CNS

Steganography.

eg: single space - 0
Double space - 1

This book is mostly about cryptography, not steganography.
0 1 0 0 0 0 1

Encode the message: ~~stop~~ STOP using the text cover steganography for the text

I(1) am(2) a(1) student(2) of(1) Ramaiah(1) institute(2) of(2) Technology, (1) I(2) pursue(1) computer(2) science(1) and(2) engineering(1) course.(1) I(1) am(2) currently(1) in(1) ~~5th~~ fifth.(2) semester(2) This(2) is(2) a(1) cryptography(2) class(1) It(2) is(1) highly(1) irritating(1) for(1) me to come to college on a Saturday.

S - 01010011
T - 01010100
O - 01001111
P - 01010000

I am a student of Ramaiah institute of Technology. I pursue computer science and engineering course. I am currently in fifth semester. This is a cryptography class. It is highly irritating for me.

eg(2): message - ~~56~~ bit.
1 bit 1 - article a - 0 the - 1.
next 5 - noun
next 4 - verb
next 1 - article
next 5 - noun.

eg: HI : 01001000 01001001

Date: A friend called the doctor.
0 10010 0001 0 01001

CNS

Multiplicative Inverse

25% 75%

12 8

$a \times b \equiv 1 \pmod n$ $\quad \gcd(a,b) = 1 \pmod n$

$a + b \equiv 1 \pmod n$

using extended euclidean to find multiplicative inverse of b in Z_n.

$r_1 \leftarrow n \quad r_2 \leftarrow b$

$t_1 \leftarrow 0 \quad t_2 \leftarrow 1$

while $(r_2 > 0)$

$q \rightarrow r_1 / r_2$

$r \leftarrow r_1 - q \times r_2$

$r_1 \leftarrow r_2 \; ; \; r_2 \leftarrow r$

$t \leftarrow t_1 - q \times t_2$

$t_1 \leftarrow t_2 \; ; \; t_2 \leftarrow t \; ;$

}

if $(r_1 = 1)$ then $b^{-1} \leftarrow t_1$

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	-

$b^{-1} = 11^{-1} = -7$ $\quad -7 \bmod 26 = 19$.

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	-

$-13 \bmod 100 = 87$

~~<key, pair>~~

Integer division

$$a = q \times n + r$$

$a \longrightarrow \mathbb{Z}$ $\quad$ $r \longrightarrow$ non negative

$n \longrightarrow$ positive $\quad$ $q \longrightarrow \mathbb{Z}$

If $r = 0$, a/n. else not.

Euclidean algorithm

$r_1 \leftarrow a \quad r_2 \leftarrow b$

While ($r_2 > 0$) {

$q \leftarrow r_1 / r_2$;

$r \leftarrow r_1 - q \times r_2$

$r_1 \leftarrow r_2$; $r_2 \leftarrow r$;

}

$\gcd(a,b) \leftarrow r_1$

a b.

Find the gcd of 2740, 1760 with the help of euclidian algorithm.

Step 1:

$r_1 = 2740 \quad r_2 = 1760$

$q = 980$

$r = 0$.

Step 2: $r_1 = 1760$

$r_2 = 0$.

$r_2 > 0$ ✗

$\therefore \gcd(2740, 1760) = 980$.

Step 1: $r_1 = 2740$, $r_2 = 1760$

$q = 1$

$r = 980$.

$r_1 = 1760 \quad r_2 = 980$

Step 2: $q = 1$.

$r = 780$

$r_1 = 980 \quad r_2 = 780$

Step 3: $q = 1$

$r = 200$

$r_1 = 780 \quad r_2 = 200$

Step 4: $q = 3$

$r = 180$

$r_1 = 200 \quad r_2 = 180$

Step 5: $q = 1$

$r = 20$.

$r_1 = 180 \quad r_2 = 20$.

Step 6: $q = 9$

$r = 0$.

$r_1 = 20, \quad r_2 = 0$.

