18/07/18

Cryptography and Coding Theory

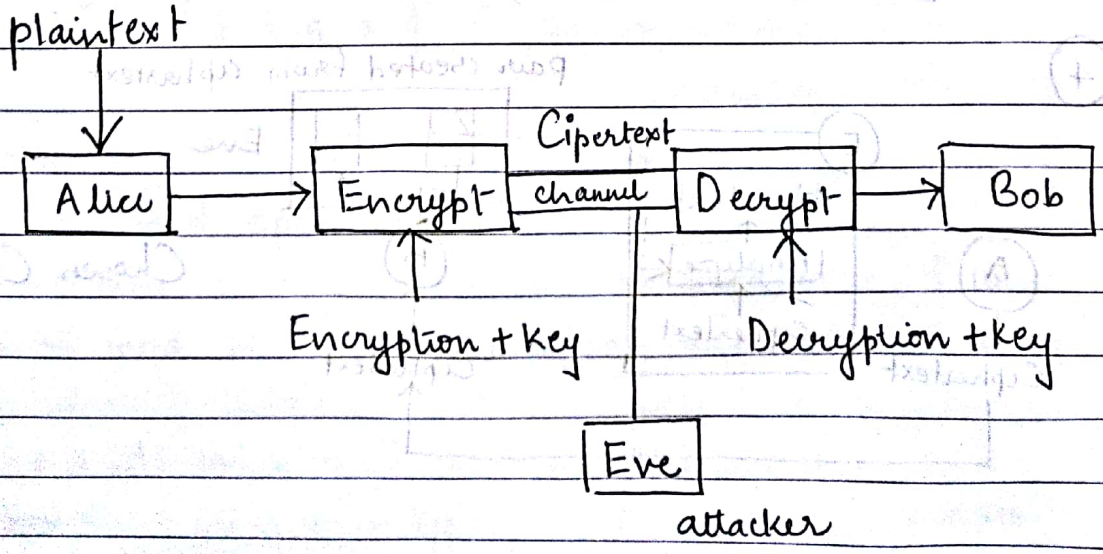
* Cryptology: study of communication over non-secure channels.
* Cryptography: process of designing systems to make channel secure.
* Cryptanalysis: deals with breaking secure systems.
* Coding Theory: deals with representing input information symbols with output information symbols called code symbols. It studies communication over noisy channels and how to ensure that the message received is a correct message as opposed to cryptography which protects communication over non-secure channels.

* Applications of CT

1. Secrecy
2. Compression
3. Errors Correction

20/7

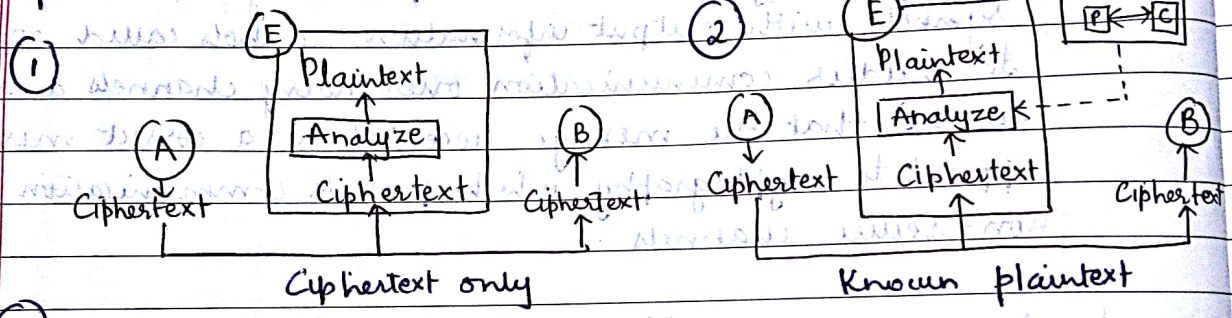
Classical CryptoSystem

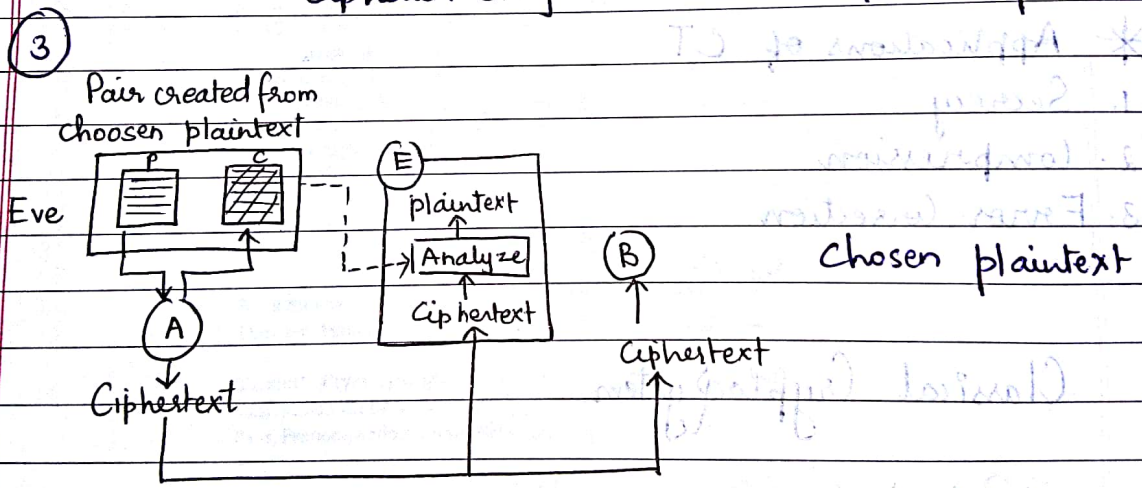


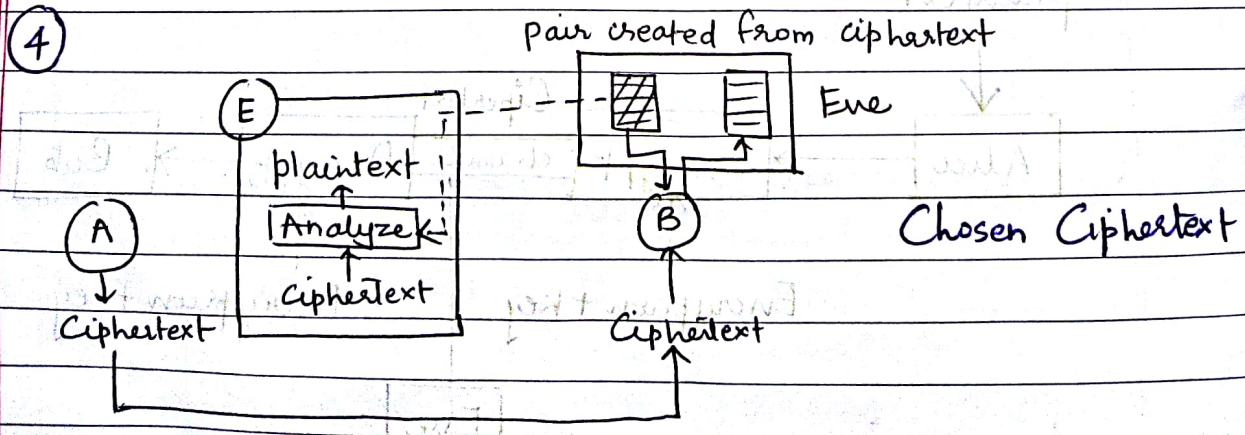
Scanned by CamScanner

* Types of Attack
  1. Ciphertext Only
  2. Known plaintext
  3. Chosen plaintext
  4. Chosen Ciphertext

(Eve)
→ She will try to read message, find key, alter message, pretend as Alice.







Scanned by CamScanner

classmate
Date
Page

* Applications of Cryptography
(1) Confidentiality
(2) Integrity
(3) Authentication → data Origin : creator of data
→ Entity:
Identification schemes
password protocols
(4) Non-Repudiation : no rejection

-18
+28
10

24/07 NUMBER THEORY

a) Divisibility

$a|b \quad b = aq + r$

Properties:
1. if $a|1$ then $a = \pm 1$
2. if $a|b$ and $b|a$ then $a = \pm b$
3. if $a|b$ and $b|c$ then $a|c$ (3, 15, 45)
4. if $a|b$ and $a|c$ then $a|(m \times b + n \times c)$ (3, 15, 9)

b) Modular Arithmetic

sets of residues (Z_n)

$Z_{10} = \{0 \ldots 9\}$ $Z_{16} = \{0 \ldots 15\}$

Z_n^* : {

$Z_{10}^* = \{2, 3, 5, 7\}$

$a \bmod n = r$

- perform mod operations

a) $27 \bmod 5 = 2$
b) $36 \bmod 12 = 0$
c) $-18 \bmod 14 = 10$ → $-4 \bmod 14 = 10 \bmod 14$
d) $-7 \bmod 10 = 3$

- add 7 to 14 in Z_{15} $= (7+14) \bmod 15 = 6$
- subtract 11 from 7 in Z_{13} $= (-4) \bmod 13 = 9$
- multiply 11 by 7 in Z_{20} $= 77 \bmod 20 = 17$

Scanned by CamScanner

27/07 Decryption of Affine

$y = \alpha x + \beta$

$x = (y - \beta)/\alpha$

$(9, 2) \rightarrow \quad x = \frac{1}{9}(y-2)$

$x = 9^{-1}(y-2) = 3(y-2) = 3y - 6$

$3y - 6 = (3y - 6 + 26) \bmod 26 = (3y + 20) \bmod 26$

- CVVWPM

C: $(3(2) + 20) \bmod 26 = 0 \Rightarrow a$

V: $(3(21) + 20) \bmod 26 = 5 \Rightarrow f$

W: $(3(22) + 20) \bmod 26 = 8 \Rightarrow i$

P: $(3(15) + 20) \bmod 26 = 13 \Rightarrow n$

M: $(3(12) + 20) \bmod 26 = 4 \Rightarrow e$

- (7, 2) ZEBBW

$x = 7^{-1}(y-2) = 15y - 30 = (15y + 22) \bmod 26$

Z: $(15 \times 25 + 22) \bmod 26 = 7 \Rightarrow h$

E: $(15 \times 4 + 22) \bmod 26 = 4 \Rightarrow e$

B: $(15 \times 1 + 22) \bmod 26 = 11 \Rightarrow l$

W: $(15 \times 22 + 22) \bmod 26 = 14 \Rightarrow o$

- (11, 2)

R: $(11 \times 17 + 2) \bmod 26 = 7 = H$; $(19 \times 7 + 14) \bmod 26 = 17 \Rightarrow r$

O: $(11 \times 14 + 2) \bmod 26 = 0 = A$; $(19 \times 0 + 14) \bmod 26 = 14 \Rightarrow o$

S: $(11 \times 18 + 2) \bmod 26 = 18 = S$; $(19 \times 18 + 14) \bmod 26 = 18 \Rightarrow s$

h: $(11 \times 7 + 2) \bmod 26 = 1 = B$; $(19 \times 1 + 14) \bmod 26 = 7 \Rightarrow h$

a: $(11 \times 0 + 2) \bmod 26 = 2 = C$; $(19 \times 2 + 14) \bmod 26 = 0 \Rightarrow a$

n: $(11 \times 13 + 2) \bmod 26 = 15 = P$; $(19 \times 15 + 14) \bmod 26 = 13 \Rightarrow n$

i: $(11 \times 8 + 2) \bmod 26 = 12 = M$; $(19 \times 12 + 14) \bmod 26 = 8 \Rightarrow i$

$x = 11^{-1}(y-2) = 19y - 38 = (19y + 14) \bmod 26$

Scanned by CamScanner

* Playfair Cipher

- We make use of a 5x5 matrix wherein we place the keyword Playfair in 5x5 form with the remaining letters of the alphabet ranging from 0 to 25
- i and j is considered same.

