IMITATION GAMES BASED ON CIPHER (CRYPTIC)

Salahuddin Alayub Faizal[1], Ahmad Rawiyani Razim Redzuan[2] and Md Rosli Md Daud[3*]

Department of Mathematics, Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, 40450 Shah Alam, Selangor

[1]2019268694@student.uitm.edu.my, [2]2019230242@student.uitm.edu.my, [3*]roslidaud@uitm.edu.my

(indicates the corresponding author)*

ABSTRACT

If we look at the point of view of internet users in Malaysia, many of them are not aware to cyber security so that some of them are deceived and become victims of cybercrime. Therefore, we need to train them to be more vigilant in this issue starting with the basics. Ciphers are the foundation of cyber security. But unfortunately, it may be a bit outdated and difficult to understand. Therefore, how do we get people to interested in learning this cipher? In learning mathematics, we need focus to understand the methods and concepts used. It is the same with learning ciphers. So, the most appropriate method to use is to apply a simple cipher that uses only one key to encrypt or decrypt as a game. We are using the Unity engine to create role play games (RPG) or downtown where players must solve cipher puzzles in each village. There are two villages, the Substitution village, and the Transposition village, which are named from cipher applied into the village. By making a challenging video game indirectly people will be interested to try and focus to solve the game and accidentally they will gain knowledge about cipher without learning in class. Once they understand the cipher then they will more easily understand the importance of cyber security education.

Keywords*: Cipher, CRYPTIC, Substitution and Transposition.*

Received for review: 08-09-2022; Accepted: 22-09-2022; Published: 01-11-2022

1. Introduction

1.1 Background of The Study

Cryptology is the study of data transmission and storage in a safe and typically secret manner. Cryptography and cryptanalysis are also included (Eric, 2017). The mathematics that supports cryptography and cryptanalysis, such as number theory and the use of equations and algorithms, is known as cryptology. Because cryptanalysis principles are very specialized and complex, this presentation will focus on some of the essential mathematical concepts underlying cryptography, as well as recent applications. To be safe for storage or transmission, data must be altered in such a way that an unauthorized individual would find it impossible to decipher its real meaning. To do this, security systems and software employ mathematical equations that are extremely difficult to solve unless requirements are satisfied. The difficulty of solving a particular equation is referred to as its intractability. These equations are the foundation of cryptography.
Cryptography is used to secure transactions and communications, to safeguard personally identifiable information (PII) and other private data, to establish identity, to prevent document tampering, and to establish trust between servers. Cryptography is a critical technology that corporations utilize to safeguard their most important assets or data. Data refers to critical information in the form of personally identifiable information (PII) about consumers, employee PII, intellectual property, business strategy, and any other private information. Since a consequence, cryptography is critical infrastructure, as sensitive data security is becoming more dependent on cryptographic solutions. Weak or obfuscated cryptography may expose critical infrastructure. The public's preoccupation with disclosed data results in brand erosion. Enterprises must pay particular attention to how cryptography is implemented and maintained throughout the organization in today's reality.

Cryptography offers a variety of encoding strategies for establishing security when interacting on a public network. The term cryptography comes from a Latin word that means "hidden writing." A simple example of cryptography is when a sender sends a message that is originally in plaintext. The message is encrypted and turned into ciphertext before transmission across the network. When this communication arrives at the receiver's end, it is decrypted and again into plaintext.

There are several classifications for cryptographic algorithms. Symmetric cryptography, asymmetric cryptography, and hashing are all subsets of cryptography. The Private key use the same key (secret key) for both encryption and decryption. Because the sole key used to decrypt the encrypted content is duplicated or shared with another person, this key is symmetric. It outperforms public key cryptography in terms of efficiency. Two keys are utilized in public keys. One key is used to encrypt data, while another is used to decode data. One key (public key) is used to encrypt plain text and convert it to ciphertext, while the recipient uses a different key (private key) to decrypt the ciphertext and read the message.

