__/__/____

Assignment - I

PES2UG20CS209
Naman Chaudhary

1. Plaintext = FIREWALL
Key = OCCURENCES

Playfair square:

O	C	U	R	E
N	S	A	B	D
F	G	H	I/J	K
L	M	P	Q	T
V	W	X	Y	Z

Encypted Message = GKEOXSPVPV

2. ~~Ciphertext~~ Plaintext : WELCOME TO PES UNIVERSITY
Key : 7
Cipher text : DLSJVTL AV WLZ BUPCLYZPAF

3. HELLO AND WELCOME TO THE WORLD OF CRYPTOGRAPHY

```
H         W           O           D
 E      D E       T     T       L
  L    N    L       E     H   R
   L  A      C  M          E O
    ●          O            W

O        G
 F      O R    Y
  C  T     A H
   R P      P
    Y
```

=> Cipher text = HWODOEDE TTLOTGLNLEHRFP
RYLACMEOCYAHOOWRP

_/_/____

4. Key 1: BRIDGE

Key 2: OVER

Plaintext: THIS IS ASSIGNMENT ONE

Cipher:

①	⑥	⑤	②	④	③	
B	R	I	D	G	E	key 1
T	H	I	S	I	S	
A	S	S	I	G	N	
M	E	N	T	O	N	
E	Q	Q	Q	Q	Q	

Ciphertext: TAME SITQ SNNQ IGOQ ISNQ HSEQ

②	④	①	③	
O	V	E	R	key 2
T	A	M	E	
S	I	T	Q	
S	N	N	Q	
I	G	O	Q	
I	S	N	Q	
H	S	E	Q	

Ciphertext: MTNONE TSSIIH EQQQQQ AINGSS

Decipher:

Key: OVER

Key 2

2	4	1	3
O	V	E	R
T	A	M	E
S	I	T	Q
S	N	N	Q
I	G	O	Q
I	S	N	Q
M	S	E	Q

=> Plaintext: TAME SITQ SNNQ IGOQ ISNQ MSE Q

Key: BRIDGE

1	6	5	2	4	3
B	R	I	D	G	E
T	H	I	S	I	S
A	S	S	I	G	N
M	E	N	T	O	N
E	Q	Q	Q	Q	Q

=> Plaintext : THISIS ASSIGNMENTONE QQQQQ

__/__/____

5. Known Plaintext	Chosen cipher text
• Plaintext cannot be selected but can observe plain-text — ciphertext pairs	• Plaintext can be selected, and encrypted to observer ciphertext & reverse the entire process
• Comparitively harder	• Comparitively easier

6. $Key = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 2 & 12 & 15 \end{bmatrix}$, Plaintext = APT $= \begin{bmatrix} 0 \\ 15 \\ 19 \end{bmatrix}$

$E = PK \bmod 26$

$$(0 \quad 15 \quad 19) \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 2 & 12 & 15 \end{bmatrix} = \begin{bmatrix} 103 & 308 & 335 \end{bmatrix} \% 26$$

$= [25 \quad 22 \quad 23] = [2 \quad W \quad X]$

Decryption: $C = [2 \quad W \quad X]$

~~K^{-1}~~ $\cdot K^{-1} C \bmod 26$

$|K| = 6(240 - 120) - 24(195 - 20) + (156 - 32) = (-3356)$

$AB = 1 \bmod 26$

~~A(-335~~ $(-3356) A = 1 \bmod 26$

$\Rightarrow \boxed{\text{A cannot be found}}$

__/__/__

7. a) gcd (6150, 704)

Euclidean algorithm. [gcd(a,b) = gcd (b,r)]

a	b	r
6150	704	518
704	518	186
518	186	146
186	146	40
146	40	26
40	26	14
26	14	12
14	12	2
12	$\boxed{2}$	0

$\Rightarrow$ gcd(6150, 704) = 2

Stein's algorithm.

$A_1 = 6150$, $B_1 = 704$, $C_1 = 1$

(both even) $\Rightarrow A_2 = 3075$, $B_2 = 352$, $C_2 = 2$

(Odd / Even) $\Rightarrow A_3 = 3075$, $B_3 = 176$, $C_3 = 2$

$A_4 = 3075$, $B_4 = 88$, $C_4 = 2$

$A_5 = 3075$, $B_5 = 44$, $C_5 = 2$

$A_6 = 3075$, $B_6 = 22$, $C_5 = 2$

$A_7 = 3075$, $B_7 = 11$, $C_7 = 2$

(odd/odd) $\Rightarrow A_8 = 3064$, $B_8 = 11$, $C_8 = 2$

(Even / odd) $\Rightarrow A_9 = 1532$, $B_9 = 11$, $C_9 = 2$

$A_{10} = 766$, $B_{10} = 11$, $C_{10} = 2$

$A_{11} = 383$, $B_{11} = 11$, $C_{11} = 2$

(odd/odd) $\Rightarrow A_{12} = 372$, $B_{12} = 11$, $C_{12} = 2$

(Even / odd) $\Rightarrow A_{13} = 186$, $B_{13} = 11$, $C_{13} = 2$

$A_{14} = 93, \quad B_{14} = 11, \quad C_{14} = 2$

$A_{15} = 82, \quad B_{15} = 11, \quad C_{15} = 2$

$A_{16} = 41, \quad B_{16} = 11, \quad C_{16} = 2$

$A_{17} = 30, \quad B_{17} = 11, \quad C_{17} = 2$

$A_{18} = 15, \quad B_{18} = 11, \quad C_{18} = 2$

$A_{19} = 4, \quad B_{19} = 11, \quad C_{19} = 2$

$A_{20} = 2, \quad B_{20} = 11, \quad C_{20} = 2$

$A_{21} = 1, \quad B_{21} = 11, \quad C_{21} = 2$

$A_{22} = 10, \quad B_{22} = 1, \quad C_{22} = 2$

$A_{23} = 5, \quad B_{23} = 1, \quad C_{23} = 2$

$A_{24} = 4, \quad B_{24} = 1, \quad C_{24} = 2$

$A_{25} = 2, \quad B_{25} = 1, \quad C_{25} = 2$

$A_{26} = 1, \quad B_{26} = 1, \quad C_{26} = 2$

$A_{26} = B_{26}$

$\therefore, \gcd(A, B) = A_{26} \cdot C_{26} = 1 \times 2$

$\therefore, \gcd(6150, 704) = 2$

6) Euclian Algorihm uses repeated modulo operator, while in Stein's algorihm, repeated bitewise shifts are used, which is faster, implies they have slightly better efficiency

8.

a) $4x \equiv 2 \pmod{3}$

$\Rightarrow 4(2) \bmod 3 = 2$

$\Rightarrow 8 \bmod 3 = 2$

$\therefore, \boxed{x = 2}$

b) $7x \equiv 4 \pmod{9}$

$\Rightarrow$ ~~$7(4)$ mod 9~~

$\Rightarrow 7(x) \bmod 9 = 4$

$\Rightarrow 7(7) \bmod 9 = 4 \quad \Rightarrow 49 \bmod 9 = 4$

$\Rightarrow \boxed{x = 7}$

c) $5x \equiv 3 \pmod{11}$

$\Rightarrow 5(5) \bmod 11 = 3 \Rightarrow 25 \bmod 11 = 3$

$\Rightarrow \boxed{x = 5}$