Network Security & Cryptography (NS&C)

URBAN EDGE

Books

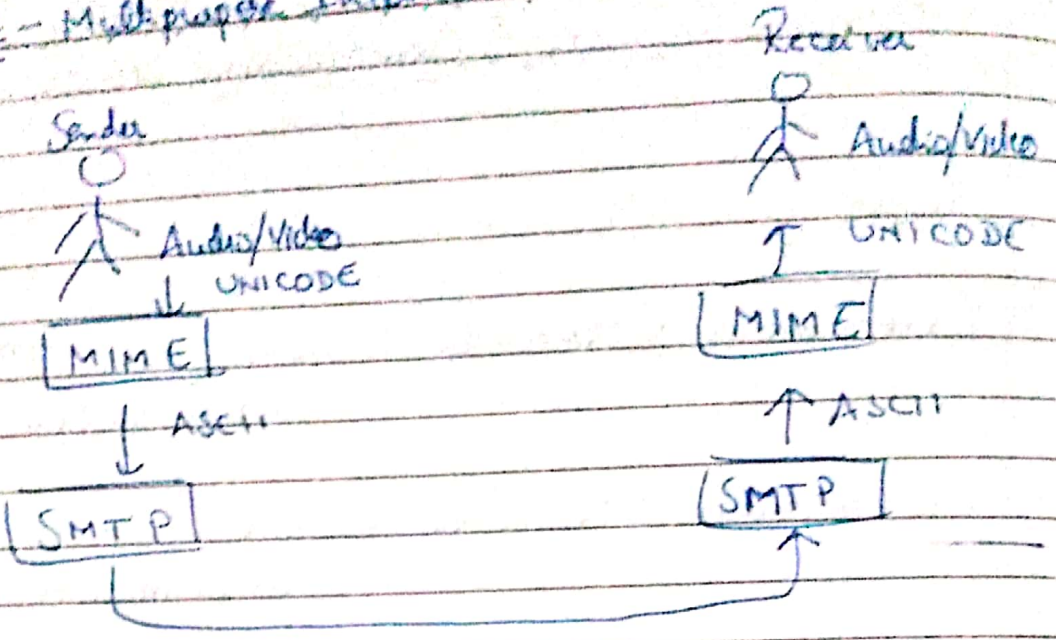
1. Cryptography & Network Security 7th Ed.
   By William Stallings
2. Cryptography & Network Security
   By Behrouz Fourozan

Evaluation

2 Tests	20%	One before mid-sem, one after
1 Mid Sem	30%	
1 End Sem	50%	

3. Cryptography & Network Security
   By Atul Kahate
4. Applied Cryptography

MIME - Multipurpose Internet Mail Extension



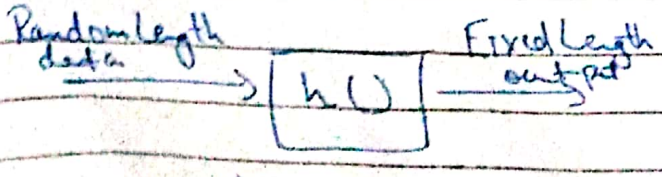
MIME converts Audio/Video to text
Unicode to ASCII

Telnet for accessing remote server/computer

FTP for transferring files to another computer

DNS for resolving IP addresses

put & get to place or get file from a server
eg.
put abc.txt
get def.txt



Hash Function

eg. MD5 (Message Digest)
SHA (Secure Hash Algorithm)

KDC - Key distribution center

Confidentiality, Integrity & Availability of information

☆ Security Attacks

- Threat to Confidentiality
  - Snooping
  - Traffic Analysis
- Threat to Integrity
  - Modification
  - Masquerading
  - Replaying
  - Repudiation
- Threat to Availability
  - Denial of Service

☆ TRADITIONAL CIPHERS - SYMMETRIC KEY CIPHER

Same key is used for encryption & decryption.
Information is shared through unsecured channel.
Keys are shared through secure channel.

