Cipher Puzzle Game : Decipher Dash

Mahfuza Naima, Annebelle Phanor & Tamica Sylvester
Mathematics and Computer Science Department

ABSTRACT

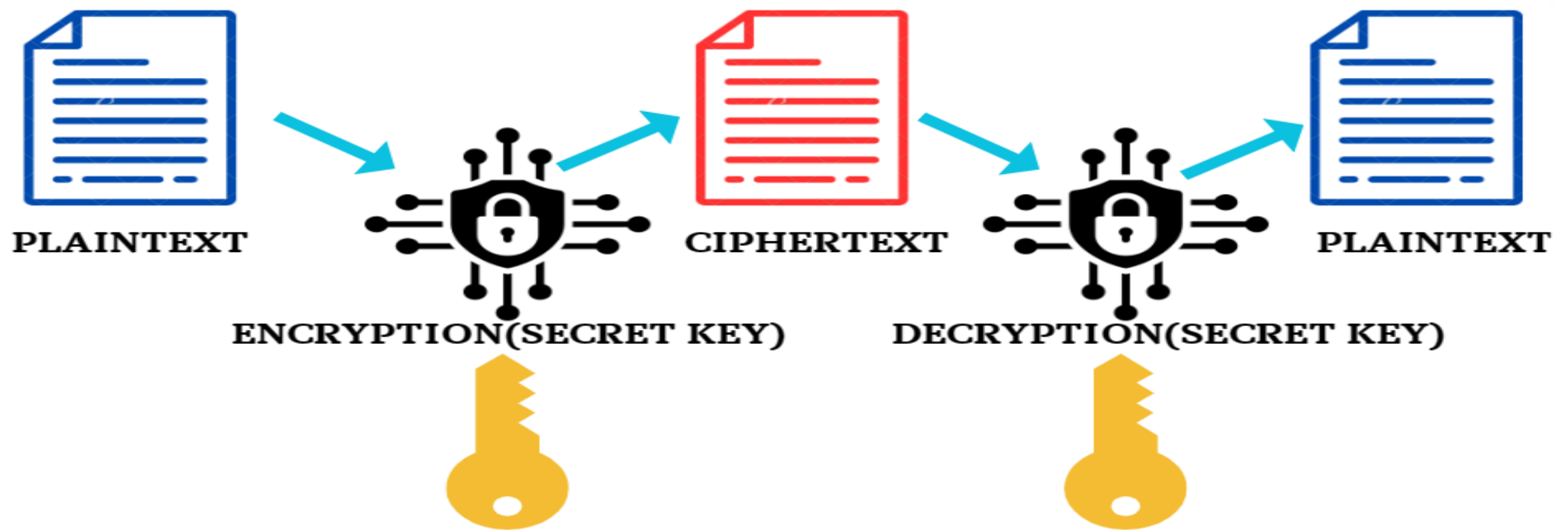
Cryptography acts like a secret code language, ensuring that data stays safe during transmission and storage, only readable by those meant to access it. Through techniques like message scrambling and specialized key unlocking, cryptography shields sensitive information such as bank details, passwords, and messages from prying eyes. While classical ciphers such as Caesar and Vigenère rely on simple substitution or transposition methods, modern ciphers like AES and RSA employ complex mathematical algorithms and keys to bolster security in today's digital landscape. This project aims to shine a light on cipher algorithms by crafting manual puzzle games, serving as a fun and educational tool to delve into the realms of network security and cryptography. By exploring how some ciphers work, participants will grasp cryptographic concepts while uncovering the strengths and limitations of each method.

OBJECTIVES

- Develop a multi-level puzzle game that tests players' ability to use traditional ciphers to decrypt texts.
- Offer an engaging educational program that examines the benefits, drawbacks, and mechanisms of several traditional ciphers.
- Encourage players' knowledge and comprehension of concepts related to network security and cryptography.