1.2 Problem Statement

Many internet users in Malaysia lack awareness, are naive, and apathetic to the critical nature of cyber security until they are duped and become victims of cybercrime (Bernama, 2021). According to Datuk Dr. Amirudin Abdul Wahab, Chief Executive Officer of Cybersecurity Malaysia, data breaches affecting enterprises can occur when businesses show a lack of concern and a negligent attitude toward the safety and security of their data (Bernama, 2019). Superiors must instil awareness in their employees, and superiors must give education and training to all staff members, including themselves about cyber security. Before this situation worsens, we must educate Malaysians about cyber security from an early age. Basically, the cipher is the foundation of cyber security. But unfortunately, this cipher may be a bit outdated and difficult to understand. Also, many Malaysians are less interested in educational game. The most common complaints relating to why educational boring are low playability and low quality, simplified structure as well as unpleasant graphics. Teenagers nowadays playing games without getting any knowledge. we must educate our students to play games and gain something that useful in their life. Basically, we create our own cryptography games and more specifically about cipher, but unfortunately, this cipher may be a bit outdated and difficult to understand.

1.3 Objective:

This study suggests several research objectives to be attained as follows:

1. To introduce the concept of cipher in the mathematics of cryptography and, therefore, grow the talent pool into the cybersecurity industry needed for the 21st century

2. To create computer games to let the student leaning interactively. the games are:
    a) basic concept of cipher and,
    b) in puzzle and RPG mode.

3. To learn mathematical ideas behind cryptographic through games.

1.4 Significance of The Project

The reason for using teenagers as specimens for this project is that they learn IT expertise faster than adults. If we look at cyber-crime cases, many of the victims involved are between 18 to 25 years old. This is because they are less attentive with their personal data.

Common methods used by hackers to control a computer or network are viruses, worms, spyware, Trojans, and ransomware. Viruses and computer worms can replicate and damage files or systems, while spyware and Trojans are often used for the collection of suspicious data.

Among the cyber security threats is phishing. Phishing is a tactic of sending fake emails that resemble emails from real sources. The purpose is to steal sensitive data such as credit card numbers and login information. Next to ransomware, ransomware is software designed to extort money by restricting user access to files or computer systems until the ransom is paid. However, the payment made does not guarantee that the file or system will be returned or restored. Lastly malware, malware is software designed to gain illegal access or cause damage to a computer.

Therefore, the most effective way to curb this problem is by making early exposure to teenagers to cyber security. Before they understand cyber security, they need to learn ciphers first. However, cipher is something that is quite complicated and difficult to understand. So, to attract teenagers to learn cipher is to make a challenging video game indirectly they will be interested to try and accidentally gain knowledge about cipher. Once they understand the cipher then they will more easily understand the importance of cyber security education.

1.5 Scope And Limitation Through The Study

Throughout this study, there are a few limitations that can be identified. The first limitation is the limitation of the time for the research such as where it is impossible to collect accurate data. Next, this study involves a small number of people and cannot be generalized to all teenagers in Malaysian.

2. Methodology and Implementation

2.1 Game Development Life Cycle:

The game is the one kind of software of program with a goal to provide entertainment. When we plan to start and developing the any games, simply adopting the software development life cycle is not enough for any game developer, as the developer face several challenges during the making any game development life cycle (Sudhir, 2018).

To overcome the problem of every game developer, a new specific approach will arrive it's known as GDLC (Game Development Life Cycle)

In order to achieve the objectives of this research, methodology can illustrate as follow:

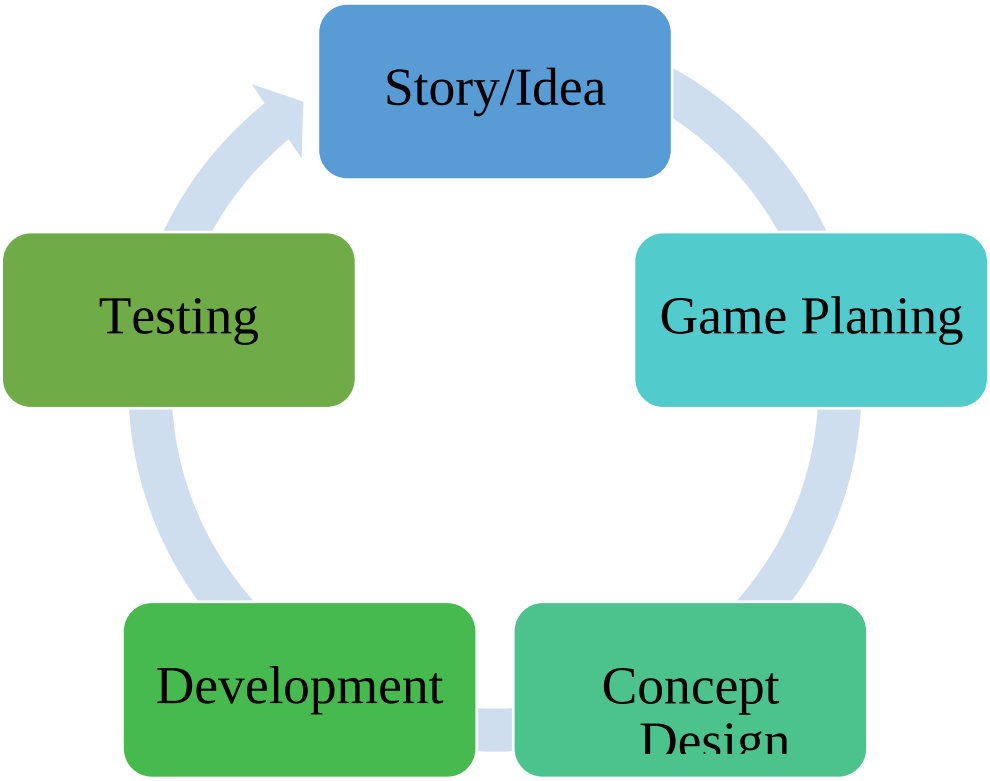

Figure 2: Game Development Life Cycle

2.2 Synopsis of The Game

CRYPTIC is not like other educational games. This game is an RPG (Role Play Game) Top Down where the player can explore and free to move in the game. At the same time, this game also can be classified as puzzle game because there have some quizzes in game. This game has no level because its open world game. There are four points in the game, first starting point where the player respawns at beginning of the game at forest and the rest points are at different villages (Substitution Village and Transposition Village) where substitution and transposition cipher puzzle located. At the beginning of the game, the player would be put in the forest, and they will be guided to go to the substitution village from the instructor. The instructor will explain about cryptology and basic of cyber security. All quizzes in the village have hint in its where players need to find or think about it.

2.3 Concept and Design

Cryptic is a breaking code game, where the player aims to break as many as possible, that required solid cryptographic knowledge. Each village has display different types of cipher, Substitution cipher and Transposition cipher. When the message is decoded, the player considers pass for that stage and can proceed to next village.

For designing this game, firstly, we find the best design for the games, for our case we choose design from Unity store and itch.io. Most of our game design is from Mystic woods by Games.