Types of Ciphers

KEY SUBSTITUTION - Replaces a symbol with another symbol
TRANSPOSITION
STREAM & BLOCK

* Substitution cipher replaces the symbol with another

In additive ciphers, the plaintext, ciphertext & key are integers in modulo 26

eg. encrypt "hello" with key = 15

h	07	(07+15) mod 26 = 22	W
e	04	19	T
l	11	00	A
l	11	00	A
o	14	03	D

The cipher is monoalphabetic i.e. 2 instances of same plaintext ciphers are encrypted same.

hello —encrypt, 15→ WTAAD

plain text — cipher text

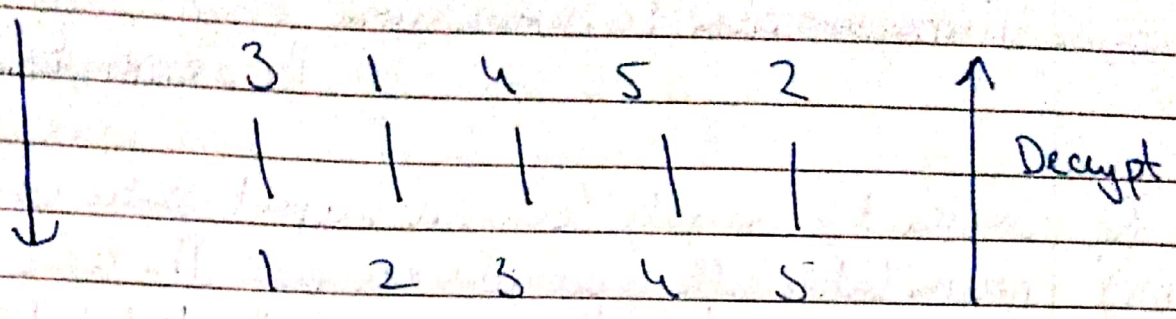
decrypt 'WTAAD' with key = 15

W	22	(22-15) mod 26 = 07	h
T	19	04	e
A	00	11	l
A	00	11	l
D	03	14	o

EDGE

* Transposition cipher reorders the symbols

eg.



The integers are positions

~~enemy~~ enemyattackstonightz (plaintext)

↓ write row by row

e n e m y
a t t a c
k s t o n
i g h t z

↓ encryption (row by row)

e e m y n
t a a c t
t k o n s
h i t z g

↓ read column by column

~~eenyntaacttkonshitzg~~

ettheakimaotycnznsg (cipher text)

The key depends on the no. of characters

You can add your own characters if the total ~~no~~ is not a multiple of key

URBAN EDGE

Computer Simulation & Modelling (CS&M)

Book: Introduction To Simulation
By Jerry Banks

Q (Pg69) Construct a computer technical support centre where a person takes calls & provides services. The time between calls ranges from 1 to 4 min with distribution as shown in Table 1.

There are 2 technical support people Able & Baker. Able is more experienced & can provide service faster than Baker. The distribution of their service times is in Table 2 & 3.

Simulate for 6 customers. Assume first customer arrives at 0

→ T1 - Distribution of arrival time

Time b/w arrival	1	2	3	4
Prob.	0.25	0.40	0.20	0.15

→ T2 - Distribution of service time for Able

Service Time	2	3	4	5
Prob.	0.30	0.28	0.25	0.17

→ T2 - Distribution of service time for Baker

Service Time	3	4	5	6
Prob.	0.35	0.25	0.20	0.20

P (1) Calculate arrival time distribution & assign random variables.

P (2) Calculate service time distribution & assign random no. for able

P (3) Calculate service time distribution & assign random no. for Baker

P (4) Calculate inter-arrival time distribution

---

(1)

	prob.	cum. prob.	Random digit
1	0.25	0.25	00-25
2	0.40	0.65	26-65
3	0.20	0.85	66-85
4	0.15	1.00	86-100

Able

(2)

2	0.30	0.30	00-30
3	0.28	0.58	31-58
4	0.25	0.83	59-83
5	0.17	1.00	84-100

Baker

(3)

3	0.35	0.35	00-35
4	0.25	0.60	36-60
5	0.20	0.80	61-80
6	0.20	1.00	81-100

(4) Random digit for arrival time 26, 98, 90, 26, 42

" " " service time 95, 21, 51, 92, 89, 38

WE ARE CELEBRATING INSTITUTE FOUNDATION DAY TOMORROW

Key 5 3 2 1 4
R 1 4 3 5

3 5 1 2 4
1 2 3 4 5

WEARE		AEWER
CELEB		LBCEE
RATIN		TNRAI
GINST		NTGIS
ITUTE		UEITT
FOUND	→	UDFON
ATION		INATO
DAYTO		YODAT
MORRO		ROMOR
WABCD		BDWAC

read column by column ↓

ALTNUUIYRBEBNTEDNOODWCRGLEADMW
GEAITOTADAREISTNOTRC

★ MODERN CIPHERS – bit oriented ciphers

n-bit plain text → Encryption ← k-bit key → Decryption → n-bit plain text

n-bit cipher text → n-bit cipher text

Modern block cipher

★ Components of modern block ciphers

→ Transposition (eg: no. of bits)
- Straight permutation 5 to 5
- Compression permutation 5 to 3
- Expansion permutation 3 to 5