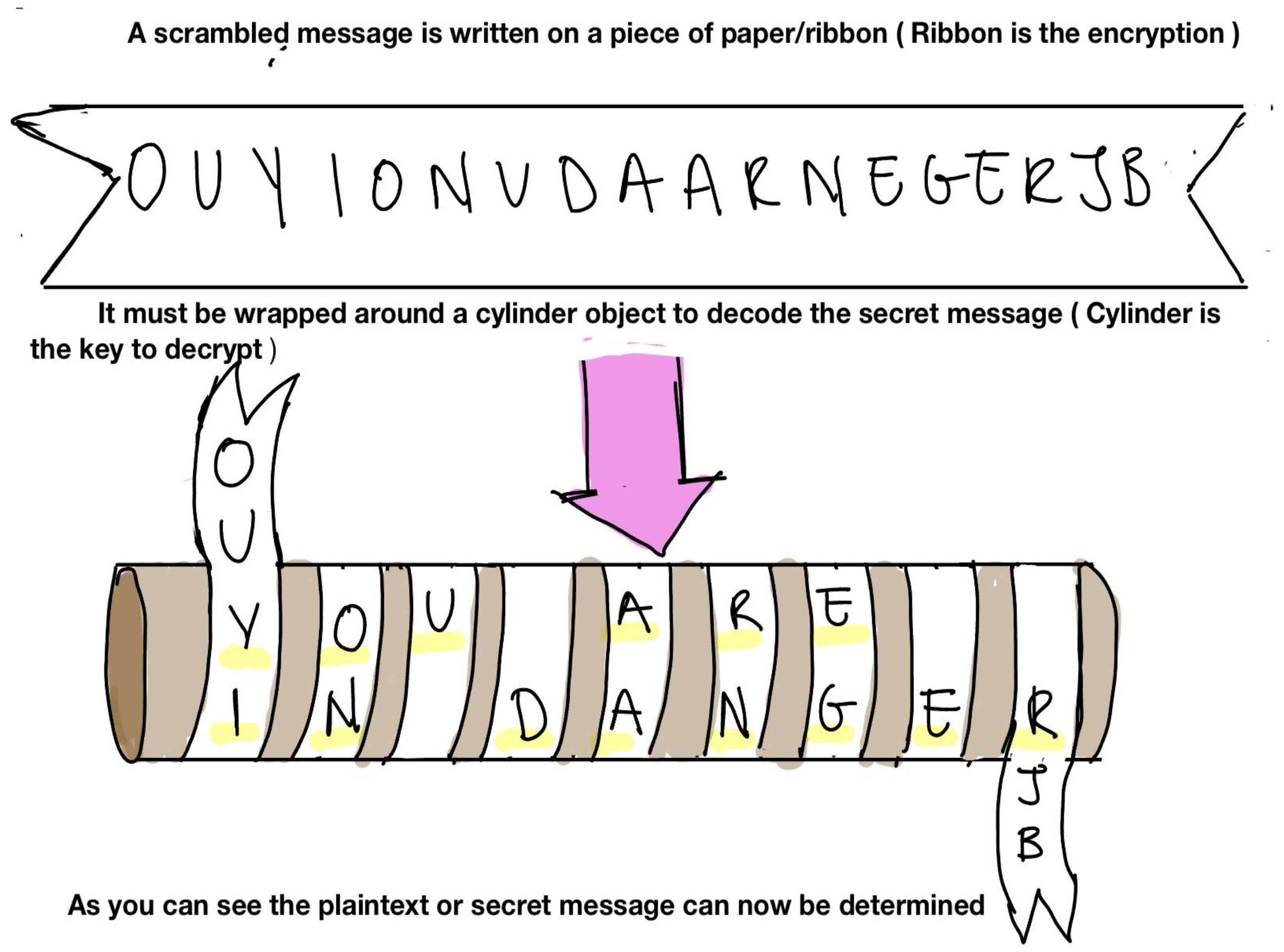
INTRODUCTION

Greetings! Cryptography is the art of encoding information to keep it secret. From ancient methods like Caesar's cipher to modern techniques like AES and RSA, this project explores a fun puzzle game that teaches different ciphers. Join us to learn traditional and modern encryption methods like of Vigenere, Scytale, Playfair, Affine, Book and Pig Pen ciphers. Get ready to crack codes and learn how to secure data!



