u20734621 – Matthew Gotte

COS 333 – Practical 1

Problem 2.2

(A)

Write the text to cypher into the table with the key CRYPTOGAHI key:

2	8	10	7	9	6	3	1	4	5
C	R	Y	P	T	O	G	A	H	I
B	E	A	T	T	H	E	T	H	I
R	D	P	I	L	L	A	R	F	R
O	M	T	H	E	L	E	F	T	O
U	T	S	I	D	E	T	H	E	L
Y	C	E	U	M	T	H	E	A	T
R	E	T	O	N	I	G	H	T	A
T	S	E	V	E	N	I	F	Y	O
U	A	R	E	D	I	S	T	R	U
S	T	F	U	L	B	R	I	N	G
T	W	O	F	R	I	E	N	D	S

Take the vertical column index from the table above, and write it into the equivalent row index of the table below with the NETWORKSCU key:

4	2	8	10	5	6	3	7	1	9
N	E	T	W	O	R	K	S	C	U
T	R	F	H	E	H	F	T	I	N
B	R	O	U	Y	R	T	U	S	T
E	A	E	T	H	G	I	S	R	E
H	F	T	E	A	T	Y	R	N	D
I	R	O	L	T	A	O	U	G	S
H	L	L	E	T	I	N	I	B	I
T	I	H	I	U	O	V	E	U	F
E	D	M	T	C	E	S	A	T	W
T	L	E	D	M	N	E	D	L	R
A	P	T	S	E	T	E	R	F	O

Take the 5-digit groups from the columns of the above table:

ISRNG	BUTLF	RRAFR	LIDLP	FTIYO	NVSEE	TBEHI	HTETA
EYHAT	TUCME	HRGTA	IOENT	TUSRU	IEADR	FOETO	LHMET
NTEDS	IFWRO	HUTEL	EITDS				

(B)

Decrypting the cypher requires:

1. Taking all 5-digit groups of the second matrix and writing it into the columns using the network security key and continue to fill the column with the next 5-digit group till the table is populated.
2. Taking the 5-digit groups generated by the rows of the newly generated table and writing them into the columns of the cryptographic key table.

Using:

ISRNG	BUTLF	RRAFR	LIDLP	FTIYO	NVSEE	TBEHI	HTETA
EYHAT	TUCME	HRGTA	IOENT	TUSRU	IEADR	FOETO	LHMET
NTEDS	IFWRO	HUTEL	EITDS				

Generate by writing into columns:

4 N	2 E	8 T	10 W	5 O	6 R	3 K	7 S	1 C	9 U
	R					F		I	
	R					T		S	
	A					I		R	
	F					Y		N	
	R					O		G	
	L					N		B	
	I					V		U	
	D					S		T	
	L					E		L	
	P					E		F	

NOTE: only the first few were done as an example for the method used, bellow if the full resulting table after the method concludes:

4 N	2 E	8 T	10 W	5 O	6 R	3 K	7 S	1 C	9 U
T	R	F	H	E	H	F	T	I	N
B	R	O	U	Y	R	T	U	S	T
E	A	E	T	H	G	I	S	R	E
H	F	T	E	A	T	Y	R	N	D
I	R	O	L	T	A	O	U	G	S
H	L	L	E	T	I	N	I	B	I
T	I	H	I	U	O	V	E	U	F
E	D	M	T	C	E	S	A	T	W
T	L	E	D	M	N	E	D	L	R
A	P	T	S	E	T	E	R	F	O

This table is now taken in 5-digit groups going left to right and top to bottom and is written into the columns of the cryptographic key table and the following is produced:

2	8	10	7	9	6	3	1	4	5
C	R	Y	P	T	O	G	A	H	I
B	E	A	T	T	H	E	T	H	I
R	D	P	I	L	L	A	R	F	R
O	M	T	H	E	L	E	F	T	O
U	T	S	I	D	E	T	H	E	L
Y	C	E	U	M	T	H	E	A	T
R	E	T	O	N	I	G	H	T	A
T	S	E	V	E	N	I	F	Y	O
U	A	R	E	D	I	S	T	R	U
S	T	F	U	L	B	R	I	N	G
T	W	O	F	R	I	E	N	D	S

NOTE: only the first few iterations are highlighted to show the method used.

This resulting table can now be read from left to right and top to bottom to obtain the original text:

BE AT THE THIRD PILLAR FROM THE LEFT OUTSIDE THE LYCEUM THEATRE TONIGHT AT SEVEN IF YOU ARE DISTRUSFUL BRING TWO FRIENDS

(c)

This method is simple to implement and effective in that it requires minimal computation and resources to cypher/decipher and is an effective method of transmitting time sensitive messages however is a symmetric cypher. This means that at some point the keys will have to be shared and could possible be intercepted making the cypher effectively useless at protecting the data it cyphers.