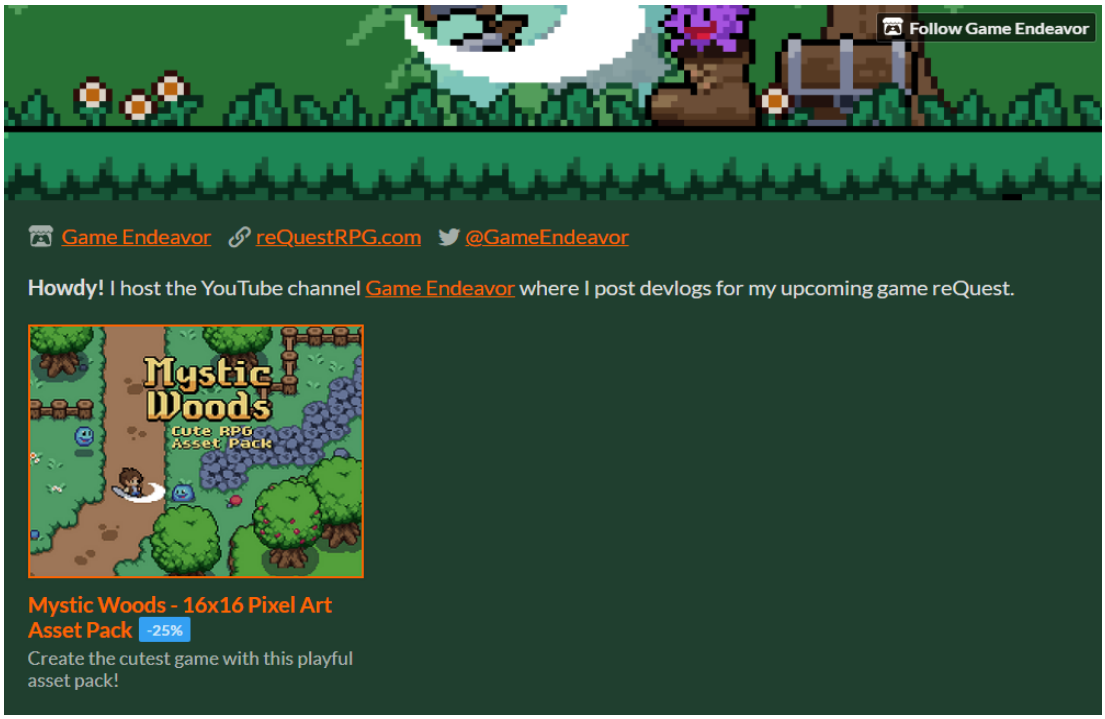

Figure 3: Game Design

At the beginning of the game player will spawning at forest. There will have instructor to guide player to the Substitution Village and Transposition Village. The instructor will explain about cryptology and basic of cyber security before they go to villages to solve cipher puzzle.

Figure 4: Beginning of The Games

In Substitution Village, player will face Substitution cipher in the village. There will appear on village community notice board about how Substitution cipher work and how to solve it. Player can also interact with villagers to find the key to solve this cipher. Below shows the formula of encryption and decryption in the board:

Figure 5: Substitution Village Bord Input

In Transposition Village, player will face transposition cipher in the village. There will appear on village community notice board about how transposition cipher work and how to solve it. Player can also interact with villagers to find the key to solve this cipher. Before player start to enter instructor will explain about Below shows the formula of encryption and decryption in the board:

Plaintext: MAKAN

1	2	3
M	A	K
A	N	x

2	3	1
A	K	M
N	x	A

Key: 231
Ciphertext: ANKXMA

Figure 6: Transposition Village Bord Input

2.4 Development

To develop this game, we choose to use Unity to build this game. This game engine can make the process of creating a game much easier and enable developers to reuse lots of functionality. It also takes care of rendering for 2D and 3D Graphics, physics and collision detection, sound, scripting and much more. With Unity, we can develop projects for many environments, including PC, PlayStation, Xbox, Nintendo Switch, iOS, and Android. Unity is used a lot in the gaming industry as it provides flexibility to work between different platforms. However, more experienced developers generally prefer the C# language.

Example of coding we use is to move the character and to make camera follow the character when character move.

This is player controller. The function of this coding to make sure character can be move by using input like keyboard, gamepad, joystick, etc. For player movement we are using C# coding like below:

```
void Update()
  {
    movement.x = Input.GetAxis("Horizontal");
    movement.y = Input.GetAxis("Vertical");
  }

  void FixedUpdate()
```

Figure 7: Coding for Player Movement

After that we have function of camera controller. Where this coding is for camera follow the character whenever character move and character will be the middle of the screen all the time. We are also setting the ratio of the game at 16:9 Aspect. For this function we are using C# coding for camera controller like below:

```
public Transform target;
void Update()
  {
    transform.position = new Vector3(target.transform.position.x, target.transform.position.y,
transform.position.z);
  }
```

Figure 8: Coding for Camera follow Player

2.5 Testing

The reason program needs to be tested before release is to expect the system to perform correctly using a given set of test cases that reflect the system's expected use. The test cases are designed to expose defects. The test cases in defect testing can be deliberately obscure and need not reflect how the system is normally used. For this game, developer is going to do a development testing, where the system is tested during development to discover bugs and defects.

In development testing there are some other types of tests (unit testing, integration testing, system testing and acceptance testing). Unit testing, where individual program units or object classes are tested. Unit testing should focus on testing the functionality of objects or methods. Component testing, where several individual units are integrated to create composite components. Component testing should focus on testing component interfaces. System testing, where some or all the components in a system are integrated and the system is tested. System testing should focus on testing component interactions.

Next is User Acceptance Testing, where users or potential users of a system test the system in their own environment. User Acceptance Testing is a process to check the system accepts the requirements of a user or not. It's performed at a time when the system used by actual users. User Acceptance Testing process related to another analogy such as to manufacture pens - While production of a ballpoint pen, the cap, the body, the tail, the clip, the ink cartridge, with the help of things mentioned above, a full ballpoint pen manufactured after that single pen produced with a combination of every single item.