CIPHER PUZZLE GAMES

Vigenere & Scytale

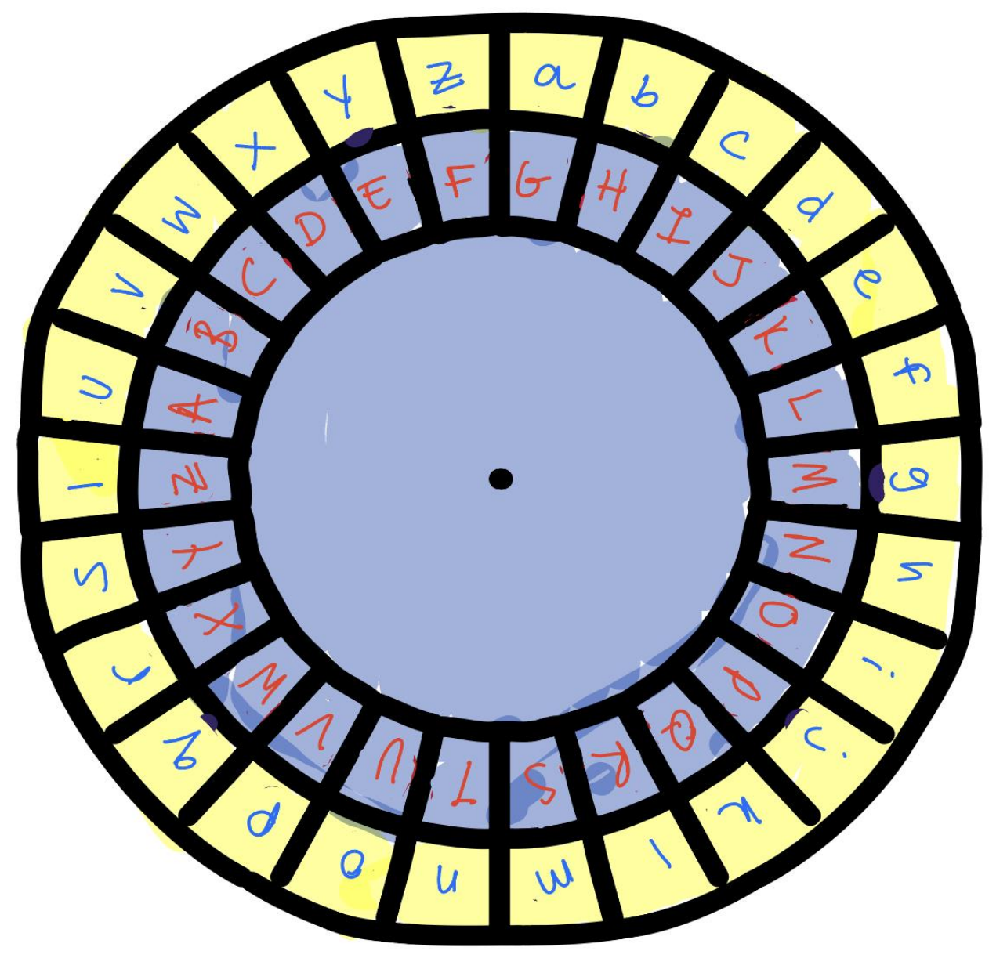


A scrambled message is written on a piece of paper/ribbon (Ribbon is the encryption)