	0	1	2	3	4
0	P	L	A	Y	F
1	I	R	B	C	D
2	E	G	H	K	M
3	N	O	Q	S	T
4	U	V	W	X	Z

* Algorithm:

1. Remove spaces in the plaintext and divide the text in the group of 2 letters. If there is double letter appearing as a group insert an x and regroup
2. Add an extra x at the end to complete the last group. Group is called diagram
3. Encrypt each 2 letter group by:

→ If the 2 letters are not in same row or column replace each letter by the letter that is in its row and is in the column of the other letter.

→ If 2 letters are in same row, replace each letter by the letter immediately to it's right with the matrix wrapping around from the last column to the first row

→ If 2 letters are in same column, replace each letter by the letter immediately below it with the matrix wrapping around from the last row to the first

Ex Meet at the school house

Scanned by CamScanner

Encrypt Meet at the school house
meet at the es ch oo lh ou se
meet at the es ch ox ol ho us ex
⇒
EGMN FQQM KN BK SV VR GQ XN KU

- Hello i am coming to ponda
he lx lo ia mc om in gt op on da
KG YV RV BP KD TG EU MO NL QO BF

← OTP
One Time Pad
10110101 (i=18)
— Convert to binary form (sequence of 0's and 1's)
— mod 2 bit by bit (XOR)
— key is a random sequence of 0's and 1's
Once a key is used it is discarded and never used again

- plaintext: 00101001 Key: 10101100
perform XOR and generate cipher text

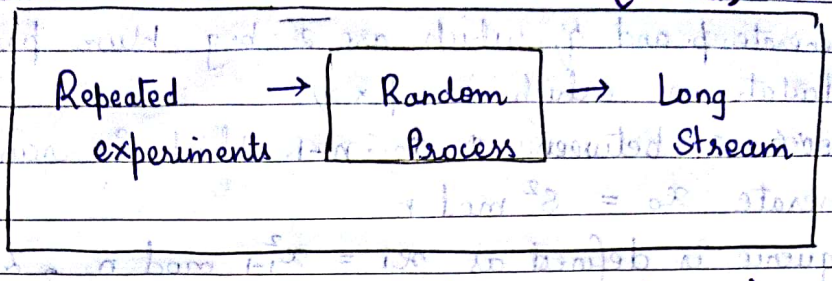
Encryption: 00101001 plaintext
⊕ 10101100 key
ciphertext= 10000101 ciphertext
⊕ 10101100 key
00101001 plaintext

Scanned by CamScanner

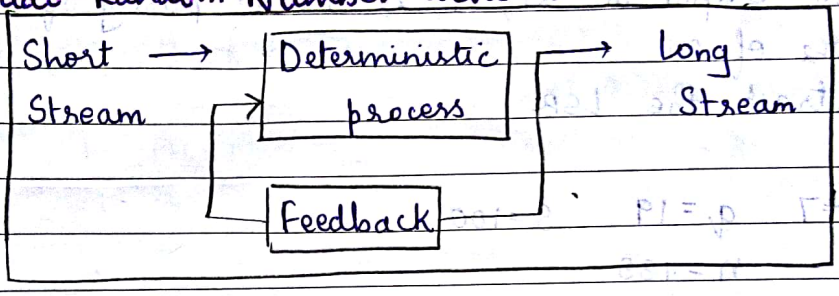
01/08

Random Number Generations

i) True Random Number Generator (TRNG)

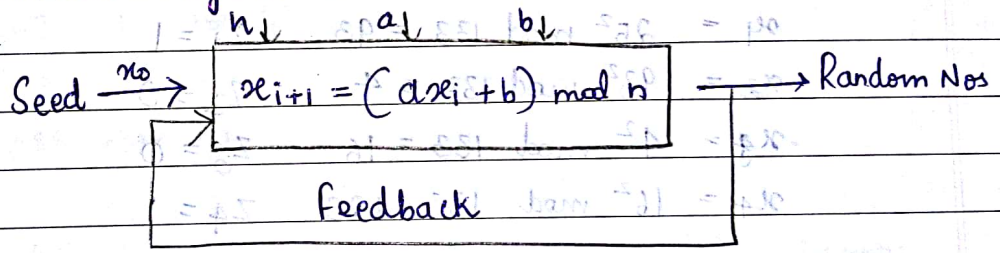


ii) Pseudo-Random Number Generator (PRNG)

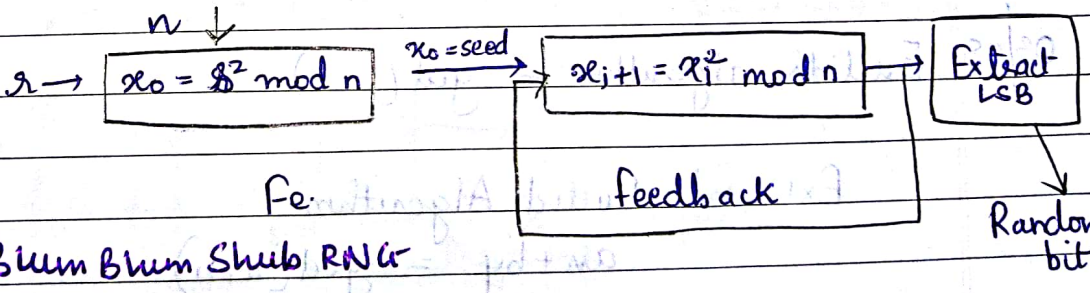


Linear Congruential RNG

a)



b)



Fe

Blum Blum Shub RNG

- Generate random no using LC RNG

$n = 17 \quad a = 4 \quad b = 5 \quad x_0 = 7$

$x_1 = (4 \times 7 + 5) \bmod 17 = 16 \quad x_2 = (4 \times 16 + 5) \bmod 17 = 1$

$x_3 = 9 \quad x_4 = 7$

16, 1, 9, 7, 16, 1, 9, 7

Scanned by CamScanner

* Algorithm of Blum Blum Shub / Quadratic Residue Generator

- Generate p and q which are 2 big blum prime numbers
- Calculate n which is $p \times q$
- Choose s between 1 to n-1 which is random seed
- Generate $x_0 = s^2 \bmod n$
- Sequence is defined as $x_i = x_{i-1}^2 \bmod n$, z_i = parity of x_i
- The output is z_1, z_2, z_3 where parity of x_i is defined as x_2 of x_i
- Extract the LSB

- $p = 7 \quad q = 19 \quad s = 100$
  $n = 133$
  $x_0 = 100^2 \bmod 133 = 25$
  $x_1 = 25^2 \bmod 133 = 93 \quad z_1 = 1$
  $x_2 = 93^2 \bmod 133 = 4 \quad z_2 = 0$
  $x_3 = 4^2 \bmod 133 = 16 \quad z_3 = 0$
  $x_4 = 16^2 \bmod 133 = 123 \quad z_4 = 1$

03/08 Euclid's algorithm → gcd(a,b)

Extended Euclid Algorithm
$an + by = \gcd(a,b)$

- Determine gcd(161,56)
  $161 = 56 \times 2 + 49$
  $56 = 49 \times 1 + 7$
  $49 = 7 \times 7 + 0 \quad \gcd(161,56) = 7$
  $161 = 56 \times 2 + 49 = 56 \times 2 + 56 - 7$
  $161 = 56 \times 3 - 7$
  $56 \times 3 - 161 = 7 = \gcd(161,56)$
  $\therefore x = -1 \quad y = 3$

Scanned by CamScanner

2560

classmate
Date
Page

*

Row	x	y	d	k
1	1	0	161	
2	0	1	56	2
3	1	-2	49	1
4	-1	3	7	7
5	8	-23	0	

$k_2 = d_1/d_2$

$x_3 = x_1 - (x_2 * k_2)$

$=$

$y_3 = y_1 - (y_2 * k_2) =$

$d_3 = d_1 - (d_2 * k_2) =$

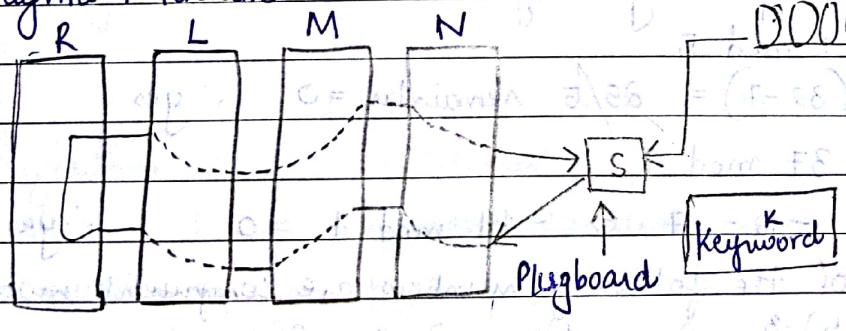
• gcd(2740, 1760)

Row	x	y	d	k
1	1	0	2740	
2	0	1	1760	1
3	1	-1	980	1
4	-1	2	780	1
5	2	-3	200	3
6	-7	11	180	1
7	9	-14	20	9
8	-88	137	0	