For this game development, we are going to use system testing and user testing because the game needs to complete first so developer can find bug easily and user testing. Each component specified above tested to ensure that each component will make the pen in a working condition. When a complete pen is integrated, System Testing is performed. Once a System Testing is over, perform Acceptance testing to confirm that each ball pen is in working condition and ready to use for customers.

In the questionnaire there some questions open ended where player should elaborate the reason why they like or dislike the game and researcher also want to know are they learning something in this game, and they need state their reason why they said like that. Because of the question is open ended question, the feedback will separate in two categories which are like and dislike the "CRYPTIC" game. The reason why researcher use open ended question is to know why respondents like to play the game and are they learning something when playing this game.

3. Results and Discussion

3.1 Introduction

This chapter discusses the findings and analysis from the feedback. In this chapter, results from data collection are shown.

3.2 Background Information (Section A)

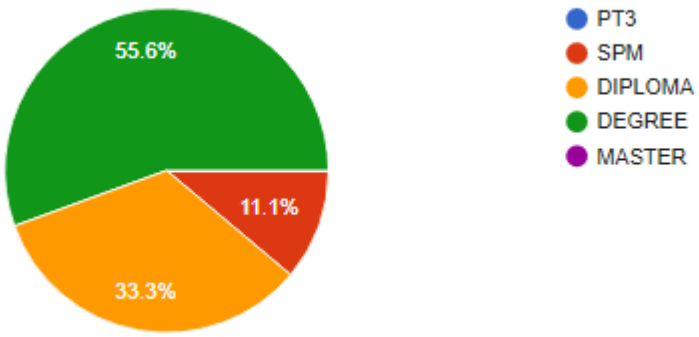

Figure 9: Education Level

In this study, the whole Figure represents a value of 18 respondents. As we can see, the pie is divided into 5 sector which is PMR, SPM, DIPLOMA, DEGREE, MASTER but we only got feedback from degree, diploma, and SPM students. We can say that majority of the respondent who play the game is a degree student. The pie chart shows that 55.6% of students are studying at bachelor's degree level. In general, we are exciting to hear interesting feedback from them. Next, we have 33.3% of diploma student who are willing to play our game and give feedback. In the pie chart we can see the orange colour is the percentage of diploma students. Lastly, we have 11.1% of SPM student. This show that SPM student and below are less interested to try play our game.

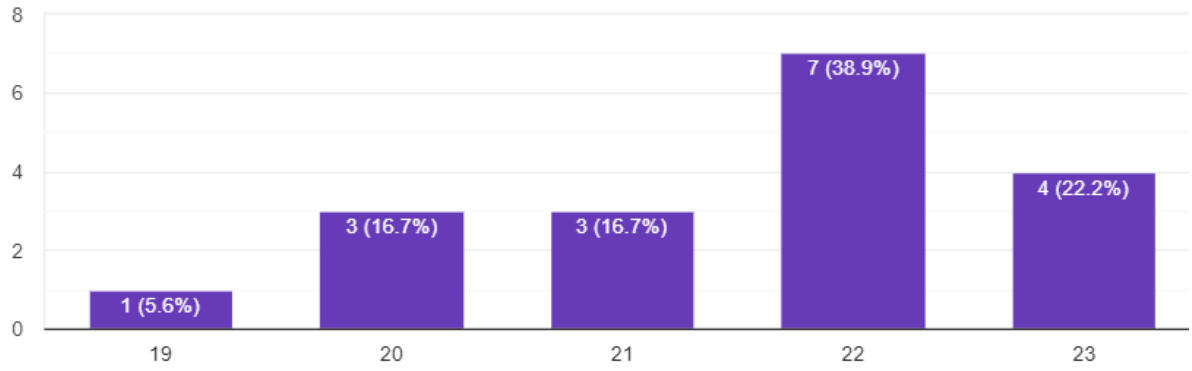

Figure 10: Respondents Age

In this part, age distribution of the participants is shown in Figure 10. The percentage of respondents in each age was as follows: 19(5.6%); 20(16.7%); 21(16.7%); 22(38.9%) and 23(22.2%). It shows that respondents aged 22 are significantly give feedback.