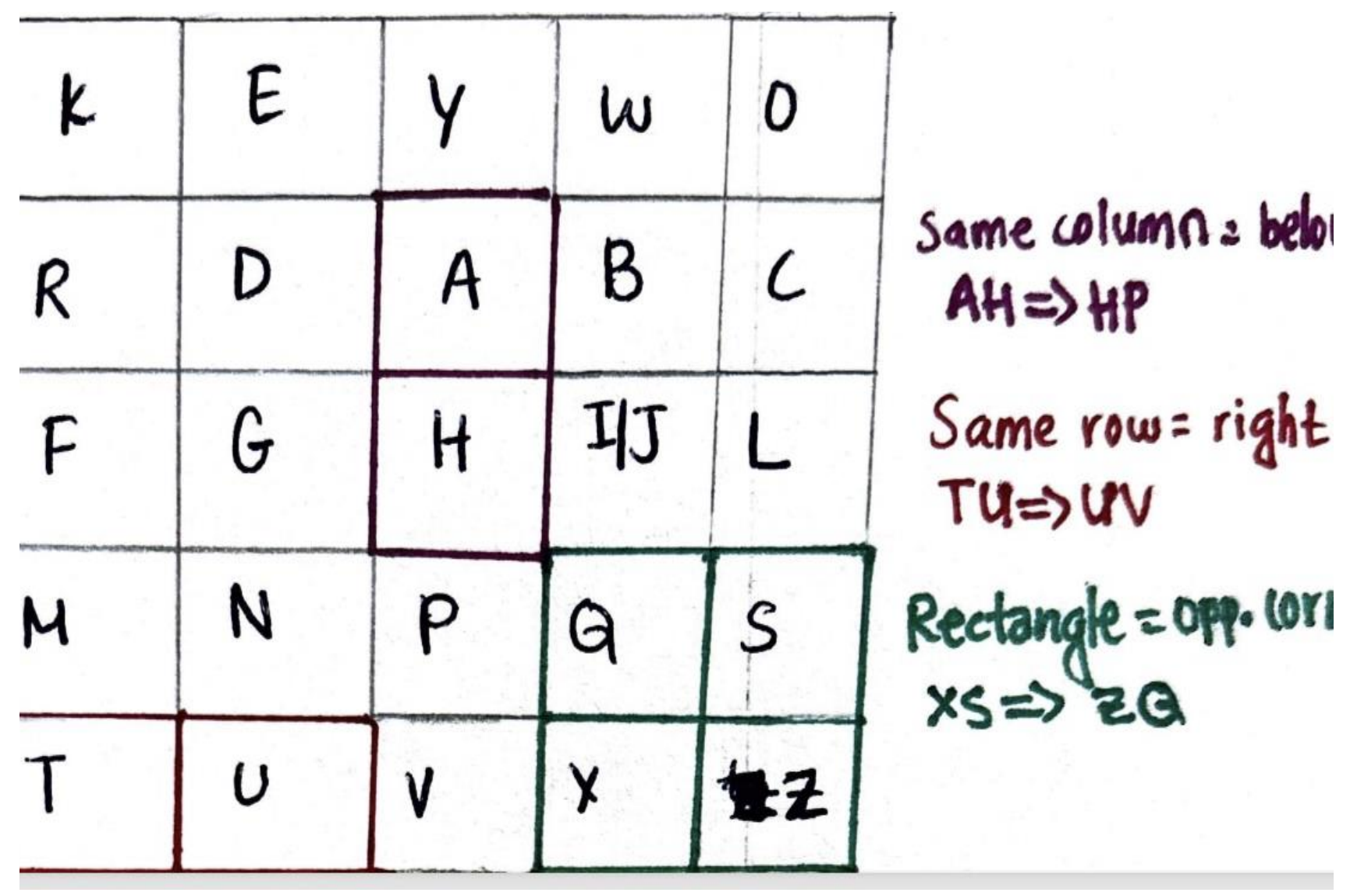
It must be wrapped around a cylinder object to decode the secret message (Cylinder is the key to decrypt)

As you can see the plaintext or secret message can now be determined

Envision a circle surround by every letter in the alphabet. A letter from the keyword should correspond with each letter in your message. Locate the message letter on the circle to begin encrypting. The wheel must be spin to encrypt/decrypt letters.



