^1 = 7 \pmod{19}$
  - $7^2 = 49 = 11 \pmod{19}$
  - $7^3 = 343 = 1 \pmod{19}$
  - $7^4 = 2401 = 7 \pmod{19}$
  - $7^5 = 16807 = 11 \pmod{19}$

Discrete Logarithms

- Let g be the generator of the group Z_n^* . Given an element $y = g^x \pmod{n}$ 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 $g^1 = g (\mathrm{mod}\ n)$
- $dlog_{n,g}(xy) = (dlog_{n,g}(x) + dlog_{n,g}(y)) \ (\mathrm{mod}(\Phi(n))$
- $dlog_{n,g}\ x^r = r\ dlog_{n,g}(x)\ (\mathrm{mod}\ \Phi(n))$

Reference

- http://nptel.ac.in/courses/106103015/11
- http://nptel.ac.in/courses/106103015/12