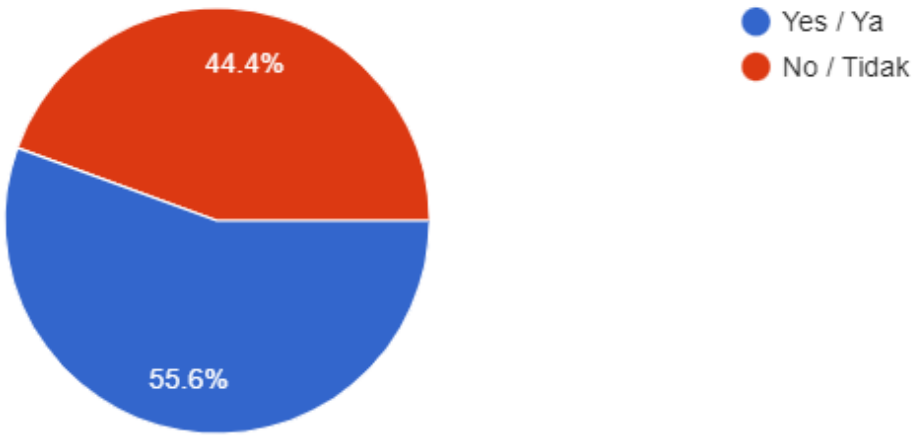

Figure 11: Mathematics or Non-Mathematics Student

Figure 11 represents a value of 18 respondents. The pie chart is divided into 2 part which is Yes and No. As we can see that respondents who is mathematic students are more than non-mathematics students. From the pie chart shows that 55.6% of the respondent are mathematics students. The rest is 44.4 respondent answer no which they are not major in mathematics. This shows that mathematics students have more interested to test playing these educational games.

3.3 Pre-Playing "CRYPTIC" (Section B)

In this study, we want to know about respondent knowledge before they play CRYPTIC.

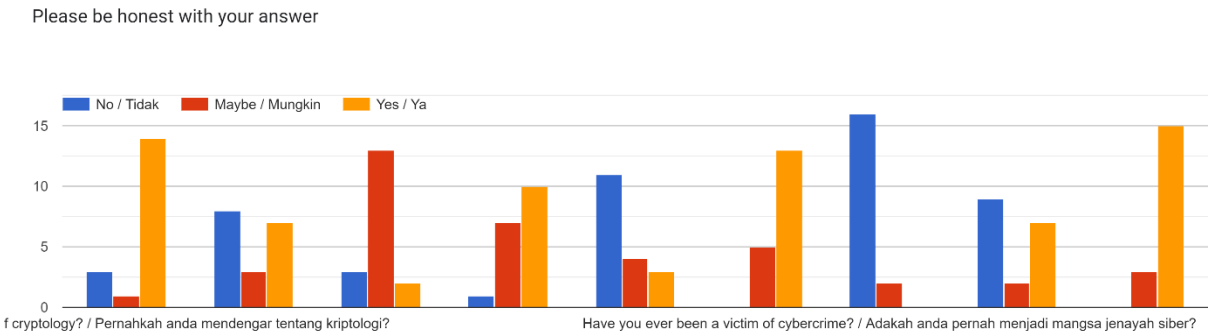

Figure 12: Pre-playing CRYPTIC Knowledge and Experience

For the question "Have you ever heard about cryptology?", most of the respondents are known and ever heard of cryptology. As we can see, 14 of the respondents choose yes. We assume that because cryptology is very famous nowadays even though they do not delve into cryptology in depth. Next the numbers of respondents who know nothing and never heard about cryptology is 3. The blue bar shows that only minor respondents who doesn't have knowledge about cryptology. Lastly, we only have 1 respondent who answer maybe.

For the question "Have you ever heard of cipher before?", the bar chart is quite balance because all respondent is doubt about cipher. The blue bar that shows number of respondents who doesn't know and never heard of it is 8. That's prove majority of students didn't have the knowledge about cipher. Lastly, we have 3 respondent who think their know about cipher.

For the question "Are you interested in cyber security?", we put the question because cyber security is related with cipher. As we can see, among of all the respondents, many of them choose maybe for the answer. It is because they think cyber security is interesting, but they don't have enough knowledge to explore about it. The bar chart shows numbers which is 8 for maybe, 2 for yes and 3 for not interested at all.