$2740(9) + 1760(-14)$

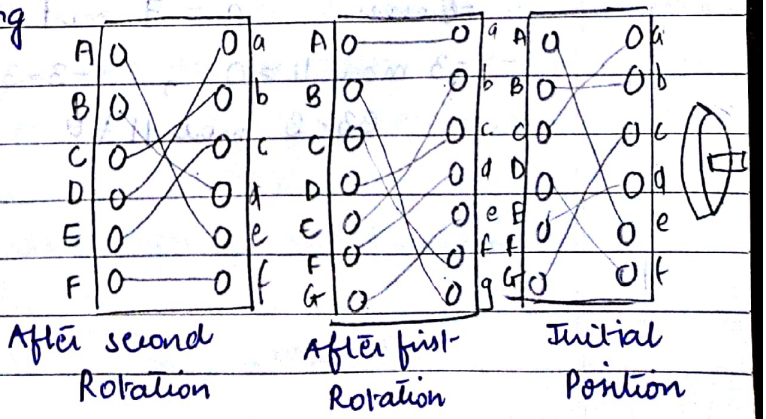
$= 20$

* Enigma Machine



R → Reversing drum (26 spring loaded contacts)

L, M, N → Rotors cipher



Scanned by CamScanner

Congruences

A congruence is used to study the properties of natural nos. Given an integer $n \geq 2$, two integers a and b are congruent modulo n if n divides a-b

$$a \equiv b \bmod n \text{ if } n \mid a-b$$

- $a = 41 \quad b = 21 \quad n = 10$

  $b \bmod n \quad 21 \bmod 10 \equiv 41$

  $\frac{(41-21)}{10}$ = remainder $\Rightarrow 0$

* If $a \equiv 0 \bmod n$ iff $n \mid a$
* $a \equiv a \bmod n$ (reflexibilty) $\forall a$.
* If $a \equiv b \bmod n$ then $b \equiv a \bmod n$ Symmetric.
* If $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $a \equiv c \bmod n$ Transitive

- Solve the following congruences.

1. $32 \equiv 7 \bmod 5$

   $(32-7) = 25/5$ remainder $= 0$ $\therefore$ yes.

2. $-12 \equiv 37 \bmod 7$

   $-12 - 37 \Rightarrow -49 \bmod 7 = 0$ $\therefore$ yes.

3. Which of the following numbers are congruent modulo 11 to 3?

   a) -8 b) -3 c) 8 d) 33 e) 36 f) 124

   $a = 3 \bmod 11$

   $-8-3 \bmod 11 = 0$, $-3-3 \bmod 11 \neq 0$ $8-3 \bmod 11 \neq 0$

   $33-3 \bmod 11 \neq 0$ $36-3 \bmod 11 = 0$ $124-3 \bmod 11 = 0$

Scanned by CamScanner

* Linear Congruences

$ax \equiv b \pmod n$

gcd(a,n) determines no of soln.

① $x+7 \equiv 3 \pmod{17}$

② $3x+2 \equiv 4 \pmod 5$

③ $2x+7 \equiv 3 \pmod{17}$

④ $5x+6 \equiv 13 \pmod{11}$

Determine possible values of x

→ ① $x \equiv 3-7 \pmod{17} \Rightarrow -4 \bmod 17$

$\gcd(1,17)=1 \quad x=13$

② $3x \equiv 2 \bmod 5$

$\gcd(3,5)=1 \quad x=4$

$3x-2 \bmod 5$ should be 0

$3x-2=10 \quad x=4$

③ $2x \equiv -4 \bmod 17$

$\gcd(2,17)=1 \quad \therefore x=15$

$2x+4 = 17\times 2$

$x+2=17 \quad x=15$

④ $5x = 7 \bmod 11$

$\gcd(5,11)=1 \quad \therefore x=8$

$5x-7 = 11\times 3$

$5x = 40 \quad x=8$

⑤ $3x = 6 \bmod 9$

$\gcd(3,9)=3 \quad x=2,5,8$

$3x-6 = 9$

* Algorithm

To solve a linear congruence equation of the form $ax \equiv b \bmod n$

An equation of this type might have no solution or a limited no of solution

Step1: assume $\gcd(a,n)=d$ if $d|b$ then there are d solutions

If $d|b$ following strategy is used to find soln

- Reduce the eqn by dividing both sides of eqn including mod by d
- Multiply both sides of reduce eqn by multiplicative inverse of 'a' to find particular soln x_0
- General soln are $x = x_0 + k(n/d)$ for $k < d-1$

Scanned by CamScanner

- $10x \equiv 2 \bmod 15$

  $\gcd(10, 15) = 5$

  $5 \nmid 2$ not possible

  $\therefore$ no solution

- $14x \equiv 12 \bmod 18$

  $\gcd(14, 18) = 2$

  $7x \equiv 6 \bmod 9$

  $\gcd(9, 7) = 1$ $\quad 7 \times b = 1 \bmod 9$ $\quad b = 4$ $\quad 28 \bmod 9 = 1$

  ~~$28x = 168$ mod 18~~

  $7x - 6 = 9 \times 4$ $\quad x_0 = 6$

  $x = 6 + 1(18/2) = 15$

$7x \equiv 6 \bmod 9$

$x = 6 \times 7^{-1} \bmod 9$

$x = 6 \times 4 \bmod 9 = 6$

10/08

a)

08/08

Determine $12x \equiv 21 \bmod 39$

$\gcd(12, 39) = 3$

$4x \equiv 7 \bmod 13$

$\frac{4 \times b}{13} = 1$

$b = 10$

$x = 7 \times 4^{-1} \bmod 13$

$x = 70 \bmod 13$

$\boxed{x_0 = 5}$

$x_1 = 5 + 1(39/3) = 5 + 13 = 18$

$x_2 = 5 + 2(13) = 31$

- a) $21x \equiv 42 \bmod 56$

  $\gcd(21, 56) = 7$

  b) $24 \equiv 42 \bmod 56$

  $\gcd(24, 56) = 8$

  c) $27x \equiv 42 \bmod 56$

  $\gcd(27, 56) = 1$

a) $3x \equiv 6 \bmod 8$

$\frac{3 \times b}{8} \quad b = 3$

$x = 6 \times 3^{-1} \bmod 8$

$x = 18 \bmod 8$

$x_0 = 2$

$x_1 = 2 + 1(56/7) = 10$

$x_2 = 2 + 2 \times 8 = 18$

$x_3 = 2 + 3 \times 8 = 26$

$x_4 = 34$ $\quad x_5 = 42$ $\quad x_6 = 50$

b) no soln. $42 \nmid 8 \neq 0$

c) $27x \equiv 42 \bmod 56$

$x = 42 \times 27^{-1} \bmod 56$

$x_0 = 42 \times 27 \bmod 56 = 14$

Scanned by CamScanner

• $7x \equiv 20 \bmod 47$ ans=23

$\gcd(7,47) = 1$ $\quad x = 20 \times 7^{-1} \bmod 47$

$x_0 = 20 \times 27 \bmod 47$

$x_0 = 23$

10/08 Find the solutions to the following linear congruences

a) $20x \equiv 4 \bmod 30$

$\gcd(20,30) = 10$

$4 \bmod 10 \neq 0$

$\therefore$ no soln

b) $20x \equiv 30 \bmod 4$

$\gcd(20,4) = 4$

$30 \bmod 4 \neq 0$

$\therefore$ no soln

c) $353x \equiv 254 \bmod 400$

$\gcd(353, 400) = 1$

$x_0 = 254 \times 353^{-1} \bmod 400$

$x_0 = 254 \times \quad \text{mod } 400 = 318$

$353x + 400y = 1$

$353 \times 17 + 400 \times 15 = 1$

$400 = 353 \times 1 + 47$

$353 = 47 \times 7 + 25$

$47 = 25 \times 1 + 22$

$25 = 22 \times 1 + 3$

$22 = 3 \times 7 + 1$

$3 = 25 - 22 \times 1$

$= 25 - (47 - 25 \times 1) \times 1$

$= 25 \times 2 - 47 \times 1$

$= (353 - 47 \times 7) \times 2 - 47 \times 1$

$= 353 \times 2 - 47 \times 15$

$= 353 \times 2 - (400 - 353 \times 1) \times 15$

$= 353 \times 17 + 400 \times (-15)$

$353x = 4318 \bmod 400$

$x_0 = 4318 \bmod 400$

$= 318$

d) $57x \equiv 87 \bmod 105$

$\gcd(57, 105) = 3$

$x_0 = 29 \times 19^{-1} \bmod 35$

$x_0 = 29 \times (-11) \bmod 35 = -319 \times 5 = 3$

$x_1 = 31 + 1(35) = 66$ $\quad 48 - (57 - 48) \times 5 = 3$

$x_2 = 31 + 2(35) = 101$ $\quad 48 - 57 \times 5 = -3$

$105 = 57 \times 1 + 48$

$57 = 48 \times 1 + 9$

$48 = 9 \times 5 + 3$

$9 = 3 \times 3 + 0$

$6(105 - 57) - 57 \times 5 = 3$ $\quad 6 \times 105 - 11 \times 57 = 3$

e) $64x \equiv 83 \bmod 105$

$\gcd(64, 105) = 1$

$x_0 = 83 \times 64^{-1} \bmod 105$

$105 = 64 \times 1 + 41$

$64 = 41 \times 1 + 23$

$41 = 23 \times 1 + 18$

$23 = 18 \times 1 + 5$

$18 = 5 \times 3 + 3$

$5 = 3 \times 1 + 2$

$3 - 2 = 1$

$3 - (5 - 3) = 1$

$(18 - 5 \times 3) \times 2 - 5 = 1$ $\quad 18 \times 2 - 5 \times 7 = 1$

$(41 - 23) \times 2 - (23 - 18) \times 7 =$

$(41 - 23) \times 2 - (23 - 41 + 23) \times 7 =$

$41 \times 9 - 23 \times 16$

Scanned by CamScanner

10013

11/43

14/08

$41 \times 9 - 25 \times 16 = 1$

$41 \times 9 - (64 - 41) \times 16 = 1$

$41 \times 25 - 64 \times 16 = 1$

$(105 - 64) \times 25 - 64 \times 16 = 1$

$105 \times 25 - 64 \times 41 = 1$

$x_0 = 83 \times (-41) \bmod 105$

$x_0 = 62$

f) $589x \equiv 209 \bmod 817$

$\gcd(589, 817) = 19$

$x_0 = 11 \times 31^{-1} \bmod 43$

$x_0 = 11 \times (-15) \bmod 43$

$x_0 = 17$

$x_1 = 17 + 1($

$95 = 38 \times 2 = 19$

$95 - (133 - 95) \times 2 = 19$

$95 \times 3 - 133 \times 2 = 19$

$(228 - 133) \times 3 - 133 \times 2 = 19$

$228 \times 3 - 133 \times 5 = 19$

$228 \times 3 - (589 - 228 \times 2) \times 5$

$= 228 \times 13 - 589 \times 5$

$= (817 - 589) \times 13 - 589 \times 5$

$= 817 \times 13 - 589 \times 18 = 19$

$817 = 589 \times 1 + 228$

$589 = 228 \times 2 + 133$

$228 = 133 \times 1 + 95$

$133 = 95 \times 1 + 38$

$95 = 38 \times 2 + 19$

$38 = 19 \times 2 + 0$

$57x \equiv 87 \bmod 105$ deleme

$\gcd(\,) = 3$

$x = -11 \quad y = 6$

$87 = 29 \times 3$

$29 \times -11 = -319 \bmod 105$

$x_0 = 101$

$x = 29 \times -11 = -319$

$y = 29 \times 6 = 174$

Scanned by CamScanner

14/08

Multiplicative Inverse

1. $11^{-1} \bmod 26$

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	0		-7	26	

$q = r_1 / r_2$

$r = r_1 - (r_2 \times q)$

$t = t_1 - (t_2 \times q)$

Chinese Remainder Theorem

If $n_1, n_2, n_3 \cdots n_k$ are pairwise relatively prime numbers and $r_1, r_2 \cdots r_k$ are any numbers, then there exists a value of x satisfying the simultaneous congruences.