Straight perm. → ISKNT → NTTNI KAAKS

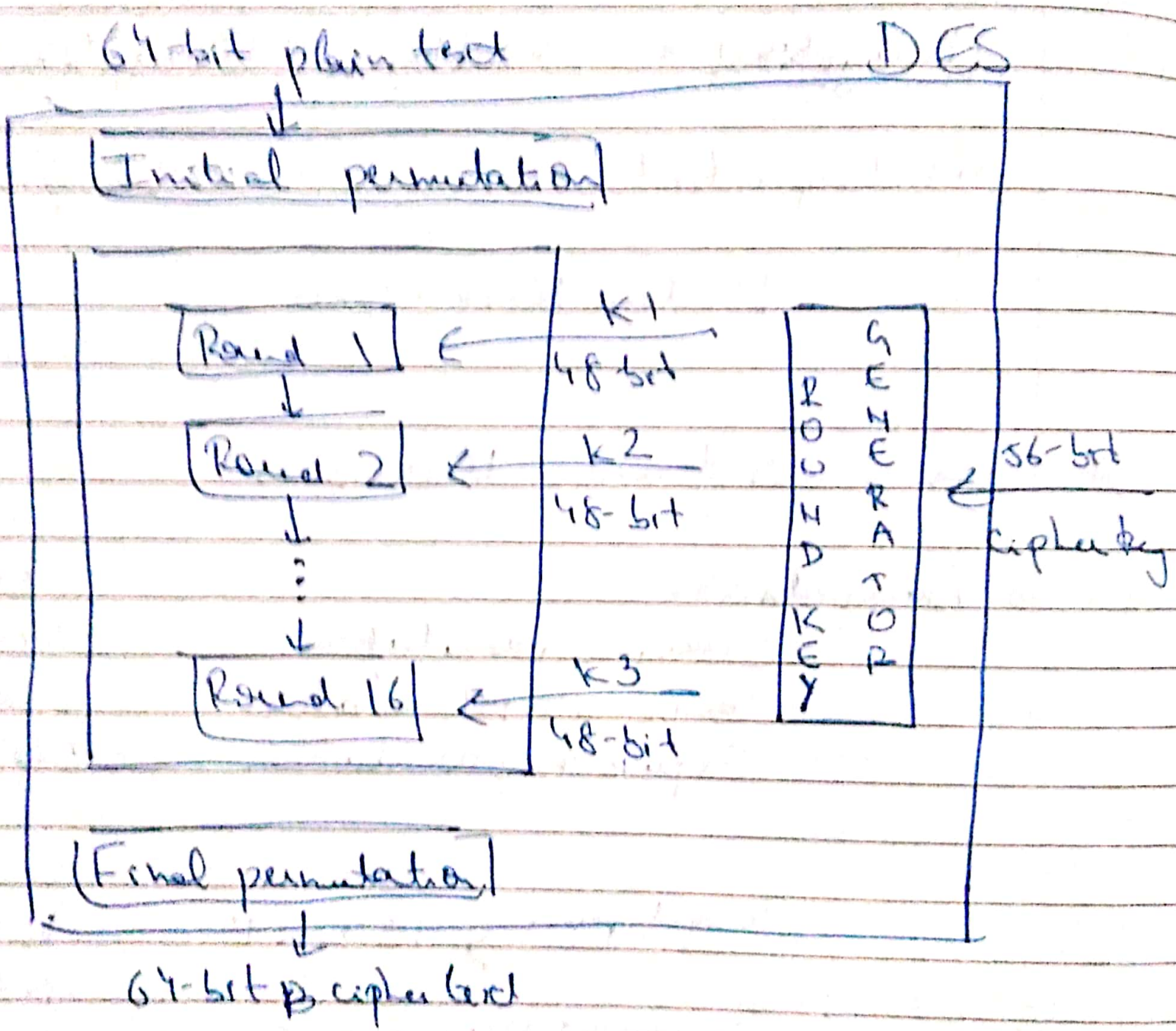
NITKS → Compression perm. → NTS

Expansion perm. → NKTATANKIS

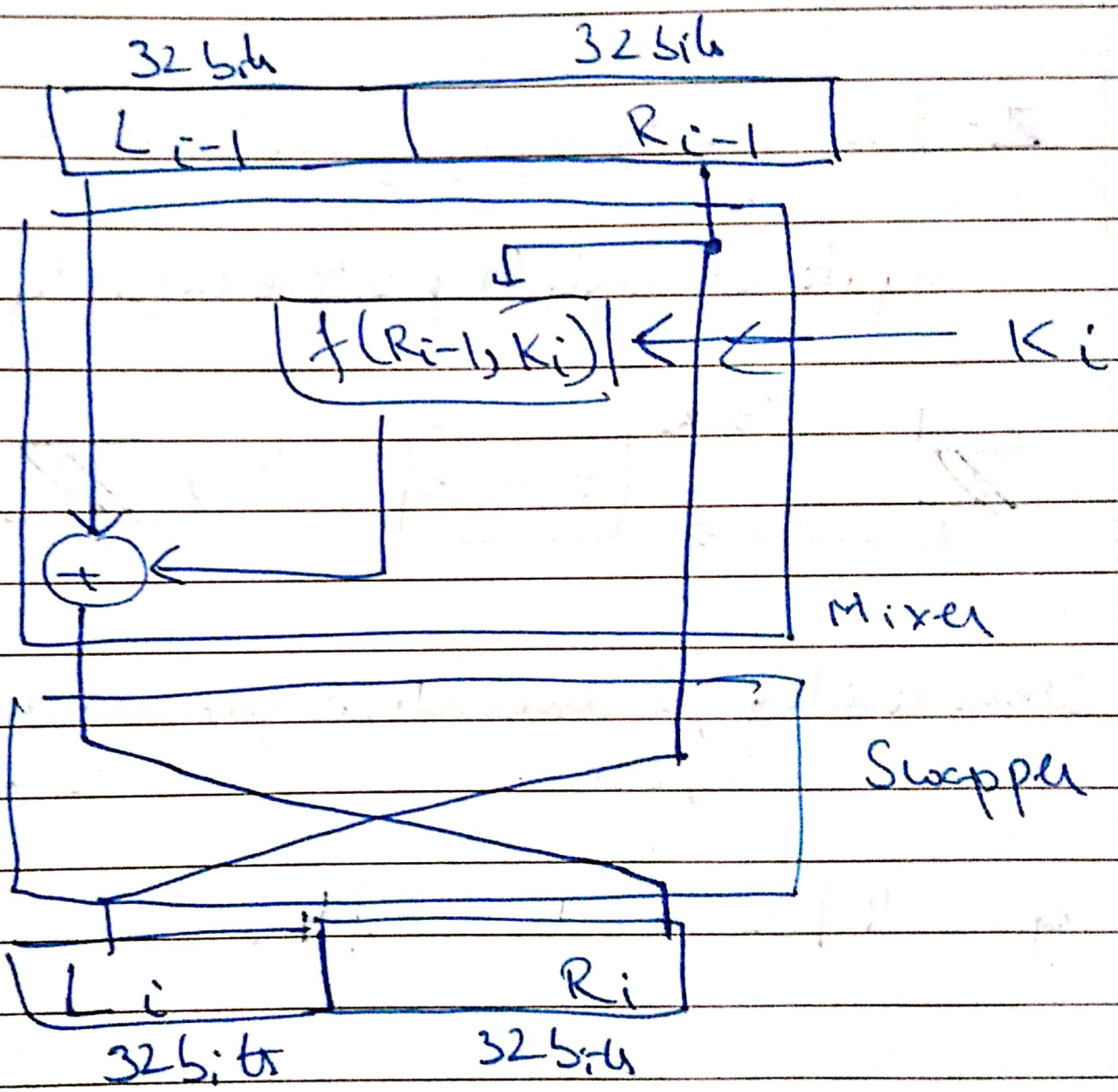
→ Substitute
→ Exclusive-OR
→ Shift
→ Swap
→ Split
→ Combine

DES

General Structure



For i^{th} round

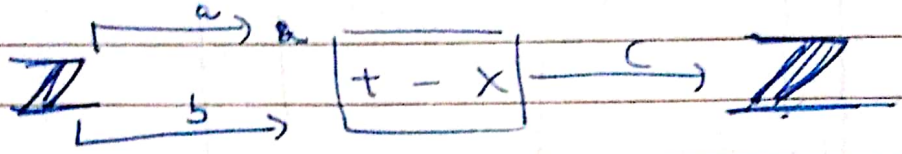


Mathematics of Cryptography

☆ Integer Arithmetic

$\mathbb{Z} = \{ \ldots -2, -1, 0, 1, 2, \ldots \}$

negative infinity to positive infinity



When dividing, if remainder is zero $\Rightarrow a/n$
; else $\Rightarrow a \nmid n$

