



Game-based Learning of Cryptographic Algorithms

Student: Gwyneth Ang Xin Yi

Supervisor: Dr Smitha K G

The screenshot shows the 'Cryptoy' web application. On the left, there is a 'Caesar Cipher' section with an explanation: 'The Caesar cipher is one of the earliest known and simplest ciphers. It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet.' It provides an example: 'For example, with a shift key of 1, A would become B, B would be replaced by C, and so on.' Below this are the formulas $E(x) = (x+k) \pmod{26}$ and $D(x) = (x-k) \pmod{26}$. A 'Caesar Cipher Warm Up' puzzle asks: 'Given that the ciphertext is TSFSFS and the key is 18, what is the plaintext?' The answer 'T S F S F S' is shown in green, and the user has entered 'B A N A N A' in the input boxes. A 'CHECK' button with a green checkmark is visible. Below this, another puzzle asks: 'Given that the ciphertext is NYLBY and the plaintext is PANDA, what is the key?'

The main interface is titled 'Decrypt the following ciphertexts!'. It features a 'Caesar Table' with a 'Key' slider set to 8. The table shows the mapping: Plaintext (A-Z) to Ciphertext (I-H, A-H). Below the table, the ciphertext 'Q C B T W R S B H W O Z W H M' is displayed. The user has entered 'C O N F I D E N T I A L I T Y' in the input boxes. A 'CHECK' button with a green checkmark is visible. Below this, a feedback message says: 'That's right! Do you know what Confidentiality is?' A text box contains the definition: 'Confidentiality prevents adversaries from reading private data.'

Project Objectives:

This project aims to produce a gamified web application (Cryptoy) that teaches users about cryptography. The main target audience is beginners to cryptography who may not necessarily have a background in Computer Science or Computer Engineering.

2 modes in Cryptoy:

“**Learning Phase**” helps users learn concepts while solving beginner level puzzles.

“**Mastery Phase**” lets users solve puzzles as a test of skills.

Gamification Framework (D6)

D6 FRAMEWORK IN CRYPTOY	
1. DEFINE OBJECTIVES	To educate people, through an enjoyable and engaging manner, on how encryption works and how it protects against cyberattacks.
2. DELINEATE TARGET BEHAVIOURS	Players feel enthusiastic about learning and are eager to exploring new concepts
3. DESCRIBE PLAYERS	Motivated by sense of accomplishment and empowerment
4. DEVISE ACTIVITY LOOPS	Feedback on learning progress
5. DO NOT FORGET THE FUN	Add in gaming elements guided by Octalysis Framework.
6. DEPLOY THE APPROPRIATE TOOLS	Build scalable web application using React.js.