$$x \equiv r_1 \pmod{n_1}$$
$$x \equiv r_2 \pmod{n_2}$$
$$x \equiv r_k \pmod{n_k}$$

Furthermore x is unique modulo $n_1 n_2 \cdots n_k$

Let $n = n_1 \cdot n_2 \cdots n_k$ there exists for $1 \le i \le k$ a number s_i such that $(n/n_i) s_i \equiv r_i \pmod{n_i}$

$$x = \sum_{i=1}^{k} \frac{n}{n_i} s_i$$

- $x \equiv 2 \bmod 4$

  $x \equiv 3 \bmod 5$

  $x \equiv 7 \bmod 9$

$\Rightarrow$ $r_1 = 2 \quad r_2 = 3 \quad r_3 = 7 \quad n_1 = 4 \quad n_2 = 5 \quad n_3 = 9$

$n = n_1 \cdot n_2 \cdot n_3 = 180$

$i=1 \quad \frac{n}{n_1} \times s_1 = \frac{180}{4} \times s_1 \equiv 2 \bmod 4 \quad 45 s_1 \equiv 2 \bmod 4$

$s_1 = 2$

$i=2 \quad \frac{180}{5} \times s_2 \equiv 3 \bmod 5 \quad 36 s_2 = 3 \bmod 5 \quad s_2 = 3$

$i=3 \quad \frac{180}{9} \times s_3 \equiv 7 \bmod 9 \quad 20 s_3 \equiv 7 \bmod 9 \quad s_3 = 8$

Scanned by CamScanner

$x = (45s_1 + 36s_2 + 20s_3) \bmod 180$

$x = 358 \bmod 180$

$358 \bmod 180 = 178$

$\therefore x \equiv 5 \bmod 7$ $\quad r_1 = 5,\ r_2 = 7,\ r_3 = 3$

$x \equiv 7 \bmod 11$ $\quad n_1 = 7,\ n_2 = 11,\ n_3 = 13$

$x \equiv 3 \bmod 13$

$n = 1001$

$i=1$ $\quad \frac{1001}{7} s_1 \equiv 5 \bmod 7$ $\quad 143 s_1 \equiv 5 \bmod 7$ $\quad s_1 = 4$

$i=2$ $\quad \frac{1001}{11} s_2 \equiv 7 \bmod 11$ $\quad 91 s_2 \equiv 7 \bmod 11$ $\quad s_2 = 6$

$i=3$ $\quad \frac{1001}{13} s_3 \equiv 3 \bmod 13$ $\quad 77 s_3 \equiv 3 \bmod 13$ $\quad s_3 = 10$

$x = (143 \times 4 + 91 \times 6 + 77 \times 10) \bmod 1001$

$x = 1888 \bmod 1001 = 887$

21/08 Congruences for $x^2 \equiv a \bmod n$

$x^2 \equiv 1 \bmod 35$

$35 = 7 \times 5$

$x^2 \equiv 1 \bmod 5$

$x^2 \equiv 1 \bmod 7$

count the no of primes $r=2$ no of soln 2^r $\quad 2^2 = 4$

$x^2 \equiv 1 \bmod 5$

$0^2 \equiv 1 \bmod 5$ ✗

$1^2 \equiv 1 \bmod 5$ ✓

$2^2 \equiv 1 \bmod 5$ ✗

$3^2 \equiv 1 \bmod 5$ ✗

$4^2 \equiv 1 \bmod 5$ ✓

$\Rightarrow x \equiv 1 \bmod 5$

$x \equiv 4 \bmod 5$

$x^2 \equiv 1 \bmod 7$

$0^2 \equiv 1 \bmod 7$ ✗

$1^2 \equiv 1 \bmod 7$ ✓

$2^2 \equiv 1 \bmod 7$ ✗ $\Rightarrow x \equiv 1 \bmod 7$

$3^2 \equiv 1 \bmod 7$ ✗ $\quad x \equiv 6 \bmod 7$

$4^2 \equiv 1 \bmod 7$ ✗

$5^2 \equiv 1 \bmod 7$ ✗

$6^2 \equiv 1 \bmod 7$ ✓

Scanned by CamScanner

$x \equiv 1 \bmod 7$
$x \equiv 1 \bmod 5$
$n = 35$
$\frac{35}{7} S_1 \equiv 1 \bmod 7$
$5 S_1 \equiv 1 \bmod 7$
$S_1 = 3$
$\frac{35}{5} S_2 = 1 \bmod 5$
$7 S_2 \equiv 1 \bmod 5$
$S_2 = 3$
$x = (5 \times 3 + 7 \times 3) \bmod 35$
$x = 1$

$x \equiv 1 \bmod 5$
$x \equiv 6 \bmod 7$
$n = 35$
$\frac{35}{7} S_1 = 1 \bmod 7$
$S_1 = 4$
$7 S_2 \equiv 1 \bmod 5$
$S_2 = 3$
$x = 5 \times 4 + 3 \times 7$
$= 41 \bmod 35$
$x = 6$

$x \equiv 1 \bmod 7 \quad x \equiv 4 \bmod 5$
$5 S_1 = 1 \bmod 7$
$S_1 = 3$
$7 S_2 \equiv 4 \bmod 5$
$S_2 = 2$
$x = 3 \times 5 + 2 \times 7 \bmod 35$
$x = 29$

$x \equiv 4 \bmod 5$
$x \equiv 6 \bmod 7$
$n = 35$
$x = 2 \times 7 + 4 \times 5 \bmod 35$
$x = 34$

2. $x^2 - 34 \equiv 0 \bmod 495$
$x^2 \equiv 34 \bmod 495$
$495 = 5 \times 11 \times 3 \times 3 = 5 \times 9 \times 11$. $2^3 = 8$ sols.

$x^2 \equiv 34 \bmod 5$
$0^2 \equiv 34 \bmod 5$ ✗
$2^2 \equiv 34 \bmod 5$ ✓
$3^2 \equiv 34 \bmod 5$ ✓

$x^2 \equiv 34 \bmod 9$
$4^2 \equiv 34 \bmod 9$
$5^2 = 34 \bmod 9$

$x^2 \equiv 34 \bmod 11$
$1^2 \equiv 34 \bmod 11$
$10^2 \equiv 34 \bmod 11$

⇒ ① $x \equiv 2 \bmod 5$
$x \equiv 4 \bmod 9$
$x \equiv 1 \bmod 11$

② $x \equiv 2 \bmod 5$
$x \equiv 4 \bmod 9$
$x \equiv 10 \bmod 11$

③ $x \equiv 2 \bmod 5$
$x \equiv 5 \bmod 9$
$x \equiv 1 \bmod 11$

④ $x \equiv 2 \bmod 5$
$x \equiv 5 \bmod 9$
$x \equiv 10 \bmod 11$

99S1

Scanned by CamScanner

24/08

(5) $x \equiv 3 \bmod 5$
$x \equiv 4 \bmod 9$
$x \equiv 1 \bmod 11$

(6) $x \equiv 3 \bmod 5$
$x \equiv 4 \bmod 9$
$x \equiv 10 \bmod 11$

(7) $x \equiv 3 \bmod 5$
$x \equiv 5 \bmod 9$
$x \equiv 1 \bmod 11$

(8) $x \equiv 3 \bmod 5$
$x \equiv 5 \bmod 9$
$x \equiv 10 \bmod 11$

(1) $99 s_1 \equiv 2 \bmod 5$ $\quad s_1 = 3$
$55 s_2 \equiv 4 \bmod 9$ $\quad s_2 = 4$
$45 s_3 \equiv 1 \bmod 11$ $\quad s_3 = 1$
$x \equiv 99 \times 3 + 55 \times 4 + 45 \times 1 \bmod 495$
$x = 67$

(2) $99 s_1 \equiv 2 \bmod 5$ $\quad s_1 = 3$
$55 s_2 \equiv 4 \bmod 9$ $\quad s_2 = 4$
$45 s_3 \equiv 10 \bmod 11$ $\quad s_3 = 10$
$x = 99 \times 3 + 55 \times 4 + 45 \times 10 \bmod 495$
$x = 967 \bmod 495 = 472$

(3) $99 s_1 \equiv 2 \bmod 5$ $\quad s_1 = 3$
$55 s_2 \equiv 5 \bmod 9$ $\quad s_2 = 5$
$45 s_3 \equiv 1 \bmod 11$ $\quad s_3 = 1$
$x = 99 \times 3 + 55 \times 5 + 45 \times 1 \bmod 495$
$x = 617 \bmod 495 = 122$

(4) $99 s_1 \equiv 2 \bmod 5$ $\quad s_1 = 3$
$55 s_2 \equiv 5 \bmod 9$ $\quad s_2 = 5$
$45 s_3 \equiv 10 \bmod 11$ $\quad s_3 = 10$
$x \equiv 1022 \bmod 495 = 32$

(5) $99 s_1 \equiv 3 \bmod 5$ $\quad s_1 = 2$
$x = 99 \times 2 + 55 \times 4 + 45 \times 1 = 463$