eg $4 \mid 32$: but $8 \nmid 92$

Prop 1. If $a/1$, then $a = \pm 1$

Prop 2. If a/b & b/a, then $a = \pm b$

Prop 3. If a/b & b/c, then a/c

Prop 4. If a/b & a/c, then $a/(m \times b + n \times c)$

Euclidean Algorithm

Fact 1. $\gcd(a, 0) = a$

Fact 2. $\gcd(a, b) = \gcd(b, r)$, where r is the remainder of dividing a by b

eg GCD of 2740 & 1760 using Euclidean Algo

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	6
	20	0	

$\therefore \gcd(2740, 1760) = 20$

eg GCD of 25 & 60

q	r_1	r_2	r
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

$\therefore \gcd(25, 60) = 5$

Modular Arithmetic

We are interested in remainders

$a \% n = r$

n is called modulus (must be +ve)
r is called remainder (non-negative)

eg. $27 \bmod 5 = 2$
$36 \bmod 12 = 0$
$-18 \bmod 14 = 10$
$-7 \bmod 10 = 3$

The set of least residues modulo n, (Z_n)

$Z_n = \{0, 1, 2, 3, \ldots, (n-1)\}$

Congruence ($\equiv$)

$2 \equiv 12 \pmod{10}$. $13 \equiv 23 \pmod{10}$
$3 \equiv 8 \pmod{5}$ $8 \equiv 13 \pmod{5}$

A residue class $[a]$ or $[a]_n$

URBAN EDGE

eg Subtract 11 from 7 in Z_{13}

$(7-11) \bmod 13 \longrightarrow (-4) \bmod 13 = 9$

★ $(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

Similarly for $-$ & $\times$

$10^n \bmod x = (10 \bmod x)^n$

★ Additive Inverse

a & b are additive inverse if

$a + b \equiv 0 \pmod n$

eg Find the all additive inverse pair in Z_{10}

(0,0) (1,9) (2,8) (3,7) (4,6) (5,5)

★ Multiplicative Inverse

a & b are multiplicative inverse if

$a \times b \equiv 1 \pmod n$

eg Find all multiplicate inverse in Z_{10}

(1,1) (3,7) (9,9)

Extended Euclidean algorithm for finding multiplicative inverse

Q Find multiplicative inverse of 11 in Z_{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	

∴ the inverse of 11 is −7 or 19

Q Find multiplicative inverse of 23 in Z_{100}

q	r_1	r_2	r	t_1	t_2	t
4	100	23	8	0	1	-4
2	23	8	7	1	-4	9
1	8	7	1	-4	9	-13
7	7	1	0	9	-13	100
	1	0		-13	100	

-13 or $(-13 * 100) = 87$

Q Find multiplicative inverse of 12 in Z_{26}

q	r_1	r_2	r	t_1	t_2	t
2	26	12	2	0	1	-2
6	12	2	0	1	-2	13
	2	0		-2	13	

as the gcd (12, 26) = 2, the inverse of 12 doesn't exist.

EDGE

Z_n for additive inverses, Z_n

Z_n^* for multiplicative inverses Z_{p^n}

for prime numbers

Q Find GCD of

(88, 220) (300, 42)

(24, 320) (401, 200)

0	88	220	88
2	220	88	44
2	88	44	0
	44	0	

gcd(88, 220) = 44

7	300	42	6
7	42	6	0
	6	0	

gcd(300, 42) = 6

0	24	320	24
13	320	24	8
3	24	8	0
	8	0	

gcd(24, 320) = 8

0	401	200	401	1	4	3	1
1	200	401	299	3	3	1	0
1	401	299	102		1	0	
2	299	102	95				
1	102	95	7				
13	95	7	4				
1	7	4	3				
1	4	3	1				

gcd(401, 200) = 1

Linear Congruence

$ax \equiv b \pmod{n}$

assume $\gcd(a, n) = d$

If $d \nmid b$, there is no solution

If $d \mid b$, there are d solution

Q Solve $10x \equiv 2 \pmod{15}$

$\gcd(10, 15) = 5$

As $5 \nmid 2$, we have no solution

Q Solve

$14x \equiv 12 \pmod{18}$

$\gcd(14, 18) = 2$

As $2 \mid 12$, we have 2 solutions

$14x \equiv 12 \pmod{18}$

$7x \equiv 6 \pmod{9}$

$x \equiv 6(7^{-1}) \pmod{9}$

$x_0 = (6 \times 7^{-1}) \bmod 9 = (6 \times 4) \pmod{9} = 6$

$x_1 = x_0 + 1 \times (18/2) = 15$

Q Solve

$3x + 4 \equiv 6 \pmod{13}$

$3x \equiv 2 \pmod{13}$

$\gcd(3, 13) = 1$

∴ equation has exactly one solution

$x_0 = (2 \times 3^{-1}) \pmod{13}$

$x_0 = 18 \bmod 13 = 5$

$3 \times 5 + 4 \equiv 19 \pmod{13} = 6$

★ Chinese Remainder Theorem (CRT)