$\gcd(2740, 1760) = 20$ (r_1)

gcd (60, 25)

Step 1: $r_1 = 60$ $r_2 = 25$

$q = 2$

$r = 10$ $r_1 - q \times r_2$

$r_1 = 25$ $r_2 = 10$

Step 2: $q = 2$

$r = 5$

$r_1 = 10$ $r_2 = 5$

Step 3: $q = 2$

$r = 0$

$r_1 = 5$, $r_2 = 0$

$\gcd(60, 25) = 5$

Extended euclidean Algorithm

$s \times a + t \times b$

$r_1 \leftarrow a$ $r_2 \leftarrow b$

$s_1 \leftarrow 1$ $s_2 \leftarrow 0$

$t_1 \leftarrow 0$ $t_2 \leftarrow 1$

while ($r_2 > 0$) {

$q \leftarrow r_1 / r_2$

$r \leftarrow r_1 - q \times r_2$;

$r_1 \leftarrow r_2$; $r_2 \leftarrow r$

$s \leftarrow s_1 - q \times s_2$;

$s_1 \leftarrow s_2$; $s_2 \leftarrow s$

$t \leftarrow t_1 - q \times t_2$

$t_1 \leftarrow t_2$; $t_2 \leftarrow t$

}

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	161	28	21	1	0	1	0	1	-5
	28	21	7	0	1	-1	1	-5	6
	21	7	0	1	-1	4	-5	6	-23
	7	0	/	/	-1	4	/	6	23

$a = 0$, $b = 45$

0	45	0	0	1	0	1	0	1	0
45	0	—	—	0	1				

Date :

~~1000~~
~~× 15~~

Symmetric Key ciphers

~~If P is~~ Substitution ciphers

↳ mono alphabetic (default key : 3)

plaintext : hello

ciphertext : KHOOR

each alphabet will be represented by ~~same~~ single character

* Additive cipher / (simplest) shift cipher / caesar cipher

$C = (P+k) \bmod 26$: P → plaintext

Q) key = 15 to encrypt message

THIS IS CNS CLASS.

19	7	8	18		8	18		2	13	18		2	11	0	18	18
↓	↓	↓	↓		↓	↓		↓	↓	↓		↓	↓	↓	↓	↓
8	22	23	7		23	7		17	2	7		17	0	15	7	7
I	W	X	H		X	H		R	C	H		R	A	P	H	H

"IWXH XH RCH RAPHH"

Q) Decrypt: WTAAD k = 15

↓	↓	↓	↓	↓
22	19	0	0	3
↓	↓	↓	↓	↓
7	4	11	11	4
H	E	L	L	O

Date : _____

* check for first three characters.

U	V	A	C	L	Y	F	Z	L	J	B	Y	L
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
20	21	0	2	11	24	5	25	11	9	1	24	11

k=1 $(C-k) \bmod 26$

T U Z B K X E Y K I A X

k=2.

S T Y A J

k=3.

R S X

k=4

Q R

k=5

P Q.

k=6

O P U W.

k=7

N O T | V E R Y | S E C U R E

k=8

Statistical analysis * find most freq letter * separate all ~~that~~ with E

k=4.

X L I L S Y W M I M W R S A J S V

T H E H O U I

E → 04 V → 21

k = 17 (21−4)

$P = C - K$

$K = C - P$

Date : _____

Multiplicative cipher

Encrypt: $C = (P \times k) \bmod 26$. Mulplicative

Decrypt: $P = (C \times k^{-1}) \bmod 26$

Multiplicative

$k = 7$,

H	E	L	L	O
↓	↓	↓	↓	↓
7	4	11	11	14
↓	↓	↓	↓	↓
49	28	77	77	98
(23)	(2)	(25)	(25)	(20)
X	C	Z	Z	U

Affine cipher

En: $T = (P \times k_1) \bmod 26$

$C = (T + k_2) \bmod 26$

De: $P = (T \times k_1^{-1}) \bmod 26$

$T = (C - k_2) \bmod 26$

$k_1 \longrightarrow Z_{26}^*$ $k_2 \longrightarrow Z_{26}$.

$Z_{26}^* = \{1, 3, 5, 7, 9, \ldots, 23, 25\}$.

Size of key domain $= 12 * 26 \longrightarrow 312$.

Q) "DO NOT HIDE" with key pair (7, 2).

	3	14	18	14	19	7	8	3	4
X	21	98	126	98	133	49	56	21	28
	23	100	128	100	135				
	24	20							

Substitution ciphers

THIS MESSAGE IS EASY. ⟶ ICFV QRVVNER FV RNWS

Plaintext ciphertext

Polyalphabetic cipher

$C = C_1 C_2 C_3 \ldots$ $k = k_1 k_1 k_2 \ldots$

$P = P_1 P_2 P_3 \ldots$

* Autokey cipher

Encr. $C_i = (P_i + k_i) \bmod 26$.