(6) $x \equiv 99 \times 2 + 55 \times 4 + 45 \times 10 \bmod 495 = 373$

(7) $x = 99 \times 2 + 55 \times 5 + 45 \times 1 = 23$ → $518 \bmod 495$

(8) $x \equiv 99 \times 2 + 55 \times 5 + 45 \times 10 \bmod 495 = 428$

Scanned by CamScanner

24/08 Solve the congruence $x^2 \equiv 1 \bmod 40$ using CRT

$40 = 2 \times 2 \times 2 \times 5 = 8 \times 5$ $\quad 2^2 = 4$ solns

$x \equiv 1 \bmod 8$ $\quad x \equiv 1 \bmod 5$

$x \equiv 3 \bmod 8$ $\quad x \equiv 4 \bmod 5$

$x \equiv 5 \bmod 8$

$x \equiv 7 \bmod 8$

(1)

$x \equiv 1 \bmod 8$
$x \equiv 1 \bmod 5$
$5s_1 \equiv 1 \bmod 8$
$s_1 = 5$
$8s_2 \equiv 1 \bmod 5$
$s_2 = 2$
$x \equiv 5 \times 5 + 8 \times 2$
$\boxed{x = 1}$

$x \equiv 1 \bmod 8$
$x \equiv 4 \bmod 5$
$5s_1 = 1 \bmod 8$
$s_1 = 5$
$8s_2 = 4 \bmod 5$
$s_2 = 3$
$x = 5 \times 5 + 8 \times 3$
$\boxed{x = 49}$

$x \equiv 3 \bmod 8$
$x \equiv 1 \bmod 5$
$5s_1 = 3 \bmod 8$
$s_1 = 7$
$8s_2 = 1 \bmod 5$
$s_2 = 2$
$x = 5 \times 7 + 8 \times 2$
$\boxed{x = 11}$

$x \equiv 3 \bmod 8$
$x \equiv 4 \bmod 5$
$5s_1 = 3 \bmod 8$
$s_1 = 7$
$8s_2 = 4 \bmod 5$
$s_2 = 3$
$x = 5 \times 7 + 8 \times 3$
$\boxed{x = 19}$

$x \equiv 5 \bmod 8$
$x \equiv 1 \bmod 5$
$5s_1 = 5 \bmod 8$
$s_1 = 1$
$8s_2 = 1 \bmod 5$
$s_2 = 2$
$x = 5 \times 1 + 8 \times 2$
$\boxed{x = 21}$

$x \equiv 5 \bmod 8$
$x \equiv 4 \bmod 5$
$5s_1 = 5 \bmod 8$
$s_1 = 1$
$8s_2 = 4 \bmod 5$
$s_2 = 3$
$x = 5 \times 1 + 8 \times 3$
$\boxed{x = 29}$

$x \equiv 7 \bmod 8$
$x \equiv 1 \bmod 5$
$5s_1 = 7 \bmod 8$
$s_1 = 3$
$8s_2 = 1 \bmod 5$
$s_2 = 2$
$x = 5 \times 3 + 8 \times 2$
$\boxed{x = 31}$

$x \equiv 7 \bmod 8$
$x \equiv 4 \bmod 5$
$5s_1 = 7 \bmod 8$
$s_1 = 3$
$8s_2 = 4 \bmod 5$
$s_2 = 3$
$5 \times 3 + 8 \times 3$
$\boxed{x = 39}$

- $x^2 \equiv 36 \bmod 77$

$77 = 7 \times 11$

$x \equiv 36 \bmod 7$
$x \equiv 1 \bmod 7$
$x \equiv 6 \bmod 7$

$x \equiv 36 \bmod 11$
$x \equiv 5 \bmod 11$
$x \equiv 6 \bmod 11$

Scanned by CamScanner

$x \equiv 6 \bmod 7$	$x \equiv 6 \bmod 7$	$x \equiv 1 \bmod 7$	$x \equiv 6 \bmod 7$
$x \equiv 5 \bmod 11$	$x \equiv 5 \bmod 11$	$x \equiv 6 \bmod 11$	$x \equiv 6 \bmod 11$
$11 s_1 = 1 \bmod 7$	$11 s_1 = 6 \bmod 7$	$11 s_1 = 1 \bmod 7$	$11 s_1 = 6 \bmod 7$
$s_1 = 2$	$s_1 = 5$	$s_1 = 2$	$s_1 = 5$
$7 s_2 = 5 \bmod 11$	$7 s_2 = 5 \bmod 11$	$7 s_2 = 6 \bmod 11$	$7 s_2 = 6 \bmod 11$
$s_2 = 7$	$s_2 = 7$	$s_2 = 4$	$s_2 = 4$
$x = 11 \times 2 + 7 \times 7$	$x = 11 \times 5 + 7 \times 7$	$x = 11 \times 2 + 7 \times 4$	$x = 11 \times 5 + 7 \times 4$
$\boxed{x = 71}$	$\boxed{x = 27}$	$\boxed{x = 50}$	$\boxed{x = 6}$

Note:

* Euler Totient function or Euler phi function $\phi(n)$

Rules

1. $\phi(1) = 0$
2. $\phi(p) = p - 1$ if p is prime
3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime
4. $\phi(p^e) = p^e - p^{e-1}$ if p is prime.

It finds the no of intigers that are both smaller than 'n' and relatively prime to n.

- what is the value of $\phi(13)$?

$$\phi(13) = 13 - 1 = 12$$

- $\phi(10) = \phi(2) \times \phi(5) = (2-1)(5-1) = 4$

- $\phi(240) = \phi(2^4 \times 3 \times 5)$

$$= \phi(2^4) \times \phi(3) \times \phi(5)$$

$$= (2^4 - 2^3)(2)(4) = 64$$

- $\phi(49) = \phi(7^2) = 7^2 - 7$

$$= 42$$

Scanned by CamScanner

Note: If n can be factored as $n = p_1^{e_1} \times p_2^{e_2} \times \dots p_k^{e_k}$ then we can combine the third and fourth rule as

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \times (p_2^{e_2} - p_2^{e_2-1}) \dots$$

- $\phi(14) = \phi(7) \times \phi(2) = 6$
- $\phi(29) = 28$
- $\phi(32) = \phi(2^5) = 2^5 - 2^4 = 16$
- $\phi(80) = \phi(2^4) \times \phi(5) = (2^4 - 2^3) \times 4 = 32$
- $\phi(100) = \phi(2^2) \times \phi(5^2) = (2^2 - 2)(5^2 - 5) = 2 \times 20 = 40$
- $\phi(101) = 100$

* Fermat's Little Thuorem

a) First Version

if p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$ and a is an integer.

b) Second Version

$a^p \equiv a \bmod p$

28/08 $\phi(10) = \phi(2) \times \phi(5) = 4$

$\phi(120) = \phi(2^3) \times \phi(3) \times \phi(5) = (2^3 - 2^2)(2)(4) = 4 \times 2 \times 4 = 32$

Scanned by CamScanner

* $\phi(26) = \phi(13) \times \phi(2) = 12$

- find the result of $6^{10} \bmod 11$

$a=6 \quad p=11 \quad p-1=10$

$6^{10} \Rightarrow a^{p-1}$

$6^{10} \bmod 11 = 1$

- $2^{43210} \bmod 101$

$p = 101$ is prime $\quad p-1 = 100$

$2^{100} \equiv 1 \bmod 101$

$2^{43210} = (2^{100})^{4321} \cdot 2^{10} \bmod 101$

$2^{43210} \bmod 101 = (1)^{432} \cdot 2^{10} \bmod 101 = 2^{10} \bmod 101$

$1024 \bmod 101 = 14$

- $3^{12} \bmod 11 \quad p-1 = 10$

$(3^{10}) \cdot 3^2 \bmod 11$

$\because 1 = 1 \cdot 3^2 \bmod 11 = 9$

- $(46)^{120} \bmod 67 \quad p-1 = 66$

$48^{66} \cdot 48^{54} \bmod 67$

$1 \cdot 48^{54} \bmod 67$ $\quad (48^2)^{66} \cdot 48^{-12} \bmod 67$

* Application : Multiplicative Inverse

If the mod value is prime and a is integer such that p does not divides a

then $a^{-1} \bmod p = a^{p-2} \bmod p$.

- $8^{-1} \bmod 17 \quad$ and $b = 15$.

$a^{p-2} \bmod p = a^{15} \bmod 17$

$= 8^{15} \bmod 17$

Scanned by CamScanner

- $5^{-1} \bmod 23 = 14$
- $60^{-1} \bmod 101 = 32$
- $22^{-1} \bmod 211 = 48$

- Using Fermat's little theorem

a) $3^{31} \bmod 7 = (3^6)^5 \cdot 3 \bmod 7$
$= 3$

b) $4^{532} \bmod 11 = (4^{10})^{53} \cdot 4^2 \bmod 11 = 5$

c) $2^{50} \bmod 17 = (2^{16})^3 \cdot 2^2 \bmod 17 = 4$

d) $2^{53} \bmod 11 = (2^{10})^5 \cdot 2^3 \bmod 11 = 8$

e) $5^{15} \bmod 13 = 5^{12} \cdot 5^3 \bmod 13 = 8$

f) $15^{18} \bmod 17 = 15^{16} \cdot 15^2 \bmod 17 = 4$

g) $(456)^{17} \bmod 17 = (456)^{16} \cdot 456 \bmod 17 = 14$

h) $(145)^{102} \bmod 101 = (145)^{100} \cdot 145^2 \bmod 101 = 17$

* Euler's Theorem

⇒ Generalisation of Fermat's little Theorem

The modulus in the fermat is prime, Modulus in the Euler's Theorem is Integer (n)

(i) If $GCD(a, n) = 1$ we can say, $a^{\phi(n)} \equiv 1 \bmod n$

(ii) It removes the condition that a and n should be co-prime
i.e. if $n = p \times q$ and $a < n$ then $a^{k \times \phi(n)} + 1 \equiv a \bmod n$ k is integer

Scanned by CamScanner

29/08 -

- $6^{24} \bmod 35$

$a = 6 \quad n = 35 \quad \gcd(6, 35) = 1$

$\phi(35) = 6 \times 4 = 24$

$$\boxed{6^{24} \bmod 35 = 1}$$

- $8^{59} \bmod 77$

$a = 8 \quad n = 77 \quad \gcd = 1$

$\phi(77) = 6 \times 10 = 60$

$8^{59} \bmod 77$

$\Downarrow \; 8^{60} \cdot 8^{-1} \bmod 77$

$8^{\phi(77)} \bmod 77 = 8^{60} \bmod 77 \cdot 8^{-1} \bmod 77$

$= 8^{75} \bmod 77$

- $20^{62} \bmod 77$

$\phi(77) = 60$

$20^{60} \cdot 20^{2} \bmod 77 = 20^{2} \bmod 77 = 15$

using second version

$\phi(77) = 60$

$K\phi(n) + 1 = 61 \qquad 1 \times 60 + 1 \quad K = 1$

$20^{61} \cdot 20 \bmod 77 = 20 \times 20 \bmod 77 = 15.$

* Primitive Roots can be determined using discrete logarithm problem. It makes use of multiplicative finite groups

$G = \langle Z_n^*, \times \rangle$

in which the operation is multiplication.