$a \quad m$

eg $x \equiv 2 \pmod{3}$

$x \equiv 3 \pmod{5}$

$x \equiv 2 \pmod{7}$

$M = 3 \times 5 \times 7 = 105$

$M_1 = 35 \qquad M_2 = 21 \qquad M_3 = 15$

$M_1^{-1} = 2 \qquad M_2^{-1} = 1 \qquad M_3^{-1} = 1$

$x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$

$= (140 + 63 + 30) \bmod 105$

$= 233 \bmod 105 = 23$

URBAN EDGE

y

$x = 3 \bmod 7$

$x = 3 \bmod 13$

$x = 0 \bmod 12$

$M = 7 \times 13 \times 12 = 1092$

$M_1 = 156 \qquad M_2 = 84 \qquad M_3 = 91$

$M_1^{-1} = 4 \qquad M_2^{-1} = 11 \qquad M_3^{-1} = 7$

$x = (3 \times 156 \times 4 + 3 \times 84 \times 11 + 0 \times 91 \times 7) \bmod 1092$

$= (1872 + 2772 + 0) \bmod 1092$

$= 4644 \bmod 1092 = 276$

y

$x \equiv 2 \bmod 7$

$x \equiv 3 \bmod 9$

$M = 7 \times 9 = 63$

$M_1 = 9 \qquad M_2 = 7$

$M_1^{-1} = 4 \qquad M_2^{-1} = 4$

$x = (2 \times 9 \times 4 + 3 \times 7 \times 4) \bmod 63$

$= (72 + 84) \bmod 63$

$= 156 \bmod 63 = 30$

9 3 6 1 9 1 0 164 1 5 0 0 URBAN EDGE

9 $x \equiv 7 \bmod 13$

$x \equiv 11 \bmod 13$

$M = 13 \times 12 = 156$

$M_1 = 12 \qquad M_2 = 13$

$M_1^{-1} = 12 \qquad M_2^{-1} = 1$

$x = (7 \times 12 \times 12 + 11 \times 13 \times 1) \bmod 156$

$= (1008 + 143) \bmod 156$

$= 1051 \bmod 156 = 115$

eg 1 $\begin{bmatrix} 3 & 4 & 6 \\ 1 & 1 & 8 \\ 5 & 8 & 3 \end{bmatrix} \times \begin{bmatrix} 2 & 0 & 1 \\ 1 & 1 & 0 \\ 5 & 2 & 4 \end{bmatrix}$

$= \begin{bmatrix} 40 & 16 & 27 \\ 43 & 17 & 33 \\ 33 & 14 & 17 \end{bmatrix}$ Mod 16

$= \begin{bmatrix} 8 & 0 & 11 \\ 11 & 1 & 1 \\ 1 & 14 & 1 \end{bmatrix}$

---

eg Z_{10}

$A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$ $\det(A) = 3 \bmod 10$

$(\det(A))^{-1} = 7 \bmod 10$

$A^{-1} = \frac{1}{3} \begin{bmatrix} 1 & 0 \\ -1 & 3 \end{bmatrix} = 7 \begin{bmatrix} 1 & 0 \\ 9 & 3 \end{bmatrix}$

adjoint of A

$\therefore A^{-1} = \begin{bmatrix} 7 & 0 \\ 3 & 1 \end{bmatrix}$

$$\begin{bmatrix} 3 & 4 & 6 \\ 1 & 1 & 8 \\ 5 & 8 & 3 \end{bmatrix}$$

$$\det(A) = 3.(-60) - 4(-37) + 6(3)$$
$$= -183 + 148 + 18 = -15$$
$$-17 \equiv 5 \pmod{16}$$

$$\text{adj}(A) = \begin{bmatrix} -61 & 37 & 3 \\ +36 & -21 & -4 \\ 26 & -18 & -1 \end{bmatrix} \equiv \begin{bmatrix} 9 & 7 & 3 \\ 6 & 9 & 6 \\ 6 & 2 & 9 \end{bmatrix} \pmod{16}$$

$$A^{-1} = \begin{bmatrix} 3 & 2 & 2 \\ 9 & 3 & 4 \\ 1 & 2 & 3 \end{bmatrix}$$

Q $3x + 5y \equiv 4 \pmod 5$
$2x + y \equiv 3 \pmod 5$

$$\begin{bmatrix} 3 & 5 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 4 \\ 3 \end{bmatrix}$$

