Q.

Please use Feistel cipher to manually encrypt and decrypt the plaintext BRUCELEE.

ENCRYPTION

L0 **R0**

BRUC **ELEE**

Key = 2

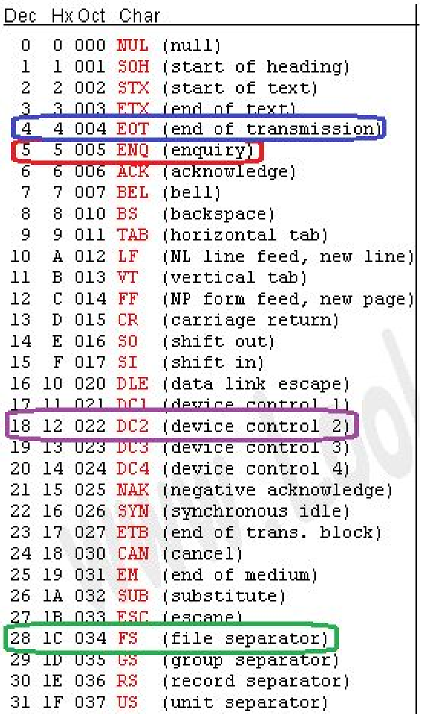
(XOR) □ GNGG

BRUC 00010 10010 10101 00011

(xor)□

GNGG 00111 01110 00111 00111

00101 11100 10010 00100 ⇒ **5 28 18 4**



Dec	Hx	Oct	Char	
0	0	000	NUL	(null)
1	1	001	SOH	(start of heading)
2	2	002	STX	(start of text)
3	3	003	ETX	(end of text)
4	4	004	EOT	(end of transmission)
5	5	005	ENQ	(enquiry)
6	6	006	ACK	(acknowledge)
7	7	007	BEL	(bell)
8	8	010	BS	(backspace)
9	9	011	TAB	(horizontal tab)
10	A	012	LF	(NL line feed, new line)
11	B	013	VT	(vertical tab)
12	C	014	FF	(NP form feed, new page)
13	D	015	CR	(carriage return)
14	E	016	SO	(shift out)
15	F	017	SI	(shift in)
16	10	020	DLE	(data link escape)
17	11	021	DC1	(device control 1)
18	12	022	DC2	(device control 2)
19	13	023	DC3	(device control 3)
20	14	024	DC4	(device control 4)
21	15	025	NAK	(negative acknowledge)
22	16	026	SYN	(synchronous idle)
23	17	027	ETB	(end of trans. block)
24	18	030	CAN	(cancel)
25	19	031	EM	(end of medium)
26	1A	032	SUB	(substitute)
27	1B	033	ESC	(escape)
28	1C	034	FS	(file separator)
29	1D	035	GS	(group separator)
30	1E	036	RS	(record separator)
31	1F	037	US	(unit separator)

⇒ **ENQ FS DC2 EOT**

ASCII Table

L1

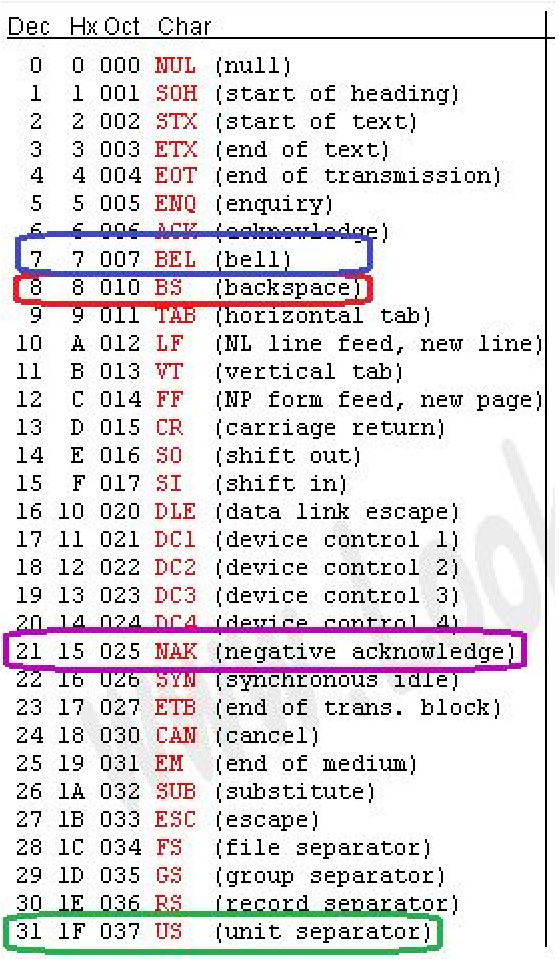
ELEE

R1

ENQ FS DC2 EOT

Key = 3

BS US NAK BEL



Dec	Hx	Oct	Char
0	0	000	NUL (null)
1	1	001	SOH (start of heading)
2	2	002	STX (start of text)
3	3	003	ETX (end of text)
4	4	004	EOT (end of transmission)
5	5	005	ENQ (enquiry)
6	6	006	ACK (acknowledge)
7	7	007	BEL (bell)
8	8	010	BS (backspace)
9	9	011	TAB (horizontal tab)
10	A	012	LF (NL line feed, new line)
11	B	013	VT (vertical tab)
12	C	014	FF (NP form feed, new page)
13	D	015	CR (carriage return)
14	E	016	SO (shift out)
15	F	017	SI (shift in)
16	10	020	DLE (data link escape)
17	11	021	DC1 (device control 1)
18	12	022	DC2 (device control 2)
19	13	023	DC3 (device control 3)
20	14	024	DC4 (device control 4)
21	15	025	NAK (negative acknowledge)
22	16	026	SYN (synchronous idle)
23	17	027	ETB (end of trans. block)
24	18	030	CAN (cancel)
25	19	031	EM (end of medium)
26	1A	032	SUB (substitute)
27	1B	033	ESC (escape)
28	1C	034	FS (file separator)
29	1D	035	GS (group separator)
30	1E	036	RS (record separator)
31	1F	037	US (unit separator)

XOR □

BS US NAK BEL

ELEE 00101 01100 00101
00101

Xor □

BS US NAK BEL 01000 11111 10101
00111

01101 10011 10000 00010

====> CR DC3 DLE STX

R2

ENQ FS DC2 EOT

L2

DECRYPTION

R2

CR DC3 DLE STX

L2

ENQ FS DC2 EOT

Key = 3

Xor □

BS US NAK BEL

BS US NAK BEL 01000 11111 10101
00111

Xor □

CR DC3 DLE STX 01101 10011 10000
00010

R1

ENQ FS DC2 EOT

00101 01100 00101 00101

|| L1

ELEE

Xor □

Key = 2

GNGG

GNGG 00111 01110 00111
00111

Xor □

ENQ FS DC2 EOT 00101 11100 10010 00100

R0

ELEE

00010 10010 10101 00011

|| L0

BRUC

Decrypted => BRUCELEE