Decr. $P_i = (C_i - k_i) \bmod 26$

Attack is today

	A	T	T	A	C	K	I	S	T	O	D	A	Y
P:	0	19	19	0	2	10	8	18	19	14	3	0	24
K:	12	0	19	19	0	2	10	8	18	19	14	3	0
C:	12	19	12	19	2	12	18	0	11	7	17	3	24
	M	T	M	T	C	M	S	A	L	H	R	D	X

Q) Plaintext: WE ARE SAFE k1 = 9

	W	E	A	R	E	S	A	F	E
P:	22	4	0	17	4	18	0	5	4
K:	9	22	4	0	17	4	18	0	5
C:	5	0	4	17	21	22	18	5	9
	F	A	E	R	V	W	S	F	J

* Playfair cipher

eg: keyword

AMAIRA

* Divide the plaintext into diagrams.

A	M	I/J	R	B
C	D	E	F	G
H	K	L	N	O
P	Q	S	T	U
V	W	X	Y	Z

3 rules:

1) same row, change to right letter (wrap)
2) same column, below letter (wrap)
3) neither, intersection (its row).

BA|LL|OO|NS → BA|LX|LO|ON|SX

x (dummy)

HE|LL|O → HE|LX|LO

HE → LC, LX → SI, LO → NH

Q) En: ATTACK using keyword: MONARCHY

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

AT|TA|CK

RS|SR|DE → RSSRDE

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Q) PLEASE SAVE ME

key: crypto.

CQOBZK ME ZA SA

CQOBZKMEZASA.

C	R	Y	P	T
O	A	B	D	E
F	G	H	I/J	K
L	M	N	Q	S
U	V	W	X	Z

Q) CT:

BM OD ZB XD VE PR KU DM UI XM MO UV IF

HI DE TH EQ OA LI NT HE TR EX ES TV MP

HIDE THE GOAL IN THE TREE STUMP

P	L	A	Y	F
I/J	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Vigenere Cipher

$K = [(k_1, k_2, \ldots k_m)(k_1, k_2 \ldots k_m)]$

En: $C_i = (P_i + k_i) \bmod 26$ De: $P_i = (C_i - k_i) \bmod 26$.

Q) SHE IS LISTENING

keyword: PASCAL

15 0 18 2 0 11

SHEISLISTENING

P: 18 7 4 8 18 11 8 18 19 4 13 8 13 6

K: 15 0 18 2 0 11 15 0 18 2 0 11 15 0

C: 7 7 22 10 18 22 23 18 11 6 13 19 2 6

HHWKSWXSLGNTCG

W E A R E D I S C O V E R E D S A V E
22 4 0 17 4 3 8 18 2 14 21 4 17 4 3 18 0 21 4
3 4 2 4 15 19 8 21 4 3 4 2 4 15 19 8 21 4 3
25 8 2 21 19 22 16 13 6 17 25 6 21 19 22 0 21 25 7

Y O U R S E L F
24 14 20 17 18 4 11 5
4 2 4 15 19 8 21 4
2 16 24 6 11 12 6 9

D E C E P T I V E
3 4 2 4 15 19 8 21 4

Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G J .

* One Time Pad. → message & key can should be same.
HELLO → 7 4 11 11 14
MONEY → 12 14 13 4 24
19 18 24 15 12 → T S Y P M.

Q) En: T E S T → 19 4 18 19
Key F R E B → 5 21 4 1
24 25 22 20 → Y Z W U.

Q) E N I G M A → 5 13 8 6 12 0
K E Y W O R → 10 4 24 22 14 17
15 17 6 2 0 17
→ P R G C A R.