$\det(A^{-1}) = 2$

$\det(A) = 3 - 10 = -7 \equiv 3 \pmod 5$

$$\text{adj}(A) = \begin{bmatrix} 1 & -5 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 3 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 0 \\ 4 & 4 \end{bmatrix} \begin{bmatrix} 4 \\ 3 \end{bmatrix} \quad \begin{pmatrix} 2 & 0 \\ 6 & 6 \end{pmatrix} \equiv \begin{bmatrix} 2 \\ 11 \end{bmatrix}$$

$3x + 2y \equiv 5 \pmod 7$
$4x + 6y \equiv 4 \pmod 7$

$$\begin{bmatrix} 3 & 2 \\ 4 & 6 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 4 \end{bmatrix}$$

$\det(A) = 10 \equiv 3 \pmod 7$

$(\det(A))^{-1} = 5$

$$5 \begin{bmatrix} 6 & -2 \\ -4 & 3 \end{bmatrix} = 5 \begin{bmatrix} 6 & 5 \\ 3 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 30 & 25 \\ 15 & 15 \end{bmatrix} \quad \begin{bmatrix} 2 & 4 \\ 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 24 \\ 11 \end{bmatrix} \begin{bmatrix} 5 \\ 4 \end{bmatrix} \quad \begin{bmatrix} 26 \\ 9 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \end{bmatrix}$$

$7x + 3y \equiv 3 \pmod 7$
$4x + 2y \equiv 5 \pmod 7$

$$\begin{bmatrix} 7 & 3 \\ 4 & 2 \end{bmatrix} \quad \det(A) = 2$$
$$(\det A)^{-1} = 4$$

$$\text{adj } A = \begin{bmatrix} 2 & -3 \\ -4 & 7 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 3 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 8 & 16 \\ 12 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 \\ 5 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 8 & 0 \end{bmatrix} \quad \begin{bmatrix} 3 \\ 5 \end{bmatrix}$$

$2x + 3y \equiv 5 \pmod 8$ — (1)

$x + 6y \equiv 3 \pmod 8$ — (2)

$$\begin{bmatrix} 2 & 3 \\ 1 & 6 \end{bmatrix} \quad \det(A) = 9 \equiv 1 \pmod 8$$

$(\det A)^{-1} = 1$

$$\text{adj}(A) = \begin{bmatrix} 6 & -3 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} 6 & 5 \\ 7 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 6 & 5 \\ 7 & 2 \end{bmatrix} \begin{bmatrix} 5 \\ 3 \end{bmatrix}$$

$$\begin{bmatrix} 45 \\ 41 \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 1 \end{bmatrix} \pmod 8$$

$x \equiv 2 \pmod 5$

$x \equiv 3 \pmod 7$

$M = 5 \times 7 = 35$

$M_1 = 7 \quad M_2 = 5$

$x = 17$

$x \equiv 6 \pmod 7$

$x \equiv 4 \pmod 8$

$M = 7 \times 8 = 56$

$M_1 = 8 \quad M_2 = 7$

$M_1^{-1} = 1 \quad M_2^{-1} = 7$

$(6 \times 8 \times 1) + (4 \times 7 \times 7)$

$= 49 + 196 = 245$

$x \equiv 1 \pmod 5$

$x \equiv 2 \pmod 7$

$x \equiv 3 \pmod 9$

$x \equiv 4 \pmod{11}$

Integers 1 to 10

n	$\phi(n)$	Euler's Totient Function
1	0	2^0
2	1	$2^1 \times 3^0$
3	2	1×1
4	2	
5	4	$2 \times 2 \times 2$
6	2	
7	6	
8	4	
9	6	
10	4	

$\phi(p) = (p-1)$

$\phi(p_1 \times p_2) = (p_1-1)(p_2-1)$

$\phi(p^e) = p^e - p^{e-1}$

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

p, p_1 & p_2 are prime

Q Elements in

1) $Z_6^* = \{1, 5\}$ $1\times1, 5\times5$

2) $Z_7^* = \{1, 2, 3, 4, 5, 6\}$ $1\times1, 2\times4, 3\times5, 6\times6$

3) $Z_{10}^* = \{1, 3, 7, 9\}$ $1\times1, 3\times7, 9\times9$

4) $Z_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ $1\times1, 2\times6, 3\times4, 5\times9, 7\times8$