For the question "Do you know about the importance of cyber security?", the bar chart shows that the highest is orange bar which is they know about the importance of cyber security. 10 out of 18 respondents click Yes while the respondents who maybe know about this is 7 and the remaining 1 respondents click no and doesn't know about importance of cyber security. As we can see, students nowadays are aware about cyber security.

For the question "Did you know that the basis of cyber security come from cryptology?", we can see clearly that most of the respondents doesn't know how deep cyber security and cryptology is relating. The blue bar in the chart shows that 11 students still have zero knowledge about basis of cyber security.

For the question "Are you aware to cybercrime happening in the country?", there are so many bad people use online platform to gain a money. This people we called it a scammer. From

the bar chart, we see 13 respondents are aware about cybercrime and the rest 5 respondents are think they know and aware about cybercrime that happen in our country.

For the question “Have you ever been a victim of cybercrime?”, majority of the respondents never been a victim of cybercrime. The bar chart shows the blue one is highest with number of 16. Then, only 2 respondents maybe been deceived by a scammer.

For the question “Has your contact ever been a victim of cybercrime?”, the bar chart shows that the highest is blue bar where most of the respondents answer no. that’s mean people surrounding them are aware about cybercrime. Meanwhile there are 7 of them who got a contact that have been a victim of cybercrime.

For the question “Do you like to learn something new?”, the reason why this question must be asking to respondents whether they like or not to learn something new because CRYPTIC is type of educational game. That’s mean the respondents will learn something after playing games. As we can see, majority of the respondents are excited to learn and experience our game. The bar chart shows the highest is Yes bar with amount of 15 while the remaining 3 is click on Maybe.

3.4 Post Playing CRYPTIC (Section C)

In this section, we collect data and feedback to know how their feel about cipher and what knowledge they gained after playing CRYPTIC Game.

3.4.1 Respondents Enjoyable Playing CRYPTIC Game

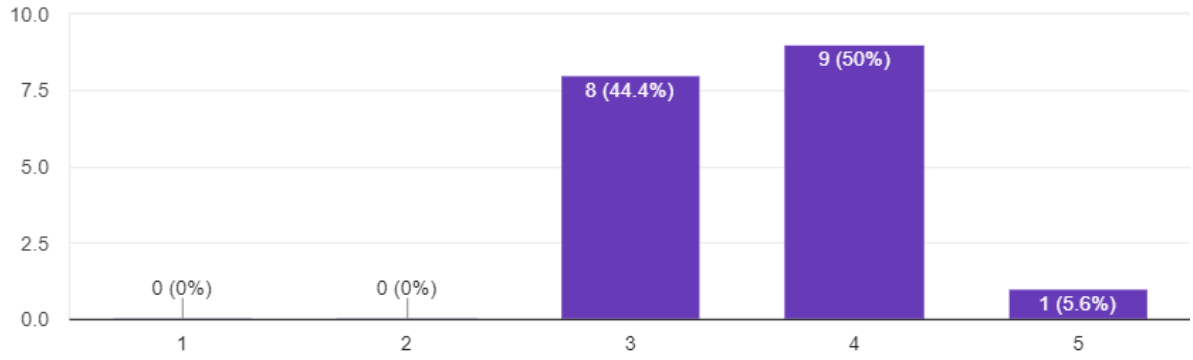

Figure 13: Enjoyable Level of Respondents Playing The CRYPTIC Game

In this section, we receive good feedback where all respondents choose normal, best, and very best. As we can see 44.4% respondent choose 3 which is normal, 50% choose 4 which is best and 5.6% choose 5 which is very best.

