

Railfence (Encryption)

PT = Hello world

k = depth = 3

message length = 10 = no. of columns

H				O				L	
	E		L		W		R		D
		L			O				

C.T. = HOLELWORDLO

H				O				L	
	E		L		W		R		D
		L			O				

Greek for Greeks

Decriptions

C.T. →

GisGisekprekece

key = 3

1	2	3	4	5	6	7	8	9	10	11	12	13
G				S				G				S
	E		K		P		R		E		K	
		E				O				E		

G
 E
 E
 K
 G
 E
 E
 K

⑥ Columnar Transposition technique

P.T. Five minutes engineering

1	2	3	4	5
F	J	V	E	M
I	N	U	T	E
S	E	N	G	I
N	E	E	R	I
N	G	-	-	-

key = 43512

C.T. = E T G R V U N G M E I I F I S N N I N E E G

1	2	3	4	5
N	E	V	E	T
N	G	N	T	I
I		E	G	F
N		M	R	I
E		E	V	S

1	2	3	4	5
E	U	I	N	E
T	N	I	N	G
G	E	F	I	N
R	M	I	N	N
V	E	S	E	N

For decryption divide the
column message length by
key length to find the
column length

$$\frac{22}{4} = 5.5$$

1	2	3	4	5
F	E	V	E	M
I	N	U	T	E
S	E	N	G	I
N	E	E	R	T
N	G	x	x	x

fill the ^{begin} letters then
again fill in column order
as per key, then read
row wise.

(7)

more complex technique is to write the message row by row and read the message off column by column, but permute the order of column.

key: 4 3 1 2 5 6 7
 P.T. a t t a c k p
 o s t p o n e
 d u n t i l t
 w o a m x y z

C.T. = TTNAAPTMTSUOAOWGLOZXPKNLYPETZ

Pure transpositional cipher is easily recognizable bcz it has same letter frequencies as original plaintext.

This can be made more secure by performing more than one stage of transposition.

Thus if the foregoing message is reencrypted using the same algorithm.

key: 4 3 1 2 5 6 7
 Input: t t n a a p t
 m t s u o a o
 d w c o i x k
 n l y p e t z

output: nscyAuoPTTWLTMpNAO1EPAXTTOKZ

Steganography :-# The methods of steganography conceal the existence of the message.

The method of cryptography render the message unintelligible to outsiders by various transformations of the text.

Eg. One possible eg. is first letter of each message in the main message

Since end come run even twice
message hidden is → Secret

Some other techniques

↳ Character marking: Selected letters of printed or typewritten text are overwritten in pencil.

↳ Invisible ink: A number of substances can be used for writing but leaves no visible trace until heat or some chemical is applied to the paper.

↳ Pin puncture: Small pin punctures on selected letters are ordinarily not visible unless paper held in front of light.

→ Typewriter correction ribbon: Used blue lines typed with a blank ribbon, the results of typing with the correction tape are visible only under a strong light.