

Ayesha Bibi

Information Security

Assignment # 02

This assignment is based on Cryptography - - - - -

Your message:

"ARRANGE A TRIP
AFTER THE EXAMS."

Task 1:-

In first product cipher..

⇒ Stage 1:-

Generate cipher text
of given message using
Caesar Cipher using "Key=3"

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

P.T: ARRANGE A TRIP AFTER

THE EXAMS. Key = 3:

C.T = DUUDQJH D WULS

DIW HU WKH HADPV

Stage #2:-

Use the output of
ceaser as input to Simple
Vigenere Cipher ----- key
will be your first name.

P.T: DUUDQJH D WULS

DIW HU WKH HADPV.

Key = Ayesha

~~Vigenere Cipher~~

P.T	D	U	U	D	Q	J	H	D	W	U	L	S	D	I
	3	20	20	3	16	9	7	3	22	20	11	18	3	8
	3	44	24	21	23	9	7	27	26	38	18	18	3	32
	0	24	4	18	7	0	0	24	4	18	7	0	0	24
Key =	A	Y	E	S	H	A	A	Y	E	S	H	A	A	Y
C.T	D	S	Y	V	X	J	H	B	A	M	S	S	D	G

P.T	W	H	U	W	K	H	H	A	D	P	V
	22	7	20	22	10	7	7	0	3	15	21
	26	25	27	29	10	31	11	18	10	15	21
	4	18	7	0	0	24	4	18	7	0	0
key	E	S	H	A	A	Y	E	S	H	A	A
C.T	A	Z	B	W	K	F	L	S	K	P	V

Formula $\Rightarrow C = E(P) = (P + k) \bmod(26)$

C.T: DSYVXJHBAMSSDGAZBWKFL
SKPV

Stage #3:

autokey = 'BIBI' key will be

your last name.

P.T = DSYVXJHBAMSSDGAZBWKFLSKPV

Key = BIBIDSYVXJHBAMSSDGAZBWKFL

P.T	D	S	Y	V	X	J	H	B	A	M	S	S	D	G
	3	18	24	21	23	9	7	1	0	12	18	18	3	6
	4	26	25	29	26	27	31	22	23	21	25	19	3	18
	1	8	1	8	3	18	24	21	23	9	7	1	0	12
key	B	I	B	I	D	S	Y	V	X	J	H	B	A	M
C.T	E	A	Z	D	A	B	F	W	X	V	Z	T	D	S

P.T. ←	A	Z	B	W	K	F	L	S	K	P	V
0	25	1	22	10	5	11	18	10	15	21	
18	43	4	28	10	30	12	40	20	20	32	
18	18	3	6	0	25	1	22	10	5	21	
key ←	S	S	D	G	A	Z	B	W	K	P	L
C.T. →	S	R	E	C	K	E	M	O	U	U	G

C.T: EAZDABFWXVZTDSSRECKE
MOUUG.