Advanced CNS H.W.

- Dheeraj Bhaskaruni
- 904303366

1] plain text = 'helpme'

Encryption fn ⇒ $c = 5m + 7 \pmod{26}$

assumption $a = 0$, $b = 1$, ... $z = 25$

Word	m (value)	$5m+7$	$c = 5m+7 \pmod{26}$	cipher text
h	7	$5(7)+7=42$	$42 \bmod 26 = 16$	q
e	4	$5(4)+7=27$	$27 \bmod 26 = 1$	b
l	11	$5(11)+7=62$	$62 \bmod 26 = 10$	k
p	15	$5(15)+7=82$	$82 \bmod 26 = 4$	e
m	12	$5(12)+7=67$	$67 \bmod 26 = 15$	p
e	4	$5(4)+7=27$	$27 \bmod 26 = 1$	b

cipher text of 'helpme' is 'qbkepb'

2]

$c = (11m + 2) \bmod 26$

To decrypt, $m = a^{-1}(c - b) \bmod 26$

$a = 11 \quad b = 2$

$m = 11^{-1}(c - 2) \bmod 26$

Finding modular inverse of 11 modulo 26

we need a^{-1} such that

$11 \times a^{-1} \equiv 1 \pmod{26}$

to get a^{-1}, substituting all possible values to make it 1

$209 \bmod 26 = 1 \iff (11 \times 19) \bmod 26 = 1$

$\Rightarrow a^{-1} = 19$

$\Rightarrow$ Decryption formula $\Rightarrow m = 19(c-2) \bmod 26$

Encrypted text	Value	Decrypt $\Rightarrow m = 19(c-2) \bmod 26$	Decrypt value	Message letters
v	21	$19(21-2) \bmod 26 = 361 \bmod 26$	23	x
m	12	$19(12-2) \bmod 26 = 190 \bmod 26$	8	i
w	22	$19(22-2) \bmod 26 = 380 \bmod 26$	16	q
z	25	$19(25-2) \bmod 26 = 437 \bmod 26$	21	v

The decryption of 'vmwz' is 'xiqv'

---

3) Given $C = MK \pmod{26}$

where block of letters is $M = [m_1, m_2]$ & cipher text is $C = [c_1, c_2]$ & the key is 2x2 matrix

$$K = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$$

following usual correspondence $a=0, b=1, \dots z=25$

plaintext $\to$ "friday". $\Rightarrow$ ciphertext = pqcfku

Block 1: fr & pq

Block 2: id & cf

Block 3: ay & ku

Block	Plain text	Cipher text
Block 1	[f, r] = [5, 17]	[P, q] = [15, 16]
Block 2	[i, d] = [8, 3]	[c, f] = [2, 5]
Block 3	[a, y] = [0, 24]	[K, U] = [10, 20]

eqns:

$$[m_1, m_2] \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix} = [c_1, c_2] \pmod{26}$$

Block 1:

$$5K_{11} + 17K_{21} = 15 \pmod{26} \quad — (1)$$

$$5K_{12} + 17K_{22} = 16 \pmod{26} \quad — (2)$$

Block 2:

$$8K_{11} + 3K_{21} \equiv 2 \pmod{26} \quad — (3)$$

$$8K_{12} + 3K_{22} = 5 \pmod{26} \quad — (4)$$

Block 3:

$$24K_{21} = 10 \pmod{26} \quad — (5)$$

$$24K_{22} = 20 \pmod{26} \quad — (6)$$

Solve for K_{21} and K_{22}

$$24K_{21} \equiv 10 \bmod 26$$

divide the equation by 2 ; $12K_{21} \equiv 5 \pmod{13}$

$\because 12 \equiv -1 \pmod{13} \Rightarrow -K_{21} = 5 \pmod{13}$

$\Rightarrow K_{21} = -5 = 8 \pmod{13}$

$\Rightarrow$ We choose positive value $\boxed{K_{21} = 8}$

same steps ,

$$24K_{22} \equiv 20 \pmod{26}$$

$$12K_{22} \equiv 10 \pmod{13}$$

$\because$ $12 \equiv -1 \pmod{13}$, this gives

$-K_{22} = 10 \pmod{13} \Rightarrow K_{22} = -10 \equiv 3 \pmod{13}$

$\Rightarrow$ we choose positive value $\boxed{K_{22} = 3}$

Solving for K_{11} and K_{12}

Substitute $K_{21} = 8$ & $K_{22} = 3$

in 3 & 4

$8K_{11} + 3(8) \equiv 2 \pmod{26} \Rightarrow 8K_{11} + 24 = 2 \pmod{26}$

$\Rightarrow 8K_{11} = 2 - 24 = -22 = 4 \pmod{26}$

$gcd(8, 26) = 4$

$\Rightarrow \quad 4K_{11} \equiv 2 \pmod{13}$

multiplicative inverse of 4 modulo 13 is 10, multiply 10 on both sides

$\because \; 4 \times 10 = 40 \equiv 1 \pmod{13}$

$\Rightarrow \quad K_{11} \equiv 2 \times 10 \equiv 20 \pmod{13} = 7$

check with eqn 1

$5(7) + 17(8) = 35 + 136 = 171 \equiv 171 - 156$

$= 15 \pmod{26}$

correct

Solve for K_{12} using eqn 4

$8K_{12} + 3(3) \equiv 5 \pmod{26} \Rightarrow 8K_{12} + 9 \equiv 5 \pmod{26}$

$8K_{12} \equiv 5 - 9 \equiv -4 \equiv 22 \pmod{26}$

$gcd(8, 26) = 2$ and 22 is divisible by 2

$4K_{12} \equiv 11 \pmod{13}$

Again, multiply by inverse of 4 modulo (13) which is 10

$K_{12} \equiv 11 \times 10 = 110 \pmod{13}$

$K_{12} \equiv 6 \pmod{13}$

Check with eqn 2

$$5K_{12} + 17K_{22} \equiv 16 \pmod{26}$$

If $K_{12} = 6$ & $K_{22} = 3$

$5(6) + 17(3) = 30+51 = 81 \equiv 81-78 = 3 \pmod{26}$
$\neq 16$

If $K_{12} = 9$ & $K_{22} = 3$

$5(19) + 17(3) = 95+51 = 146 \equiv 146-130 = 16 \pmod{26}$

$K_{12} = 9$

$\Rightarrow$ The determined key is

$$K = \begin{bmatrix} 7 & 19 \\ 8 & 3 \end{bmatrix} \pmod{26}$$

$\boxed{\text{Verified}}$

$\boxed{4}$ (a) $17^{-1} \bmod 101$

$\Rightarrow \quad 17x \equiv 1 \pmod{101}$

Extended Euclidian algo

1] $101/17 \quad \Rightarrow \quad 101 = 17 \times 5 + 16$ (rem=16)

2] $17/16 \quad \Rightarrow \quad 17 = 16 \times 1 + 1$ (rem = 1)

3] $16/1 \quad \Rightarrow \quad 16 = 1 \times 16 + 0$

$\because$ remainder is 0, gcd is the last non zero remainder $\Rightarrow$ $\gcd(17, 101) = 1$

Back substitution

$$1 = 17 - 16 \times 1$$

$$\Rightarrow \quad 16 = 101 - 17 \times 5$$

$$1 = 17 - (101 - 17 \times 5)$$
$$= 17 - 101 + 17 \times 5$$
$$= 17 \times \underline{\underline{6}} - 101$$

$$\Rightarrow \quad 17 \times 6 - 101 \times 1 = 1$$

$$\Rightarrow \quad \boxed{x = 6} \quad \Rightarrow \quad \boxed{17^{-1} \equiv 6 \pmod{101}}$$

(b) $357^{-1} \bmod 1234$

EED

$$1234 = 357(3) + 163$$
$$357 = 163(1) + 31$$
$$163 = 31(5) + 8$$
$$31 = 8(3) + 7$$
$$8 = 7(1) + 1$$

$$\Rightarrow \quad GCD(357, 1234) = 1$$

$$8 = 7 + 1$$
$$8 = 31 - 8(3) + 1$$
$$8(4) = 31 + 1$$
$$(163 - 31(5)).(4) = 31 + 1$$
$$163(4) = 31(21) + 1$$
$$163(4) = (357 - 163(2))(21) + 1$$
$$163(4\cancel{6}) = 357(21) + 1$$

$(1234 - 357(3))(46) = 357(21) + 1$

$357(-159) \equiv 1 \mod 1234$

$357(1075) \equiv 1 \mod 1234$

$\Rightarrow$ $\boxed{357^{-1} \bmod 1234 = 1075}$

(c) $3125^{-1} \pmod{9987}$

EED:

~~1234~~ $9987 = 3125 \times 3 + 612$

$3125 = 612 \times 5 + 65$

$612 = 65 \times 9 + 27$

$65 = 27 \times 2 + 11$

$27 = 11 \times 2 + 5$

$11 = 5 \times 2 + 1$

$5 = 1 \times 5 + 0$

$GCD(3125, 9987) = 1$

Back subs:

$1 = 11 - 5 \times 2$

$5 = 27 - 11 \times 2$

$11 = 65 - 27 \times 2$

$27 = 612 - 65 \times 9$

$65 = 3125 - 612 \times 5$

$113 \times 5 + 12 = 565 + 12 = 577$

$\Rightarrow 612 = 9987 - 3125 \times 3$

$1 = 113 + (577 \times 3) \times 3125 - 577 \times 9987$

$577 \times 3 = 1731, \quad 113 + 1731 = 1844$

$1844 \times 3125 - 577 \times 9987 = 1$

$\Rightarrow \quad 3125^{-1} \equiv 1844 \pmod{9987}$

$\Rightarrow \boxed{3125^{-1} \pmod{9987} = 1844}$

$\boxed{6}$ $\quad Pr[a] = 1/2 \quad Pr[b] = 1/3 \quad Pr[c] = 1/6$

$H(P) = \frac{1}{2}\log_2 2 + \frac{1}{3}\log_2 3 + \frac{1}{6}\log_2 6 = \frac{2}{3} + \frac{1}{2}\log_2 3 \simeq 1.459$

$\boxed{H(P) = 1.459}$

$H(K) \Rightarrow P_r[K_1] = Pr[K_2] = Pr[K_3] = 1/3$

$H(K) = \log_2(3) = 1.585$ bits

H(C)

$\Rightarrow$ K_1 sends $a \to 1$ $b \to 2$ $c \to 3$

K_2 $a \to 2$ $b \to 3$ $c \to 4$

K_3 $a \to 3$ $b \to 4$ $c \to 1$

$\Rightarrow$

P	K	C	$P_r[P]$	$P_r[K]$	Product $P_r[P,K]$
a	K_1	1	1/2	1/3	1/6
a	K_2	2	1/2	1/3	1/6
a	K_3	3	1/2	1/3	1/6
b	K_1	2	1/3	1/3	1/9
b	K_2	3	1/3	1/3	1/9
b	K_3	4	1/3	1/3	1/9
c	K_1	3	1/6	1/3	1/18
c	K_2	4	1/6	1/3	1/18
c	K_3	1	1/6	1/3	1/18

$\Rightarrow$ $P_r[C=1] = \frac{2}{9}$

$P_r[C=2] = \frac{5}{18}$

$P_r[C=3] = \frac{6}{18} = \frac{1}{3}$

$P_r[C=4] = \frac{3}{18} = \frac{1}{6}$

$\Rightarrow$ $H(C) = -\sum_{c \in \{1,2,3,4\}} P_r[c] \log_2(P_r[c]) \Rightarrow H(C) \simeq 1.955$ bits

$\underline{H(K)}$ Keys choosen equiprobably

$$H(K) = \frac{1}{3}\log_2 3 + \frac{1}{3}\log_2 3 + \frac{1}{3}\log_2 3 \simeq 1.585 \text{ bits}$$

$\underline{H(K/C)}$

$$H(K/C) = H(K) + H(P) - K(C) \approx 1.089$$

$\underline{H(P|C)}$

$$H(P|C) = H(P,C) - H(C)$$

$$H(P,C) = H(P) + H(C/P)$$

once P is fixed, the randomness in C, comes from K

$$\Rightarrow H(C|P) = \sum_{P \in \{a,b,c\}} P_r[P]\, H(C|P=p) = \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{6}\right)\log_2(3)$$

$$= \log_2(3) \simeq 1.585 \text{ bits}$$

$$\Rightarrow H(P,C) = H(P) + H(C|P) = 1.459 + 1.585$$

$$= 3.044$$

$$\Rightarrow H(P|C) = H(P,C) - H(C) = 3.044 - 1.955$$

$$\approx 1.089 \text{ bits}$$

7\]

$x \equiv 12 \pmod{25}$

$x \equiv 9 \pmod{26}$

$x \equiv 23 \pmod{27}$

Chinese Remainder Theorem :-

$\gcd(25,26) = 1$; $\gcd(26,27) = 1$; $\gcd(27,25) = 1$

Modulus, $M = 25 \times 26 \times 27 = 17550$

$\Rightarrow$ Computing individual terms

(i) $x \equiv 12 \pmod{25}$

$M_1 = \frac{M}{25} = 702$

$702 \cdot y_1 \equiv 1 \pmod{25}$

$\Rightarrow 2 \cdot y_1 \equiv 1 \pmod{25} \Rightarrow \boxed{y_1 = 13}$

(ii) $x \equiv 9 \pmod{26}$

$M_2 = \frac{M}{26} = 675$

$675\, y_2 \equiv 1 \pmod{26}$

$\Rightarrow 25\, y_2 = 1 \pmod{26} \Rightarrow \boxed{y_2 = 25}$

(iii) $x \equiv 23 \pmod{27}$

$M_3 = \frac{M}{27} = 650$

$650\, y_3 = 1 \pmod{27} \Rightarrow \boxed{y_3 = 14}$

$2 \cdot y_3 \equiv 1 \pmod{27}$

Applying CRT formula

$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

$x = 12 \times 702 \times 13 + 9 \times 675 \times 25 + 23 \times 650 \times 14$

$x = 470687$

$\Rightarrow \quad x \equiv 470687 \bmod 17550 \Rightarrow x \equiv 14387 \bmod (17550)$