* Hill Cipher key is m x m matrix
En: C = K*P mod 26
SHORT EXAMPLE
18 7 14 17 19 4 23 0 12 15 11 4
(18/7) (14/17) (19/4) (23/0) (12/15) (11/4)

key: HILL → 7 8 11 11
$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$
7×18 + 8×7 = 182 → 0 $\begin{pmatrix} A \\ P \end{pmatrix}$
11×18 + 11×7 = 275 → 15

$\begin{pmatrix} 14 \\ 17 \end{pmatrix}$ $\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 14 \\ 17 \end{pmatrix} = 7\times14 + 8\times17$

$K^{-1} = \frac{1}{|K|} \cdot K_{adj}$

A P | A D | J T | F T | W L | F J $\quad K = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$

$\begin{pmatrix} A \\ P \end{pmatrix}\begin{pmatrix} A \\ D \end{pmatrix}\begin{pmatrix} J \\ T \end{pmatrix}\begin{pmatrix} F \\ T \end{pmatrix}\begin{pmatrix} W \\ L \end{pmatrix}\begin{pmatrix} F \\ J \end{pmatrix}$ $\quad P = k^{-1} * C \bmod 26.$

$|K| = 77 - 88 = -11 \bmod 26$
$= 15$

Multiplicative inverse of 15 in Z_{26}.

q	r1	r2	r	t1	t2	t
1	26	15	11			

$K^{-1} = \frac{1}{15}\begin{pmatrix} 11 & -8 \\ -11 & 7 \end{pmatrix} \bmod 26$

$K^{-1} = \begin{pmatrix} 11/15 & -8/15 \\ -11/15 & 7/15 \end{pmatrix}$

$= \frac{1}{15}\begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix}$

$= 7\begin{pmatrix} 25 & 22 \\ 6 & 1 & 23 \end{pmatrix}$

Hill cipher. (De to En)

Plain: SAF EME SSA GES
cipher: HDS JOE YQO CAA

$K = \begin{pmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{pmatrix}$

$k^{-1} = \frac{1}{|K|} * K_{adj}$

$|K| = 2(24 - 221) - 8(42 - 136) + 15(91 - 32)$.
$= -394 + 752 + 885$
$= 1243 \bmod 26.$
$= 21$

$21^{-1} \bmod 26 = ?$
$21(?) \bmod 26 = 1.$
$21(1) \bmod 26 = 21$ not equal to 1
$21(2) \bmod 26 = 42$
$21(5) \bmod 26 = 1$

$adj\ k = \begin{bmatrix} -197 & 94 & 59 \\ 147 & -108 & 38 \\ 76 & 71 & -48 \end{bmatrix}^T$

$= \begin{bmatrix} -197 & 147 & 76 \\ 94 & -108 & 71 \\ 59 & 38 & -48 \end{bmatrix}$

Date:

$$= \begin{bmatrix} 11 & 147 & 76 \\ 94 & 22 & 71 \\ 59 & 38 & 4 \end{bmatrix}$$

$K^{-1} = D^{-1} \text{adj } K$

$= 5 \times \text{adj } K = \begin{bmatrix} 55 & 735 & 380 \\ 470 & 110 & 355 \\ 295 & 190 & 20 \end{bmatrix} \bmod 26$

$$K^{-1} = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix}$$

$P = K^{-1} C \bmod 26.$

$$= \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \begin{bmatrix} 8 \\ 14 \\ 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix} \quad \text{e m e}$$

Q) Encrypt : RETREAT NOW . using key phrase : BACKUP.

RET | REA | TNO | WXX

$$K = \begin{bmatrix} B & A & C \\ K & U & P \\ A & B & C \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{bmatrix}$$ 3×3

$$\begin{bmatrix} R \\ E \\ T \end{bmatrix} \begin{bmatrix} R \\ E \\ A \end{bmatrix} \begin{bmatrix} T \\ N \\ O \end{bmatrix} \begin{bmatrix} W \\ X \\ X \end{bmatrix}$$ 3×1

$$\begin{bmatrix} 17 \\ 4 \\ 19 \end{bmatrix} \begin{bmatrix} 17 \\ 4 \\ 0 \end{bmatrix} \begin{bmatrix} 19 \\ 13 \\ 14 \end{bmatrix} \begin{bmatrix} 22 \\ 23 \\ 23 \end{bmatrix}$$

$$\begin{bmatrix} 55 \\ 535 \\ 47 \end{bmatrix} \begin{bmatrix} 17 \\ 250 \\ 4 \end{bmatrix} \begin{bmatrix} 47 \\ 660 \\ 41 \end{bmatrix} \begin{bmatrix} 68 \\ 1025 \\ 67 \end{bmatrix}$$

$$\begin{bmatrix} 3 \\ 15 \\ 21 \end{bmatrix} \begin{bmatrix} 17 \\ 16 \\ 4 \end{bmatrix} \begin{bmatrix} 21 \\ 10 \\ 15 \end{bmatrix} \begin{bmatrix} 16 \\ 11 \\ 17 \end{bmatrix}$$

