COMPUTER SECURITY ASSIGNMENT

ADITYA
1605004

12. Using the Euclidean algorithm, find the gcd of :

(a) 88 and 220

q	r_1	r_2	r
0	88	220	88
2	220	88	44
2	88	44	0

$\boxed{\text{GCD}(88, 220) = 44}$

(b) 300 and 42

q	r_1	r_2	r
7	300	42	6
7	42	6	0
	$\textcircled{6}$	0	

$\boxed{\text{GCD } (300, 42) = 6}$

(c) 24 and 320

q	r_1	r_2	r
0	24	320	24
13	320	24	8
3	24	8	0
	$\textcircled{8}$	0	

$\boxed{\text{GCD } (24, 320) = 8}$

ADITYA
1605004

(d) 401 and 700

q	r_1	r_2	r
0	401	700	401
1	700	401	299
1	401	299	102
2	299	102	95
1	102	95	7
13	95	7	4
1	7	4	3
1	4	3	1
3	3	1	0
	$\boxed{1}$	0	

GCD (401, 700) = 1

16. Using the ext. Euclidean algo., find gcd:

(a) 4 and 7

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	4	7	4	1	0	1	0	1	0
1	7	4	3	0	1	-1	1	0	1
1	4	3	1	1	-1	2	0	1	-1
3	3	1	0	-1	2	-7	1	-1	4
	1	0		2	-7		-1	4	

GCD (4, 7) = 1

$s = 2$

$t = -1$

ADITYA
1605006

(b) 291 and 42

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
6	291	42	39	1	0	1	0	1	-6
1	42	39	3	0	1	-1	1	-6	7
13	39	3	0	1	-1	14	-6	7	-97
	3	0		-1	14		7	-97	

GCD (291, 42) = 3

s = -1

t = 7

(c) 84 and 320

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
						1	0	1	0
0	84	320	84	1	0	1	0	1	0
3	320	84	68	0	1	-3	1	0	1
1	84	68	16	1	-3	4	0	1	-1
4	68	16	4	-3	4	-19	1	-1	5
4	16	4	0	4	-19	80	-1	5	-21
	4	0		-19	80		5	-21	

GCD(84, 320) = 4

S = -19

t = 5

(d) 400 and 60

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
									-6
6	400	60	4	1	0	1	0	1	
			0	0	0	1	-15	-6	91
15	60	4							
	4			1	-15		-6	91	

GCD (400, 60) = 4

s = 1

t = -6

ADITYA
1605004

21. Encrypt the message "this is an exercise" using one of the following ciphers. Decipher while ignoring the text.

~~[illegible]~~

<text> = "this is an exercise"

Ans.

cipher	plaintext	ciphertext
Additive cipher (key = 20)	<text>	NBCMCMUHY RYLWCMY
Multiplicative cipher (key = 15)	<text>	ZBQKQKANIHIVEQKI
Affine, (key = 15, 20)	<text>	TVKEKEU HCBCPYKEC

22. Encrypt <text> = "the house is being sold tonight".

cipher	plaintext	ciphertext
Vigenere (key = "dollars")	<text>	WVPSOLKHWDME ZFJGZWDKGQWRST
Autokey (key = 7)	<text>	AALLVIMWMATFMVTYG ZOWHBVONA

25. Use a Hill cipher "We live in an insecure world".

Use:

$$key = \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$$

ADITYA

1605004

$$\underset{c}{\begin{bmatrix} 8 & 20 \\ 21 & 0 \\ 5 & 18 \\ 11 & 3 \\ 13 & 13 \\ 11 & 3 \\ 22 & 12 \\ 2 & 14 \\ 19 & 10 \\ 6 & 12 \\ 2 & 07 \\ 4 & 25 \end{bmatrix}} = \underset{P}{\begin{bmatrix} 22 & 4 \\ 11 & 8 \\ 21 & 4 \\ 08 & 13 \\ 00 & 13 \\ 08 & 13 \\ 18 & 4 \\ 02 & 20 \\ 17 & 4 \\ 22 & 14 \\ 17 & 11 \\ 03 & 25 \end{bmatrix}} \times \underset{K}{\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}}$$

IUVAFSLDNNL DWMCOTKGMCHE$\boxed{Z}$

bogus.

ADITYA
1605004