Playfair & Affine

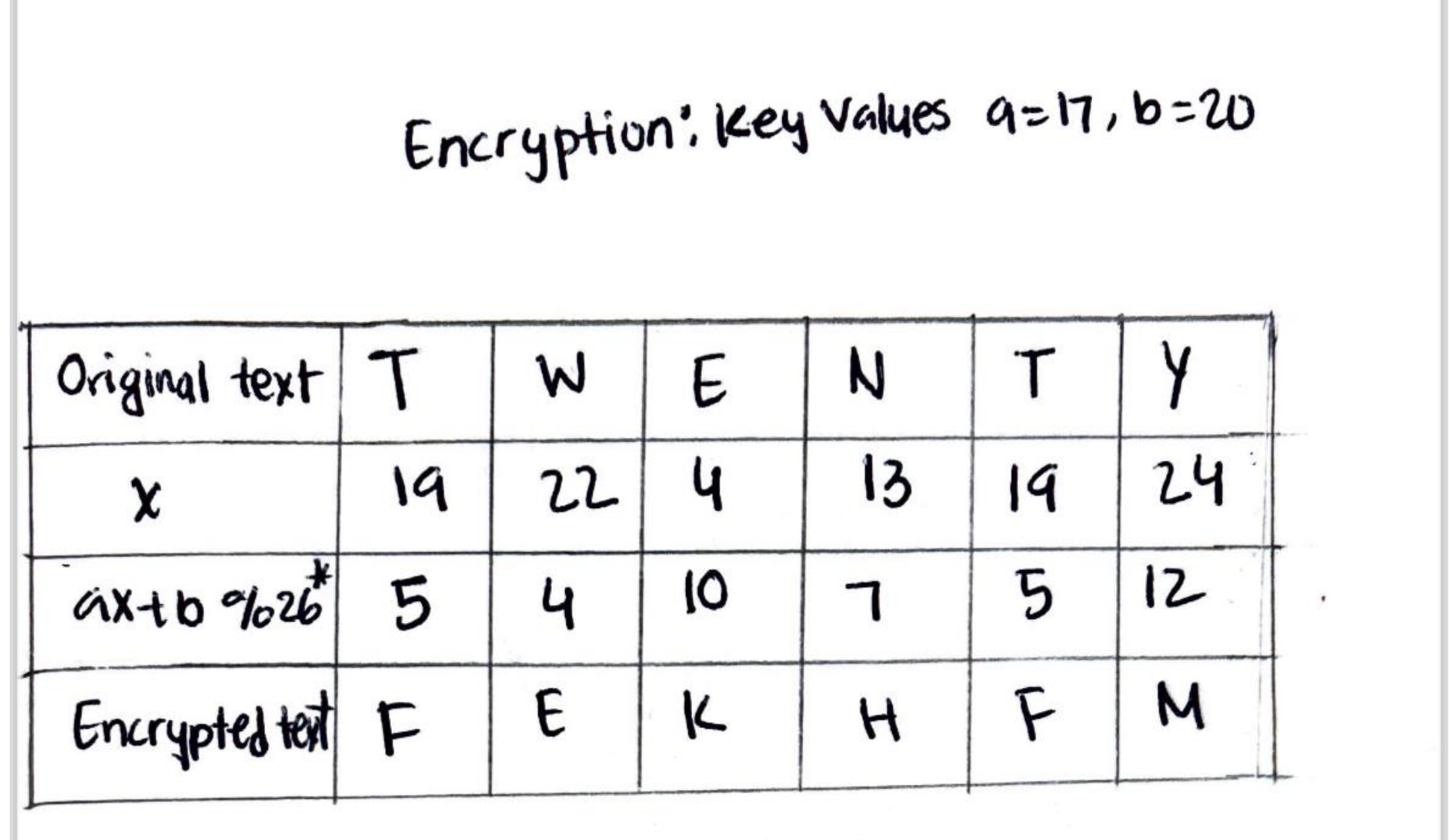


K	E	Y	W	O
R	D	A	B	C
F	G	H	I/J	L
M	N	P	Q	S
T	U	V	X	Z

Same column = below
AH => HP

Same row = right
TU => UV

Rectangle = opp. cor
XS => ZQ



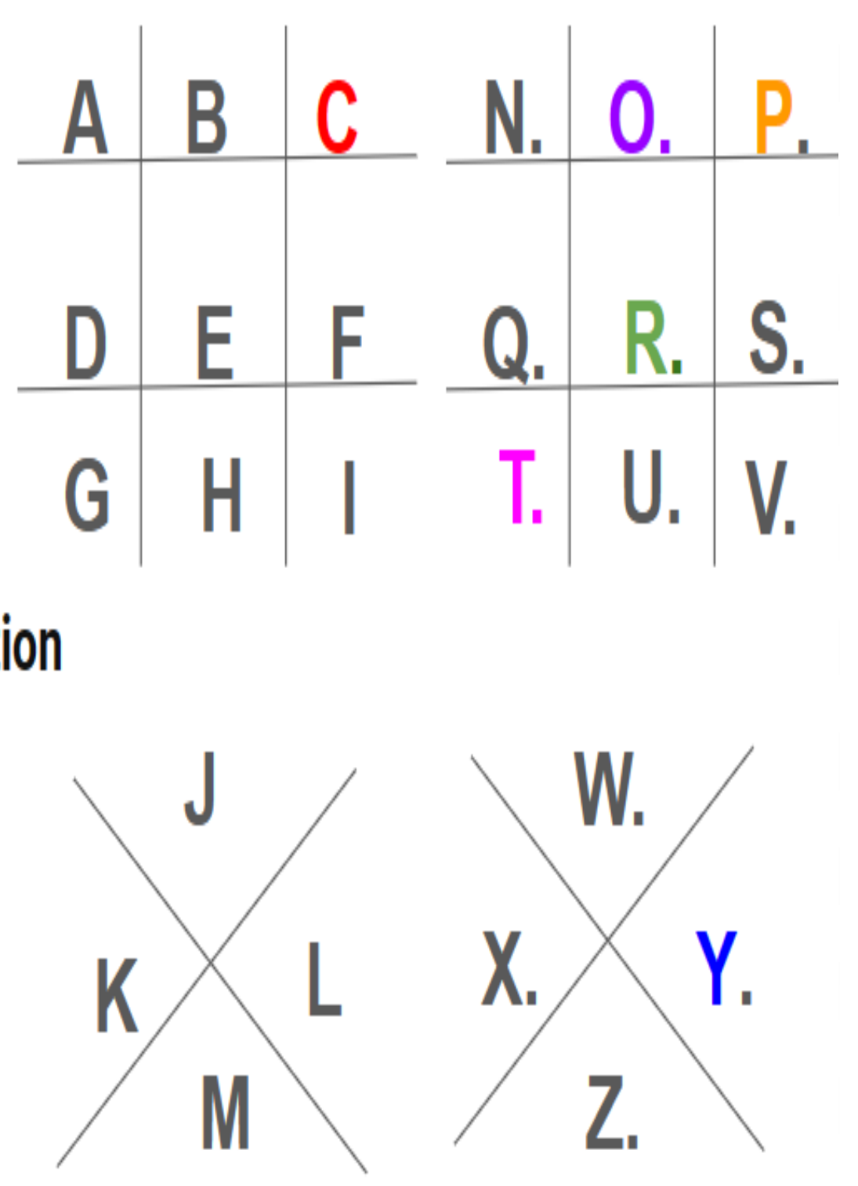
Encryption: Key Values a=17, b=20

Original text	T	W	E	N	T	Y
x	19	22	4	13	19	24
ax+b %26*	5	4	10	7	5	12
Encrypted text	F	E	K	H	F	M

Book & Pig Pen

How to Create a Pigpen Cipher

- Draw geometrical figures (2 tic-tac-toe and 2 X-shaped figures)
- Fill in the alphabet
- To encrypt a message, replace each letter with the symbol in the corresponding section of the Pigpen Cipher.