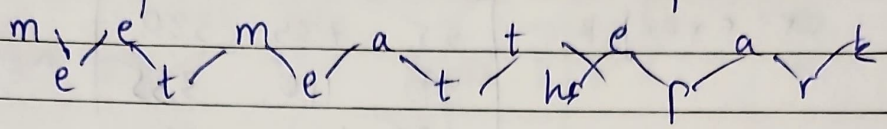
$$\begin{bmatrix} D \\ P \\ V \end{bmatrix} \begin{bmatrix} R \\ Q \\ E \end{bmatrix} \begin{bmatrix} V \\ K \\ P \end{bmatrix} \begin{bmatrix} Q \\ L \\ R \end{bmatrix} \longrightarrow DPV \mid RQE \mid VKP \mid QLR.$$

Transposition ciphers.

① Keyless Transposition cipher.

* Rail fence cipher

eg meet me at the park.



cipher : MEMATEAKETETHPR.

*

P: row by row · C: column wise

cipher: mmta eehr eaek ttp.

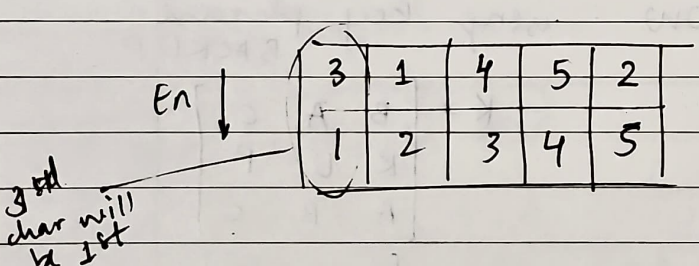
m e e t
m e a t
t h e p
a r k.

② Keyed transposition cipher

ENEMY ATTACKS TONIGHT.

~~KEY~~.

ENEMY ATTAC' KSTON' IGHTZ



EEMYN TAACT TKONS HITZG

③ Combining two approaches:

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

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

e tthe|akima|otycn|zntsg.

Date: _____

Eg: CRYPTOGRAPHY IS VERY SIMPLE using the key 3 2 1 5 4. The sender and receiver has agreed upon. having 5 column transmission

C	R	Y	P	T
O	G	R	A	P
H	Y	I	S	V
E	R	Y	S	I
M	P	L	E	Z

→

Y	R	C	T	P
R	G	O	P	A
I	Y	H	V	S
Y	R	E	I	S
L	P	M	Z	E

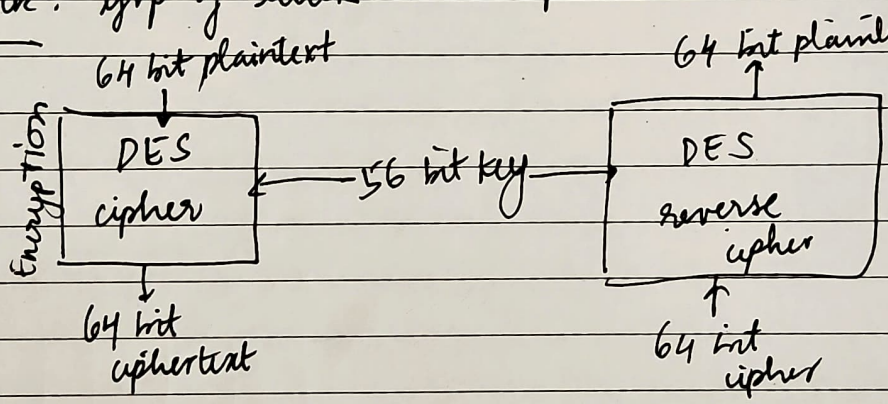
YRIYL RGYRP COHEM TPVIZ PASSE

Stream and Block Ciphers.

(1) Stream. En: $D = E_{K_{3n}}(P_n)$.

(2) Block: type of letters and cipher the blocks.

DES



Diffusion & Confusion

- Diffusion: change in plaintext, ciphertext also changes
- Confusion: if single key bit is changed, cipher text also changes.

(*) DES structure