$\Rightarrow \boxed{x = 14387 \pmod{17550}}$

8] (a) compute powees and factor therom

1] $2^{32} \bmod 227$

$2^2 = 4$

$2^4 = 16$

$2^8 = 16^2 = 256 - 227 = 29$

$2^{16} = 29^2 = 84 \equiv 841 - 3(227) = 160$

$2^{32} = 160^2 = 25600 \equiv 2560 - 112 \cdot (227) = 176$

$\Rightarrow \quad 2^{32} \equiv 176 \pmod{227}$

factor over base

$176 = 16 \times 11 = 2^4 \cdot 11$

2] $2^{40} \bmod 227$

$$2^{40} = 2^{32} \cdot 2^{8} \Rightarrow 2^{32} \equiv 176 \qquad 2^{8} = 29$$

$$\Rightarrow 176 \times 29 = 5104$$

Reduce:

$$\Rightarrow 227 \times 22 = 4994 \Rightarrow 5104 - 4994 = 110$$

factor over base $= 110 \Rightarrow 2 \times 5 \times 11$

3] $2^{59} \bmod 227$:

$$59 = 32 + 16 + 8 + 3 \quad (\because 2^{59} = 2^{32} \cdot 2^{16} \cdot 2^{8} \cdot 2^{3})$$

$$\Rightarrow 176 \times 160 \times 29 \times 8 = 6533120$$

Reduce $6533120 \pmod{227} = 60$

factor over base $= 60 \Rightarrow 2^{2} \cdot 3 \cdot 5$

4] $2^{156} \bmod 227$

$$2^{156} = \left(\left(2^{32}\right)^{2}\right)^{2} \cdot 2^{16} \cdot 2^{8} \cdot 2^{4}$$

$$= \left(\left(176\right)^{2}\right)^{2} \times 160 \times 29 \times 16$$

2^{128} compute

$2^{32} \equiv 176$

$176^2 \Rightarrow 30976 - 227(136) = 104$

$2^{64} = 104$

$2^{128} \Rightarrow 2^{64} \times 2^{64} \Rightarrow 104 \times 104 - 227(47)$

$= 147$

$\Rightarrow$ $2^{128} \times 2^{16} \times 2^{8} \times 2^{4}$

$147 \times 160 \times 29 \times 16 = 10913280$

$\Rightarrow$ $10913280 \pmod{227} = 28$

factor over base $\Rightarrow 4 \cdot 7 = 2^2 \cdot 7$

(b) Compute Discrete logs

1] $2^{32} \equiv 2^4 \cdot 11$

$32 \equiv 4 + \log_2(11) \mod 226$

$\Rightarrow \boxed{\log_2(11) \equiv 32 - 4 = 28}$

2] $2^{40} \equiv 2 \cdot 5 \cdot 11$

$40 \equiv 1 + \log_2(5) + \log_2(11) \pmod{226}$

$\Rightarrow \boxed{\log_2(5) \equiv 40 - 1 - 28 = 11}$

3) $2^{59} \equiv 2^2 \cdot 3 \cdot 5$

$\Rightarrow$

$59 \equiv 2 + \log_2(3) + \log_2(5) \pmod{226}$

$\Rightarrow \boxed{\log_2(3) = 59 - 2 - 11 = 46}$

4) $2^{156} \equiv 2^2 \cdot 7$

$156 \equiv 2 + \log_2(7) \pmod{226}$

$\boxed{\log_2(7) \equiv 156 - 2 = 154}$

---

9) $57s + 93t = \gcd(57, 93)$

$\gcd(57, 93)$

$93 = 57 \times 1 + 36$

$57 = 36 \times 1 + 21$

$36 = 21 \times 1 + 15$

$21 = 15 \times 1 + 6$

$15 = 6 \times 2 + 3$

$6 = 3 \times 2 + 0$

from ①

$$
\begin{aligned}
3 &= 15-(6\times 2) \\
&= 15-2(21-15) \\
&= 15-2(21)+2(15) \\
&= 3(15)-2(21) \\
&= 3(36-21)-2(21) \\
&= 3(36)-3(21)-2(21) \\
&= 3(36)-5(21) \\
&= 3(36)-5(57-36) \\
&= 8(36)-5(57) \\
&= 8(93-57)-5(57) \\
&= 8(93)-13(57)
\end{aligned}
$$

