

Midterm Activity No. 3 Substitution Cipher – Part 2

Name: Zambrona, Raph Kenneth M.
Subj. & Sec. IAAS -4B

Date: 10/10/2025

1: Create Your Cipher Identity

Each pair must generate their own:

- **Team Name:** CipherNomads
- **Unique Keyword for Playfair Cipher:** INCEPTION

2: Playfair Cipher Challenge

- **Secret Phrase: CODED CLUES UNDER THE BRIDGE**

Step 1 – Prepare the Message: Remove spaces and repeated letters (insert X between identical letters in a pair; pad at end if needed). → **CODEDCLUESUNDERTHEBRIDGE**

CO | DE | DC | LU | ES | UN | DE | RT | HE | BR | ID | GE |

Step 2 – Playfair Cipher Grid (Keyword: INCEPTION) (Replace J with I)

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

Step 3 – Encryption

Using the grid, the encrypted message becomes:

Encrypted Message: NA BP AP UZ BY QP BP MA KC AS PT KN

Step 4 – Decryption

Decrypting using the same grid yields:

Decrypted Message: NABPAPUZBYQBPMAKCASPTKN

 Decrypted Message: CODED CLUES UNDER THE BRIDGE

Short creative story (3 sentences):

A midnight courier dropped a folded scrap with the words **NABPAPUZBYQBPBMAKCASPTKN**. Only those who knew the “INCEPTION” method our team's keyword could unfold the secret. Decoding it revealed an old instruction: a map hidden under the bridge.

3: Hill Cipher Challenge

- **Short Phrase: TREASURE**

$$M = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$$

T(19) R(17) E(4) A(0) S(18) U(20) R(17) E(4)

(19, 17, 4, 0, 18, 20, 17, 4)

Split into column vectors (pairs):

- (19,17), (4,0), (18,20), (17,4)

Step 3 – Encryption: compute $C=M \cdot P \pmod{26}$

Pair	Computation	Encrypted
(19,17)	$(3 \times 19 + 3 \times 17 = 57 + 51 = 108 \rightarrow 4), (2 \times 19 + 5 \times 17 = 38 + 85 = 123 \rightarrow 19)$	(4,19) = E T
(4, 0)	$(3 \times 4 + 3 \times 0 = 12 \rightarrow 12), (2 \times 4 + 5 \times 0 = 8 \rightarrow 8)$	(12, 8) = M I
(18, 20)	$(3 \times 18 + 3 \times 20 = 114 \rightarrow 10), (2 \times 18 + 5 \times 20 = 136 \rightarrow 6)$	(10, 6) = K G
(17, 4)	$(3 \times 17 + 3 \times 4 = 63 \rightarrow 11), (2 \times 17 + 5 \times 4 = 54 \rightarrow 2)$	(11, 2) = L C

Final Hill ciphertext (letters): ETMIKGLC

Final Hill ciphertext (numeric pairs): (4,19), (12,8), (10,6), (11,2)

Step 4 – Decryption:

$$M = \begin{pmatrix} 5 & -3 \\ -2 & 3 \end{pmatrix}.$$

Multiply adjugate by $\det^{-1} \{-1\}^{-1} = 3$ and reduce mod 26:

$$M^{-1} \equiv 3 \cdot \begin{pmatrix} 5 & -3 \\ -2 & 3 \end{pmatrix} \equiv \begin{pmatrix} 15 & -9 \\ -6 & 9 \end{pmatrix} \equiv \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \pmod{26}.$$

So

$$M^{-1} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \pmod{26}.$$

Pair 1: (4,19)

First value: $(15 \times 4 + 17 \times 19) = 60 + 323 = 383 \rightarrow 383 \bmod 26 = 19 \rightarrow T$

Second value: $(20 \times 4 + 9 \times 19) = 80 + 171 = 251 \rightarrow 251 \bmod 26 = 17 \rightarrow R$

Decrypted pair: (19,17) \rightarrow T R

Pair 2: (0,2)

First value: $(15 \times 0 + 17 \times 2) = 0 + 34 = 34 \rightarrow 34 \bmod 26 = 8 \rightarrow I$

Second value: $(20 \times 0 + 9 \times 2) = 0 + 18 = 18 \rightarrow 18 \bmod 26 = S$

Decrypted pair: (8,18) \rightarrow I S

Pair 3: (18,20)

First value: $(15 \times 18 + 17 \times 20) = 270 + 340 = 610 \rightarrow 610 \bmod 26 = 4 \rightarrow E$

Second value: $(20 \times 18 + 9 \times 20) = 360 + 180 = 540 \rightarrow 540 \bmod 26 = 20 \rightarrow U$

Decrypted pair: (4,20) \rightarrow E U

Pair 4: (17,4)

First value: $(15 \times 17 + 17 \times 4) = 255 + 68 = 323 \rightarrow 323 \bmod 26 = 11 \rightarrow L$

Second value: $(20 \times 17 + 9 \times 4) = 340 + 36 = 376 \rightarrow 376 \bmod 26 = 12 \rightarrow M$

Decrypted pair: (11,12) \rightarrow L M

Cipher	Keyword / Matrix	Encrypted Message	Decrypted Message
Playfair	INCEPTION	NABPAPUZBYQPBPMACASPTKN	CODED CLUES UNDER THE BRIDGE
Hill	[3 3] [7 5]	ETMIKGLC	TREASURE