The set Z_n^* contains those integers from 1 to n-1 that are relatively prime to n, with the identity element $p = 1$

When the modulus of the group is prime we have

$G = \langle Z_p^*, \times \rangle$

This group is a special case of the first group.

Scanned by CamScanner

- **Order of the Group**
The order of the finite group G is the no of elements in the group G which are having a multiplicative inverse.

- **Order of an Element**
The order of an element 'a' is the smallest integer 'i' such that a^i is congruent to e mod n where e=1

- In the group $G = \langle Z_n^*, \times \rangle$ when the order of an element is same $\phi(n)$ then that element is called the primitive root of that group.

* **Algorithm :**
Suppose if we want to find ~~roots~~ out all the primitive roots of 7

Step1 : Calculate $\phi(n)$
Step2 : Determine what are the multiplicative inverse of this number
Step3 : Calculate the order of each element using the formula
$a^i \equiv e \bmod n$ where $e=1$
Step 4: If $\phi(n)$ becomes equal to order of 'a' then that number is called the primitive root of n.

$\Rightarrow \phi(7) = 6 \qquad Z_7^*$

$a=1 \quad 1\times1 \equiv 1 \bmod 7 \qquad a=4 \quad 4\times2 \equiv 1 \bmod 7$
$a=2 \quad 2\times4 \equiv 1 \bmod 7 \qquad a=5 \quad 5\times3 \equiv 1 \bmod 7$
$a=3 \quad 3\times5 \equiv 1 \bmod 7 \qquad a=6 \quad 6\times6 \equiv 1 \bmod 7$

$\boxed{a^i \equiv 1 \bmod n}$

$a=1, \quad 1^1 \equiv 1 \bmod 7$ .... same for all 6 . order(1)=1
$a=2, \quad 2^6 \equiv 1 \bmod 7 \quad 2^3 \equiv 1 \bmod 7 \quad 2^6 \equiv 1 \bmod 7$ order(2)=3
$a=3, \quad 3^6 \equiv 1 \bmod 7$ order(3)=6
order(4)=3 $a=4, \quad 4^3 \equiv 1 \bmod 7 \quad 4^6 \equiv 1 \bmod 7$
$a=5, \quad 5^6 \equiv 1 \bmod 7$ order(5)=6
order(6)=2 $a=6, \quad 6^2 \equiv 1 \bmod 7 \quad 6^4 \equiv 1 \bmod 7 \quad 6^6 \equiv 1 \bmod 7$

Scanned by CamScanner

$\phi(n) = \phi(7) = 6$

order(3) = 6 and order(5) = 6

∴ primitive roots are 3 and 5

- $n = 10$ Z_8.

$Z_{10}^* \{1, 3, 7, 9\}$ $\phi(10) = \phi(2) \times \phi(5) = 4$

$a = 1$; $|X| \equiv 1 \bmod 10$

31/08 • Determine the primitive roots mod 13

$\phi(13) = 12$ $Z^*_{13} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

order(2) = (12) order(7) = (12) order(12) = 2

order(3) = 3 order(8) = 4

order(4) = 6 order(9) = 3

order(5) = 4 order(10) = 6

order(6) = (12) order(11) = 10

primitive roots of 13 = 2, 6, 7, 11

a) If group $G = \langle Z_n^*, X \rangle$ has primitive roots only if $n = 2, 4, p^t, 2p^t$ in which p is an odd prime (not 2) and t is an integer

b) The number of primitive roots can be calculated as $\phi(\phi(n))$

Scanned by CamScanner

a. Find $(20^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}) \bmod 7$ using fernels little theorem.

b. Determine value of x; $x^{103} \equiv 4 \bmod 11$ using FLT.

a) $p = 7 \quad p-1 = 6$

$2^{20} \Rightarrow (2^6)^3 2^2 \bmod 7 = 4$

$3^{30} \bmod 7 = (3^6)^5 \bmod 7 = 1$

$4^{40} \bmod 7 = (4^6)^6 \cdot 4^4 \bmod 7 = 4$

$5^{50} \bmod 7 = (5^6)^8 \cdot 5^2 \bmod 7 = 4$

$6^{60} \bmod 7 = (6^6)^{10} \bmod 7 = 1$

$4 + 1 + 4 + 4 + 1 \bmod 7 = 14 \bmod 7 = 0$

b) $p = 11 \quad p-1 = 10$

$(x^{10})^{10} x^3 \bmod 11$

$x^3 \equiv 4 \bmod 11$

$x = 5$

c. $x^{86} \equiv 6 \bmod 29$

$p-1 = 28$

$(x^{28})^3 \cdot x^2 \equiv 6 \bmod 29$

$x^2 \equiv 6 \bmod 29$

$x = 8, 21$

d) Determine the last three digits of 7^{803} using Eulers theorem

$n = 1000 \quad a = 7 \quad \phi(1000) = \phi(10^3) = \phi(2^3) \times \phi(5^3)$

$= (2^3 - 2^2) \times (5^3 - 5^2) = 400$

$(7^{400})^2 \cdot 7^3 \bmod 1000 = 343$

Scanned by CamScanner

a. Using Euler's theorem, find units digit of 3^{250}

b. last 2 digits of 3^{250}

a. $n=10 \quad \phi(10) = \phi(2) \times \phi(5) = 4$

$(3^4)^{62} \cdot 3^2 \bmod 10 = 9$

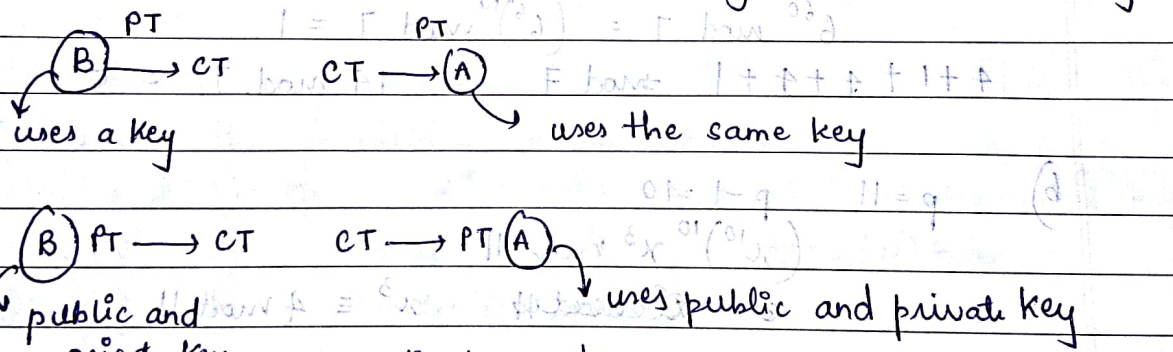
b. $n=100 \quad \phi(10^2) = \phi(2^2) \times \phi(5^2) = (2^2-2)(5^2-5) = 40$

$(3^{40})^6 \cdot 3^{10} \bmod 100 = 49$

11/09/18

Unit 3

Public Key CryptoSystem = Asymmetric : Different key
= Symmetric : Same key



public key : sharable
private key : non-shared

* RSA (Ron Rivest, Shamir, Adleman)

Step1 : Select 2 primes p and q such that $p \neq q$. Calculate $n = p \times q$
Calculate totient $\phi(n)$

step4 : Select integer e such that $\gcd(\phi(n), e) = 1$ and $1 \leq e < \phi(n)$

Step5 : Calculate d by congruence $d \equiv e^{-1} \bmod \phi(n)$

Scanned by CamScanner

Step 6: The public key is given as $P_u = (e, n)$
$P_R = (d, n)$

Step 7: Plaintext is given as $m < n$
Ciphertext is generated using formula $c = m^e \bmod n$

Step 8: $m = c^d \bmod n$

- $p = 17 \quad n = 187 \quad q = 11 \quad e = 7$

$$\phi(n) = \phi(17) \times \phi(11) = 16 \times 10 = 160$$

$$\gcd(160, 7) = 1$$

$$d = 7^{-1} \bmod 160$$

q	r_1	r_2	r	t_1	t_2	t
22	160	7	6	0	1	−22
1	7	6	1	1	−22	23
6	6	1	0	−22	23	−160
	1	0		23	−160	

$d = 23 \bmod 160$

$d = 23$

$P_U (7, 187)$

$P_R (23, 187)$

$m = 88$

$c = 88^7 \bmod 187 \quad 88^4 \cdot 88^2 \cdot 88^1$

$88^2 \bmod 187 = 77$

$88^4 \bmod 187 = 132$

$c = 132 \times 77 \times 88 \bmod 187 = 11$

$m = 11^{23} \bmod 187 \quad 11^{16} \cdot 11^4 \cdot 11^2 \cdot 11$

- $11^2 \bmod 187 = 121$

$11^4 \bmod 187 = 55$

$11^8 \bmod 187 = 33$

$11^{16} \bmod 187 = 154$

$m = 11 \times 121 \times 55 \times 154 \bmod 187 = 88$

Scanned by CamScanner

tutorial Attacks on RSA

560 ÷ 13

17622628

- $n = 11413$ $e = 7467$ $c = 5859$
  $p = 101$ $q = 113$ $\phi(n) = 100 \times 112 = 11200$

$d = e^{-1} \bmod \phi(n) = 7467^{-1} \bmod 11200$

q	r_1	r_2	r	t_1	t_2	t
1	11200	7467	3733	0	1	-1
2	7467	3733	1	1	-1	3
3733	3733	1	0	-1	3	-11200
	1	0		3	-11200	

5990

$d = 3 \bmod 11200 = 3$

$m = c^d \bmod n = 5859^3 \bmod 11413$

$m = 1415$

$c = m^e \bmod n = 1415^{7467} \bmod 11413$

* Primality Testing

1. Fermat Primality Test
2. Miller Rabin Test
3. Solovay Strassen Test

(1) Let $n > 1$ wherein $n \in \mathbb{Z}$ choose a random integer a with $1 < a < n-1$:

If $a^{n-1} \not\equiv 1 \bmod n$ then n is composite

If $a^{n-1} \equiv 1 \bmod n$ then n is probably prime

- 561 passes fermat Test ? $a = 2$ 954

2^{560} $2^{512} \cdot 2^{32} \cdot 2^{16}$

$2^8 \bmod 560 = 256$

$2^{16} \bmod 560 = 460$

$2^{32} \bmod 561 = 103$

Scanned by CamScanner

$a = bq + r$

$a - bq$

classmate Date Page

(2) Miller Rabin Test

input = the integer $n \geq 2$

output → yes/no

step 1 : $n-1 = 2^k \cdot m$

step 2 : Choose a random integer a $1 \leq a \leq n-1$

step 3 : $b = a^m \bmod n$

if $(b \equiv 1 \bmod n)$ then return ("n is prime")

for $(i = 0$ to $k-1)$

if $(b \equiv -1 \bmod n)$

then return ("n is prime");

else

$b = b^2 \bmod n$

return ("n is composite");

- 561 $560 = 2^4 \cdot 35$ $a = 2$

$b = 2^{35} \bmod 561 = 263 \bmod 561$

$i = 0$ $b = 263^2 \bmod 561 = 166$

$i = 1$ $b = 166^2 \bmod 561 = 67$

$i = 2$ $b = 67^2 \bmod 561 = 1$

$i = 3$ $b = 1^2 \bmod 561 = 1$

561 is composite

- 349 $a = 2$

$348 = 2^2 \cdot 87$ $a = 2$

$b = 2^{87} \bmod 349$ $2^{64} \cdot 2^{16} \cdot 2^4 \cdot 2^2 \cdot 2^1$

$2^8 \bmod 349 = 256$ $2^{16} \bmod 349 = 273$ $2^{32} \bmod 349 = 192$

$2^{64} \bmod 349 = 219$

$b = 219 \times 273 \times 16 \times 4 \times 2 \bmod 349 = 213$

$i = 0$ $b = 213^2 \bmod 349 = 348$

$i = 1$ $b \equiv -1 \bmod 349$

$\therefore$ 349 is prime

Scanned by CamScanner

③ Soloray Strassen

Let n be ~~not~~ odd integer, choose several integers a, $1 < a < n-1$

If a divided by n $\neq a^{(n-1)/2} \bmod n$

For some a, then n is composite

28/09/18 RSA attacks

- Low exponent attacks
- Short plaintext
- Timing Attacks

* Key Exchange Protocol:

① User A selects random integer $X_A < q$, where X_A is A's private key, q is a prime number. 29/09/18

User B selects random integer $X_B < q$, X_B is B's private key.

② User A computes $Y_A = \alpha^{X_A} \pmod q$

α is a primitive root of A, Y is a public key.

User B computes $Y_B = \alpha^{X_B} \bmod q$

③ Each side keeps X value private and makes Y values available publicly

④ A computes the key $K = (Y_B)^{X_A} \bmod q$

$K = (Y_A)^{X_B} \bmod q$

- $q = 353 \quad \alpha = 3 \quad X_A = 97 \quad X_B = 233$

$Y_A = 3^{97} \bmod 353 \quad 3^{64} \cdot 3^{32} \cdot 3$

$3^{24} \bmod 353 = 81 \quad 3^8 \bmod 353 = 207 \quad 3^{16} \bmod 353 = 136$

$3^{32} \bmod 353 = 140 \quad 3^{64} \bmod 353 = 185 \quad 3^{128} \bmod 353 = 337$

$Y_A = 185 \times 140 \times 3 \bmod 353 = 40$

$Y_B = 3^{233} \bmod 353 = 3^{128} \cdot 3^{64} \cdot 3^{32} \cdot 3^8 \cdot 3 \bmod 353$

$= 337 \times 185 \times 140 \times 207 \times 3 \bmod 353 = 248$

Scanned by CamScanner

(1) Man in middle
(2) Meet in Middle

$K = (Y_B)^{X_A} \bmod q = 248^{97} \bmod 353$

$248^{64} \cdot 248^{32} \cdot 248 \bmod 353$

$248^2 \bmod 353 = 82$ $248^4 \bmod 353 = 17$ $248^8 \bmod 353 = 289$

$248^{16} \bmod 353 = 213$ $248^{32} \bmod 353 = 185$ $248^{64} \bmod 353 = 337$

$K = (Y_A)^{X_B} \bmod q = 40^{233} \bmod 353$

$40^{128} \cdot 40^{64} \cdot 40^{32} \cdot 40^8 \cdot 40 \bmod 353$

$40^2 \bmod 353 = 188$ $40^4 \bmod 353 = 44$ $40^8 \bmod 353 = 171$

$40^{16} \bmod 353 = 295$ $40^{32} \bmod 353 = 187$ $40^{64} \bmod 353 = 22$

$40^{128} \bmod 353 = 131$

$K = 337 \times 185 \times 248 \bmod 353 = 160$

$K = 133 \times 58 \times 187 \times 256 \times 133 \bmod 353 = 160$

29/09/16 Apply Diffie Hellman key exchange on

$q = 71$ $\alpha = 7$ $X_A = 5$ $X_B = 12$

$Y_A = 7^5 \bmod 71 = 51$

$Y_B = 7^{12} \bmod 71 = 27 \times 58 \bmod 71 = 4$

$7^2 \bmod 71 = 49$ $7^4 \bmod 71 = 58$

$K = 4^5 \bmod 71 = 30$

$K = 51^{12} \bmod 71 = 30$

- Global ~~and~~ Public Elements
  - q prime number
  - α $\alpha < q$ is a primitive root

* Key Generation by Alice
  - Select private key X_A $X_A < q-1$
  - calculate Y_A $Y_A = \alpha^{X_A} \bmod q$
  - public key $[q, \alpha, Y_A]$
  - private key X_A

Scanned by CamScanner

* Encryption by Bob with Alice's public key

plaintext	$m < q$
select random integer k	$k < q$
calculate the new k	$K_1 = (Y_A)^k \bmod q$
calculate c_1	$c_1 = \alpha^k \bmod q$
calculate c_2	$c_2 = K_1 M \bmod q$
ciphertext	(c_1, c_2)

* Decryption by Alice with Alice's private key

ciphertext	(c_1, c_2)
Calculate K	$K_1 = (c_1)^{X_A} \bmod q$
plaintext	$M = c_2 K_1^{-1} \bmod q$

This entire system is called ELGAMAL CRYPTOSYSTEM
Hence we do encryption and decryption.

- Perform the elgamal cryptosystem on $q = 19$, 19 has primitive roots 2, 3, 10, 13, 14 $X_A = 5$ $\alpha = 10$ $M = 17$ $K = 6$

$$Y_A = \alpha^{X_A} \bmod q = 10^5 \bmod 19 = 3$$

$$K_1 = Y_A^k \bmod q = 3^6 \bmod 19 = 7$$

$$C_1 = 10^6 \bmod 19 = 11$$

$$C_2 = 7 \times 17 \bmod 19 = 5$$

ciphertext = (11, 5)

$$K = 11^5 \bmod 19 = 7$$

$$M = 5 \cdot 11 \bmod 19 = 17$$

1. Determine ciphertext, plaintext $M = 5$ is encrypted using elgamal $q = 11$ $\alpha = 7$ $y_A = 2$ and random no $K = 4$. Perform the encryption, determine ciphertext and show that decryption gives same plaintext $X_A = 3$

2. Elgamal scheme with a common prime $q = 71$ and primitive root $\alpha = 7$. If B has public key $Y_B = 2$ and A chooses a random integer $K = 2$. what is the ciphertext of $M = 30$ (ii) If A chooses different K so that encoding of $M = 30$ gives $C = (59, c_2)$ determine c_2.

Scanned by CamScanner

1. $M = 5 \quad q = 11 \quad \alpha = 7 \quad y_A = 2 \quad k = 4 \quad x_A = 3$

$K_1 = 2^4 \bmod 11 = 5$

$C_1 = 7^4 \bmod 11 = 3$

$C_2 = 5 \cdot 5^3 \bmod 11 = 3$

Ciphertext $(3, 3)$

$K_1 = 3^3 \bmod 11 = 5 \qquad M = 3 \times 5^{-1} \bmod 11 = 3 \times 9 \bmod 11 = 5$

2. $q = 71 \quad \alpha = 7 \quad y_B = 2 \quad k = 2 \quad M = 30$

$K_1 =$

$C_1 = 7^2 \bmod 71 = 49$

* Factorisation of Big Primes

a) Fermat Factorisation method
   ↳ difference of Square method

b) $(p-1)$ factoring
   Designed by Pollard; also known as pollard $(p-1)$ factoring

- In Fermat factorisation the idea is to express n as difference of 2 squares.

$$n = x^2 - y^2 = (x+y)(x-y)$$

$p = x+y \quad q = x-y$

eg: $n = 295927$

$295927 + 1^2 = 295928 \qquad 295927 + 2^2 = 295931$

$295927 + 3^2 = 295936 \rightarrow$ perfect square

$295927 = 544^2 - 3^2 = (544+3)(544-3) = 547, 541$

- $n = 8051 \qquad n = 4963789$

$8051 + 7^2 = 8100 \qquad 90+7, \ 90-7 \rightarrow (97, 83)$

$4963789 + 150^2 = 4986289 \qquad 2233 + 150, \ 2233 - 150$

$(2383, 2083)$

Scanned by CamScanner

Same method but different way

$$n = pq = (a+b)(a-b)$$

$$a = \frac{p+q}{2} \qquad b = \frac{p-q}{2}$$

$$a^2 - b^2 = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$$

$$= \frac{1}{4}\left(p^2 + 2pq + q^2 - p^2 + 2pq - q^2\right)$$

$$= \frac{1}{4}(4pq) = pq = n$$

- $n = 8051 \qquad a = \sqrt{8051} = 89.72 \simeq 90$

$$b^2 = 90^2 - 8051 = 49 = 7^2$$

$90+7, \quad 90-7$

- $n = 18923$

$$18923 + 11^2 = 138^2$$

$$138+11 = 149 \qquad 138-11 = 127$$

✳ $p-1$ factoring

Let n be a composite odd positive integer.

Let p divide n where p is prime such that $p-1$ divides $B!$ where B is known as Bound chosen by us.