$\varphi(6) = \varphi(3) \times \varphi(2)$
$= 2 \times 1 = 2$

$\varphi(10) = \varphi(2) \times \varphi(5)$
$= 1 \times 4 = 4$

$\varphi(29) = 28$

$\varphi(32) = 16$

$\varphi(80) = 32$ $80 = 2^4 \times 5$
$(16-8) \times 4 = 32$

$\varphi(100) = 40$ $100 = 2^2 \times 5^2$

$\varphi(101) = 100$

$\varphi(41) = 40$

$\varphi(27) = 18$

$\varphi(231) = 120$ $231 = 3 \times 7 \times 11$

$\varphi(440) = 160$ $440 = 2^3 \times 5 \times 11$

Fermat's Little Theorem

$a^{p-1} \equiv 1 \pmod{p}$, iff p is prime & $p \nmid a$

$a^p \equiv a \pmod{p}$

Q $3^{201} \pmod{11}$

$3^{10 \times 20} \times 3 \pmod{11}$

$(3^{10})^{20} \times 3 \pmod{11}$ — using Fermat's Little Theorem

$(1)^{20} \times 3 \pmod{11} \equiv 3 \pmod{11}$

Q $5^{15} \pmod{13}$

$5^{12} \times 5^3 \pmod{13}$

$5^3 \pmod{13} \equiv 125 \pmod{13} \equiv 8 \pmod{13}$

Q $15^{18} \pmod{17}$

$15^{16} \times 15^2 \pmod{17}$

$1 \times 15^2 \pmod{17} \equiv 225 \pmod{17} \equiv 4 \pmod{17}$

Q $(456)^{17} \pmod{7}$

$\equiv 456 \pmod 7 \equiv 14 \pmod 7$

Q $(145)^{102} \pmod{101}$

$\equiv (145)^{100} \times 145^2 \pmod{101}$

$\equiv 21025 \pmod{101}$

$\equiv 17 \pmod{101}$

Mersenne

$M_n = 2^n - 1$

n	F_n	
2	17	✓
3	257	✓
4	65537	
5		
6		
7		
8		
9		
10		
11		

p	M_p	
2	3	✓
3	7	✓
4	15	X
5	31	✓
6	63	X
7	127	✓
8	255	X
9	511	X
10	1023	X
11	2047	X
	$2047 = 23 \times 89$	

Fermat

$F_n = 2^{2^n} + 1$

Every number can be expressed as sum of 2 primes

$10 = 3+7 = 5+5$

$24 = 11+13$

$28 = 11+17$

$16 = 11+5$ [illegible]

[illegible]

1. $Z_{[illegible]}^{*} = 12$
2. $Z_{[illegible]}^{*} = 18$
3. $Z_{28}^{*} = 22$

$Z_{224}^{*} = (2^5 - 2^4)(7-1)$ $\quad 224 = 2^5 \times 7$

$= 16 \times 6 = 96$

Q. Write down the equation for mersenne number

$M_p = 2^p - 1$

175

51

$$\begin{bmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{bmatrix}$$

Z_{26}

$3[5(144-68) - 7(48-85) + 2(12-45)]$
$- 5[1(144-68) - 7(96-221) + 2(24-117)]$
$+ 7[1(32-85) - 4(96-221) + 2(30-39)]$
$- 2[1(12-45) - 4(24-117) + 7(30-39)]$

$= 3[[illegible] + 256 - 66] - 5[76 + 875 - 186]$
$+ 7[-32 + [illegible] - 18] - 2[-33 + 384 - 63]$

$$\begin{bmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{bmatrix}$$

URBAN EDGE

$= (3 \times 494) - (5 \times 765) + (7 \times 445) - (2 \times 288)$

$= 1482 - 3825 + 3115 - 576$

$= 196 \equiv 14 \pmod{26}$

$$\begin{bmatrix} 3 & 4 & 6 \\ 1 & 1 & 8 \\ 5 & 8 & 3 \end{bmatrix}$$ mod 26

$3(3-64) - 4.(3-40) + 6(8-5)$

$-185 + 148 + 18 = -17 \pmod{26}$

$\equiv 3 \pmod{26}$

$$\begin{bmatrix} -61 & 37 & 3 \\ 36 & -21 & -4 \\ 26 & -18 & -1 \end{bmatrix} \equiv \begin{bmatrix} 9 & 7 & 3 \\ 6 & 9 & 6 \\ 6 & 2 & 9 \end{bmatrix}$$ mod 7

$$\begin{bmatrix} 27 & 21 & 9 \\ 18 & 27 & 18 \\ 18 & 6 & 27 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 9 \\ 8 & 2 & 8 \\ 8 & 6 & 2 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 63 & 49 & 21 \\ 42 & 63 & 42 \\ 42 & 14 & 63 \end{bmatrix}^T \qquad \begin{bmatrix} 3 & 9 & 1 \\ 2 & 3 & 2 \\ 2 & 4 & 3 \end{bmatrix}^T$$

hello

$$\begin{bmatrix} 3 & 2 & 2 \\ 9 & 3 & 4 \\ 1 & 2 & 3 \end{bmatrix}$$