Name:
Student I.D:

Quiz 1

SOEN321: Fall 2020

IT IS REQUIRED TO SHOW THE DETAILS OF ALL OF YOUR CALCULATIONS

Prob. 1
Consider the Hill cipher in which the ciphertext is related to the plaintext using the form

$$(c1\ c2) = (p1\ p2) \begin{pmatrix} k1 & k2 \\ k3 & k4 \end{pmatrix} \bmod 26$$

The cryptanalyst observed the following plaintext/ciphertext pairs (p1 p2)/(c1 c2):
~~(15 2)/(18 17)~~ and ~~(2 11)/(3 22)~~. (5 6)/(21 2) and (11 1)/(20 25)

Determine the key corresponding to this system. Show all the details of your calculations.

Prob. 2
Consider an RSA system with ~~p=19~~, ~~q=17~~, and ~~e=247~~. Find the plaintext corresponding to ~~c=131~~.

p=13 q=7 e=31 c=33

Quiz 1

(1) $c_1 \; c_2 = p_1 \, p_2 (K)$

$$\begin{pmatrix} 21 & 2 \\ 20 & 25 \end{pmatrix} = \begin{pmatrix} 5 & 6 \\ 11 & 1 \end{pmatrix} K \mod 26$$

$$K = \begin{pmatrix} 5 & 6 \\ 11 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 21 & 2 \\ 20 & 25 \end{pmatrix} \mod 26$$

$$= \frac{1}{-61} \begin{pmatrix} 1 & -6 \\ -11 & 5 \end{pmatrix} \begin{pmatrix} 21 & 2 \\ 20 & 25 \end{pmatrix} \mod 26$$

$$= \frac{1}{17} \begin{pmatrix} 1 & 20 \\ 15 & 5 \end{pmatrix} \begin{pmatrix} 21 & 2 \\ 20 & 25 \end{pmatrix} \mod 26$$

$$= 23 \begin{pmatrix} 1 & 20 \\ 15 & 5 \end{pmatrix} \begin{pmatrix} 21 & 2 \\ 20 & 25 \end{pmatrix} \mod 26$$

$$= \begin{pmatrix} 23 & 460 \\ 345 & 115 \end{pmatrix} \begin{pmatrix} 21 & 2 \\ 20 & 25 \end{pmatrix} \mod 26$$

$$= \begin{pmatrix} 23 & 18 \\ 7 & 11 \end{pmatrix} \begin{pmatrix} 21 & 2 \\ 20 & 25 \end{pmatrix} \mod 26$$

$$= \begin{pmatrix} 843 & 496 \\ 367 & 289 \end{pmatrix} \mod 26$$

$$K = \begin{pmatrix} 11 & 2 \\ 3 & 3 \end{pmatrix}$$

$17^{-1} \mod 26$

$\gcd(17, 26)$

euclidian alg.

$26 = 1 \cdot 17 + 9$

$17 = 1 \cdot 9 + 8$

$9 = 1 \cdot 8 + 1$

extended euclidian

$1 = 9 - 8$

$1 = 9 - (17 - 9)$

$1 = 9 - 17 + 9 = 2 \cdot 9 - 17$

$1 = 2(\cancel{26} - 17) - 17 \; \underline{\text{mod } 26}$

$1 = -2 \cdot 17 - 17$

$1 = -3 \cdot 17 \mod 26$

$1 = \boxed{23} \cdot 17 \mod 26$

↳ check!

$23 \cdot 17 = 391$

$391 \mod 26 = 1$ ✓

② $p=13$ $q=7$ $e=31$ $c=33$

$2^0 - 1$

$2^1 - 2$

$2^2 - 4$

$2^3 - 8$

2^4

$m = c^d \bmod n$

$n = pq = 13 \cdot 7 = 91$

$m = 33^7 \bmod 91$

$7 = 111$

$33^1 = 33 \bmod 91 \leftarrow 1$

$33^2 = (33)^2 = 88 \bmod 91 \leftarrow 1$

$33^4 = (88)^2 = 9 \bmod 91 \leftarrow 1$

$m = 33 \cdot 88 \cdot 9 \bmod 91$

$= ((33 \cdot 88) \bmod 91) \cdot 9 \bmod 91$

$= 83 \cdot 9 \bmod 91$

$= 19 \bmod 91$

$m = 19$

$d = e^{-1} \bmod \phi(n)$

$\phi(n) = (1-p)(1-q)$

$= 12 \cdot 6$

$= 72$

$31^{-1} \bmod 72$

euclidian $\gcd(31, 72)$

$= 72 = 2 \cdot 31 + 10$

$31 = 3 \cdot 10 + \boxed{1}$

extended euclidian

$1 = 31 - 3(72 - 2 \cdot 31) \bmod 72$

$1 = 31 + 6 \cdot 31 \bmod 72$

$1 = 7 \cdot 31 \bmod 72$

check

$7 \cdot 31 = 217$

$217 \bmod 72 = 1$ ✓