By Eulers Theorem

$$2^{p-1} \equiv 1 \bmod p$$

$$2^{B!} \equiv 1 \bmod p \quad \text{because } p-1 \mid B!$$

$$\Rightarrow p \mid (B! - 1)$$

Hence $p \mid (2^{B!} - 1, n)$ gcd

Step1 : Calculate $B!$

Step2 : perform $2^{B!} \bmod n$

Step3 : Determine gcd of $(2^{B!} - 1, n) \Rightarrow$ gives first factor(1)

Step4 : $q = p/n$

Scanned by CamScanner

1001

421 X 135979

- n = 317017 B = 5
- n = 57247159 B = 8

$2^{120} \bmod 317017$ 2^{64} 2^{32} 2^{16} 2^{8}

$2^8 \bmod 317017 = 256$ $2^{16} \bmod 317017 = 65536$

$2^{32} \bmod 317017 = 20980$ $2^{64} \bmod 317017 = 140804$

$140804 \times 20980 \times 65536 \times 256 \bmod 317017$

$= 230947$

$\gcd(2^{120}-1, 317017) = \gcd(230946, 317017) = 61$

$q = 5197$ $p = 61$

- n = 57247159 $2^{40320} \bmod 57247159$

32768 4096 2048 1024 256

2^2 2^2 2^2 2^2 2^2 2^{128}

$2^{16} \bmod n = 65536$ $2^{32} \bmod n = 1430371$

$2^{64} \bmod n = 4982140$ $2^{128} \bmod n = 37803108$

$2^{256} \bmod n = 4294390$ $2^{512} \bmod n = 13930363$

$2^{1024} \bmod n = 24912544$ $2^{2048} \bmod n = 21494897$

$2^{4096} \bmod n = 54441932$ $2^{8192} \bmod n = 46798230$

$2^{16384} \bmod n = 53017020$ $2^{32768} \bmod n = 45234900$

$45234900 \times 54441932 \times 21494897 \times 24912544 \times 4294390 \times 37803108 \bmod 57247159$

$= 4311420 \times 8632654 \times 24460556 \bmod 57247159$

$= 4292025 \times 24460556$

$4548897 \mid 4548900$

$\gcd(4548900-1, 57247159)$

X12 ⇒ 266371
X1 ⇒ 188528
X1 ⇒ 77843
X2 ⇒ 34842
X2 ⇒ 8219
X4 ⇒ 1626
X5 ⇒ 1129
X14 ⇒ 400
X2 ⇒ 329
X1 ⇒ 71

X4 ⇒ 45

Scanned by CamScanner

* Discrete Logarithms :-

We fix prime p and we consider α, β as non-integers p, the equation is given as

$$\beta = \alpha^x \bmod p$$

The problem of finding x is called as discrete log problem.

If n is a smallest positive integers such that $\alpha^n = 1 \bmod p$ we may assume $0 \le x < n$ and we denote $x = L_\alpha(\beta)$ of β with respect to x

- Determine the value of x using discrete log problem.

1. $\alpha = 3 \quad \beta = 4$ and $p = 7$
   $4 = 3^x \bmod 7 \quad x = L_3(4) \quad x = 4$
2. $\alpha = 2 \quad \beta = 9 \quad p = 11$
   $9 = 2^x \bmod 11 \quad x = L_2(9) \quad x = 6$
3. $\alpha = 5 \quad \beta = 6 \quad p = 7$
   $6 = 5^x \bmod 7 \quad x = L_5(6) \quad x = 3$
4. $\alpha = 7 \quad \beta = 12 \quad p = 41$
   $12 = 7^x \bmod 41 \quad x = 13$.

03/10/18

* Solovoy Strassen Primality Test (probably prime)

a) Choose a random integer a in the range $1 \le a \le n-1$
b) Compute $X \leftarrow \left(\frac{a}{n}\right)$
c) If $X = 0$ then return n is composite.
d) $y = a^{\frac{n-1}{2}} \bmod n$
e) If $X \equiv Y \bmod n$ return n is prime
   If $X \not\equiv Y \bmod n$ return n is composite

Scanned by CamScanner

$\left(\frac{a}{n}\right)$ ⇒ Jacobi Symbol

$\frac{a}{n} \approx \frac{a}{p \times q}$ $\left(\frac{a}{p}\right)$ ⇒ Legendre Symbol

- $\frac{a}{p} = \begin{cases} 1 & \text{if } a \text{ is quadratic residue mod } p \\ 0 & \text{when } a \text{ divides } p \\ -1 & \text{if } a \text{ is non quadratic residue mod } p \end{cases}$

Q. Take $p=7$, what are quadratic residue mod 7

$a/p \equiv a^{(p-1)/2} \bmod p$

$a=1 \left(\frac{1}{7}\right) \equiv 1^3 \bmod 7 = 1$ $a=4 \left(\frac{4}{7}\right) \equiv 4^3 \bmod 7 = 1$

$a=2 \left(\frac{2}{7}\right) \equiv 2^3 \bmod 7 = 1$ $a=5 \left(\frac{5}{7}\right) \equiv 5^3 \bmod 7 = -1$

$a=3 \left(\frac{3}{7}\right) \equiv 3^3 \bmod 7 = -1$ $a=6 \left(\frac{6}{7}\right) \equiv 6^3 \bmod 7 = -1$

quadratic residue mod 7 (1, 2, 4)
non-quadratic residue mod 7 (3, 5, 6)

*• Jacobi Symbol satisfies many formulas that the legendre symbol ~~th~~ does.

Consider $(a,b) \in Z$ and $(m,n) \in Z^*$

1. If $a \equiv b \bmod n$ we can write it as $\frac{a}{n} = \frac{b}{n}$
2. If $\left(\frac{ab}{n}\right)$ we can write as $\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
3. If $\left(\frac{-1}{n}\right) \Rightarrow (-1)^{(n-1)/2}$

   $\left(\frac{2}{n}\right) \Rightarrow (-1)^{\frac{n^2-1}{8}}$
4. $\frac{n}{m} \Rightarrow (-1)^{\left(\frac{n-1}{2}\right)\left(\frac{m-1}{2}\right)} \times \frac{m}{n}$ (quadratic Reciprocity)

Scanned by CamScanner

If $m = 2^k \cdot t$ then $\frac{m}{n} = \left(\frac{2^k \cdot t}{n}\right) = \left(\frac{2}{n}\right)^k \left(\frac{t}{n}\right)$

* $\left(\frac{2}{p}\right) = 1$ if $p \equiv +/- 1 \bmod 8$

Q. $a = 7 \quad n = 59$

$\frac{7}{59} = 1$ both are prime

a) $\frac{219}{383}$ b) $\frac{2}{135}$ c) $\frac{10}{287}$ d) $\frac{10}{91}$

a) $\frac{219}{383} = 219^{191} \bmod 383$

$\frac{383}{219} (-1)^{20819} = \frac{383}{219} \cdot (-1)$

$\frac{219}{383} = \frac{383}{3} \times \frac{383}{173} (-1) = \left(\frac{2}{3}\right)^1 \times \left(\frac{98}{173}\right)^{36} (-1)$

$= 2 \bmod 3 \times 98^{36} \bmod 173 \cdot (-1)$

$18^{32} \cdot 18^4$

$2 \times 37 = 74$

$74 \bmod 173$

$= 148$

$-1 \times 1 \cdot (-1) = 1$

b) $\frac{2}{135}$ $135 \bmod 8 = (-1)$

Scanned by CamScanner

05/10/18 Perform Solovay Strassen Test for

a) $a = 2 \quad n = 13$

b) $a = 3 \quad n = 13$

$y_1 = 2^6 \bmod 13 = (-1)$

$y_2 = 3^6 \bmod 13 = (1)$

$X_1 = \frac{2}{13} = (-1)^{\frac{n^2-1}{8}} = (-1)^{21} = -1 = y_1$

$\therefore$ 13 is probably prime

$X_2 = \frac{3}{13} = (-1)^{6 \times 1} \frac{13}{3} = (+1) = y_2$

c) $a = 10 \quad n = 287$

$X = \frac{10}{287} = \frac{2}{287} \times \frac{5}{287}$

$\frac{2}{287} = (-1)^{(287^2-1)/2} = (-1)^{\cdots} = 1$

$\frac{5}{287} = \frac{287}{5} (-1)^{2 \times 143} = \frac{287}{5} = 2^2 \bmod 5 = 1$

$X = 1 \times -1 = -1$

$Y = 10^{143} \bmod 287 \qquad 10^1 \cdot 10^2 \cdot 10^4 \cdot 10^8 \, 10^{128} \bmod 287$

$10^2 \bmod 287 = 100 \quad 10^4 \bmod 287 = 242 \quad 10^8 \Rightarrow 16 \quad 10^{16} \Rightarrow 256 \quad 10^{32} \Rightarrow 100$

$10^{64} \bmod 287 = 242 \quad 10^{128} \bmod 287 = 16$

$Y = 10 \times 100 \times 242 \times 16 \times 16 \bmod 287 = 180$

$X \neq Y \bmod 287$

$\therefore$ 287 is composite

d) $a = 2 \quad n = 337$

$X = \frac{2}{337} = (-1)^{\frac{337^2-1}{8}} = (-1)^{14196} = 1$

$Y = a^{(n-1)/2} \bmod n = 2^{168} \bmod 337 \qquad 168 \Rightarrow 2^8 \cdot 2^{32} \cdot 2^{128}$

$2^8 \bmod 337 = 256 \quad 2^{16} \Rightarrow 158 \quad 2^{32} \Rightarrow 26 \quad 2^{64} \Rightarrow 2 \quad 2^{128} \Rightarrow 4$

$Y = 4 \times 26 \times 256 \bmod 337 = (1)$

$X \equiv y \bmod n \qquad 337$ is prime

Scanned by CamScanner

* Quadratic Sieve

Let n be an integer, there exists integer x and y with $x^2 \equiv y^2 \bmod n$ but $x \not\equiv \pm y \bmod n$ then n is composite.

Moreover gcd(x-y, n) gives you the non trivial factor of n.

Q. N = 91 - take which have a square

$81 \equiv -10 \bmod 91 \Rightarrow 3^4 \equiv -2.5$

$64 \equiv -27 \bmod 91 \Rightarrow 2^6 \equiv -3^3$

$49 \equiv -42 \bmod 91 \Rightarrow 7^2 \equiv -7 \times 3 \times 2$

$36 \equiv -55 \bmod 91 \Rightarrow 2^2 \cdot 3^2 \equiv -5 \times 11$

$25 \equiv -66 \bmod 91 \Rightarrow 5^2 \equiv -3 \times 11 \times 2$

$16 \equiv -75 \bmod 91 \Rightarrow 2^4 \equiv -5^2 \times 3$

$9 \equiv -82 \bmod 91 \Rightarrow 3^2 \equiv -41 \times 2$

$4 \equiv -87 \bmod 91 \Rightarrow 2^2 \equiv -29 \times 3$

$1 \equiv -90 \bmod 91 \Rightarrow 1 \equiv -3^2 \times 5 \times 2$

* n = 3427

Step1: Take Square root of n = 59

Step2: $59^2 \bmod n = 54$

Scanned by CamScanner