$\Rightarrow \quad s=-13 \; ; \quad t=8$

Problem 5
Code:

code.py

```python
# problem 5
1 usage
def decrypt(ciphertext, key):
    plaintext = ""
    for character in ciphertext:
        if character.isalpha():
            shift = (ord(character) - ord('A') - key) % 26
            plaintext += chr(shift + ord('A'))
        else:
            plaintext += character
    return plaintext

ciphertext = "BEEAKFYDIXUQYHYJIQRYHTYoIQFBQDUYIIIKFUHCQD"

print("ciphertext:", ciphertext)
print("\nTrying all keys (0-25):\n")

for key in range(26):
    decrypted_text = decrypt(ciphertext, key)
    print(f"Key {key:2d}: {decrypted_text}")
```

Output:

```
/usr/local/bin/python3.11 /Users/dheeraj_bhaskaruni/Documents/Prep/adv_cns_hw/cpde.py
Ciphertext: BEEAKFYDIXUQYHYJIQRYHTYoIQFBQDUYIIIKFUHCQD

Trying all keys (1-25):

Key  1: ADDZJEXCHWTPXGXIHPQXGSXTHPEAPCTXHHHJETGBPC
Key  2: ZCCYIDWBGVSOWFWHGOPWFRWSGODZOBSWGGGIDSFAOB
Key  3: YBBXHCVAFURNVEVGFNOVEQVRFNCYNARVFFFHCREZNA
Key  4: XAAWGBUZETQMUDUFEMNUDPUQEMBXMZQUEEEGBQDYMZ
Key  5: WZZVFATYDSPLTCTEDLMTCOTPDLAWLYPTDDDFAPCXLY
Key  6: VYYUEZSXCROKSBSDCKLSBNSOCKZVKXOSCCCEZOBWKX
Key  7: UXXTDYRWBQNJRARCBJKRAMRNBJYUJWNRBBBDYNAVJW
Key  8: TWWSCXQVAPMIQZQBAIJQZLQMAIXTIVMQAAACXMZUIV
Key  9: SVVRBWPUZOLHPYPAZHIPYKPLZHWSHULPZZZBWLYTHU
Key 10: RUUQAVOTYNKGOXOZYGHOXJOKYGVRGTKOYYYAVKXSGT
Key 11: QTTPZUNSXMJFNWNYXFGNWINJXFUQFSJNXXXZUJWRFS
Key 12: PSSOYTMRWLIEMVMXWEFMVHMIWETPERIMWWWYTIVQER
Key 13: ORRNXSLQVKHDLULWVDELUGLHVDSODQHLVVVXSHUPDQ
Key 14: NQQMWRKPUJGCKTKVUCDKTFKGUCRNCPGKUUUWRGTOCP
Key 15: MPPLVQJOTIFBJSJUTBCJSEJFTBQMBOFJTTTVQFSNBO
Key 16: LOOKUPINSHEAIRITSABIRDIESAPLANEISSSUPERMAN
Key 17: KNNJTOHMRGDZHQHSRZAHQCHDRZOKZMDHRRRTODQLZM
Key 18: JMMISNGLQFCYGPGRQYZGPBGCQYNJYLCGQQQSNCPKYL
Key 19: ILLHRMFKPEBXFOFQPXYFOAFBPXMIXKBFPPPRMBOJXK
Key 20: HKKGQLEJODAWENEPOWXENZEAOWLHWJAEOOOQLANIWJ
Key 21: GJJFPKDINCZVDMDONVWDMYDZNVKGVIZDNNNPKZMHVI
Key 22: FIIEOJCHMBYUCLCNMUVCLXCYMUJFUHYCMMMOJYLGUH
Key 23: EHHDNIBGLAXTBKBMLTUBKWBXLTIETGXBLLLNIXKFTG
Key 24: DGGCMHAFKZWSAJALKSTAJVAWKSHDSFWAKKKMHWJESF
Key 25: CFFBLGZEJYVRZIZKJRSZIUZVJRGCREVZJJJLGVIDRE

Process finished with exit code 0
```

Based on the output **key 16** seems to have legitimate meaning, “LOOKUPINSHEAIRITSABIRDIESAPLANEISSSUPERMAN”