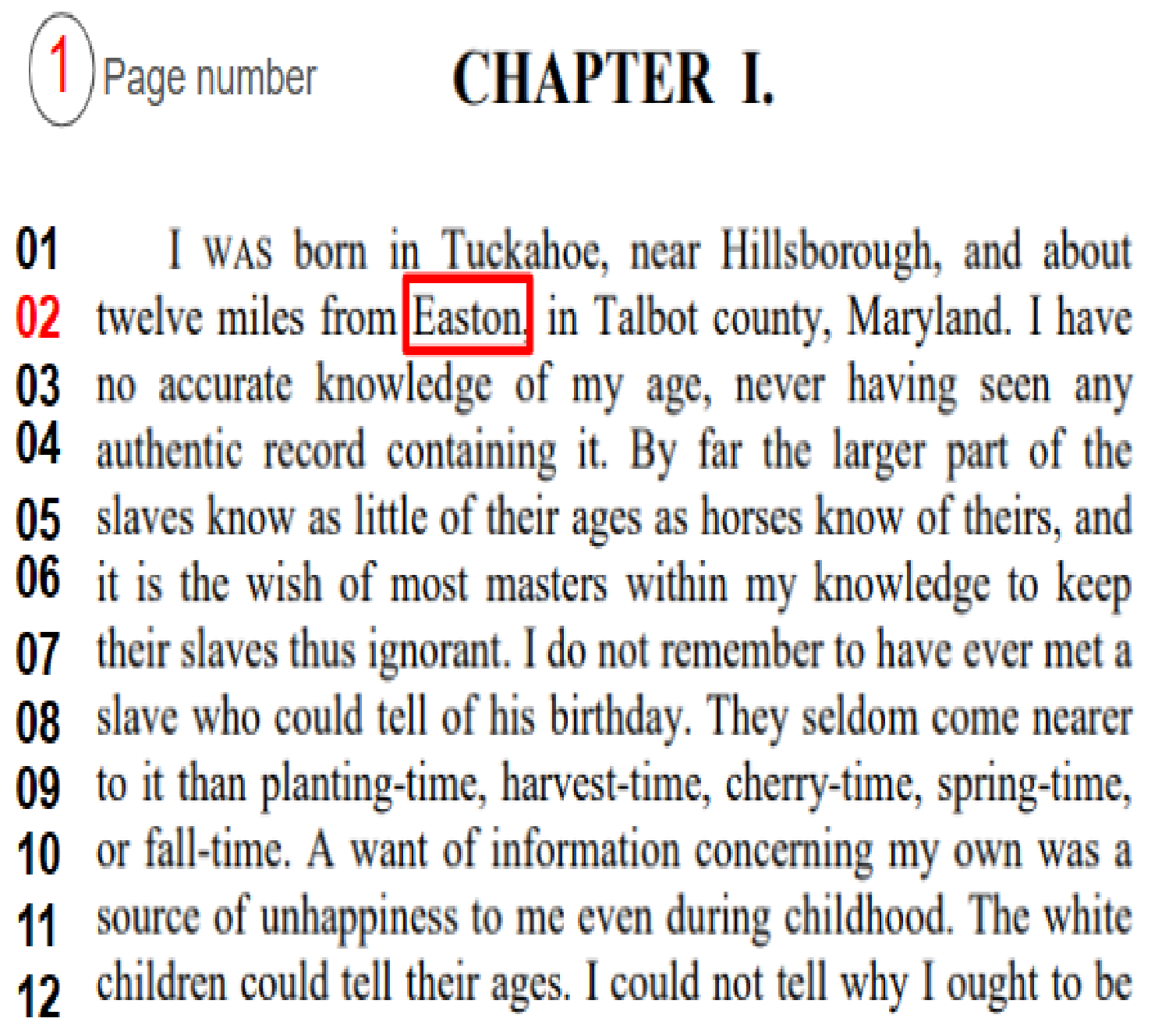
Plaintext: CRYPTO

Ciphertext:

Book Cipher

- Choose a word that you want to encrypt in the book
  - Chosen word: “Easton”
- Write the page number , page line and word position of your chosen word

“Easton”: 01 02 04



① Page number

CHAPTER I.

01 I WAS born in Tuckahoe, near Hillsborough, and about
02 twelve miles from Easton, in Talbot county, Maryland. I have
03 no accurate knowledge of my age, never having seen any
04 authentic record containing it. By far the larger part of the
05 slaves know as little of their ages as horses know of theirs, and
06 it is the wish of most masters within my knowledge to keep
07 their slaves thus ignorant. I do not remember to have ever met a
08 slave who could tell of his birthday. They seldom come nearer
09 to it than planting-time, harvest-time, cherry-time, spring-time,
10 or fall-time. A want of information concerning my own was a
11 source of unhappiness to me even during childhood. The white
12 children could tell their ages. I could not tell why I ought to be

Do the children remember my birthday

010706 010407 011201 010708 010609 010807 (Decrypt this!!!)

CONCLUSIONS

In conclusion, creating the decipher dash puzzle games required careful consideration of how to balance difficulty and create complex levels. However, the advantages were clear in that they helped players better understand network security concepts and conventional ciphers. We discovered the value of user participation and unambiguous instructional design during the process. For an even more engaging experience, we hope to enhance the level progression and add a wider range of cipher types the next time.

REFERENCES

- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.
- GeeksForGeeks. (n.d.). Retrieved April 12, 2024, from https://www.geeksforgeeks.org

ACKNOWLEDGEMENTS & CONTACT

We would like to acknowledge our CS465 course instructor, Dr. Thitima Srivatanakul, for providing valuable instruction and informing us on the theory of ciphers.

Mahfuza.naima@yorkmail.cuny.edu
Annebelle.phanor@yorkmail.cuny.edu
Tamica.sylvester@yorkmail.cuny.edu