3.4.2 Respondent Performance

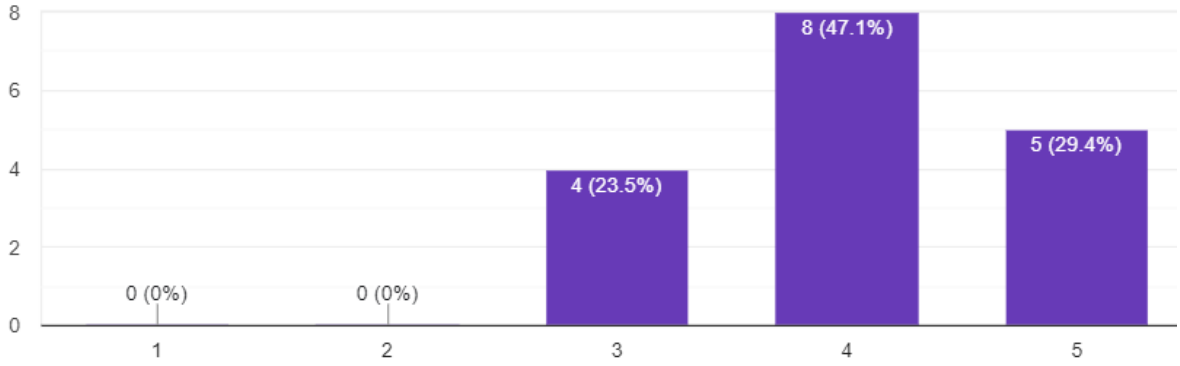

Figure 14: Respondent Performance

In this section, we create a simple game to make sure all the respondents can answer and finished it. The level of difficulty is amateur because some of the respondent maybe not familiar with cipher. As we can see in the bar chart, only 29.4% of respondent trying their best to solve the cipher puzzle. Then we have 47.1% choose Yes and 23.5% choose normal. It is shown that our game is easy and can play without no pressure.

3.4.3 Hardest Section in Game

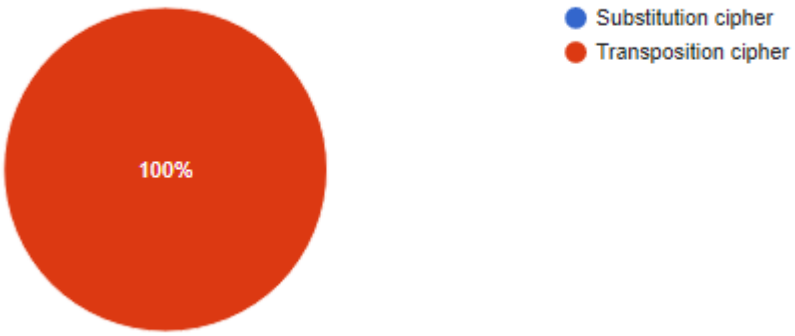

Figure 15: Hardest Village

In this section, the whole pie represents a value of 17 respondents. As we can see, the pie is divided into 2 sector which is Substitution cipher and Transposition cipher. From the pie chart, we can say clearly that all the respondent who play the game choose Transposition cipher for the most difficult. The pie chart show that 100% of respondents think Transposition cipher is the hardest.

3.4.4 Time Taken by Respondents to Solve Puzzle

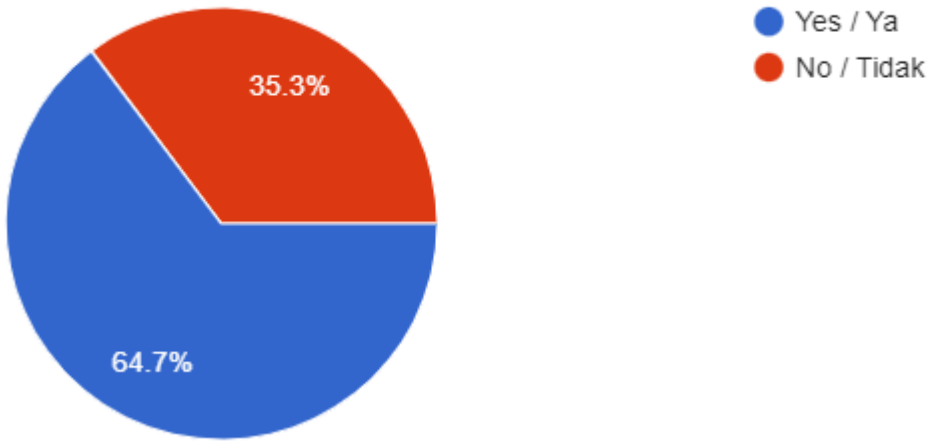

Figure 16: Time to Solve Puzzle

In this section, we want to know about time taken to solve the puzzle. The pie chart shows that 64.7% of respondent answer Yes. Its mean our game is quite challenging. Next only 35.3% of the respondent doesn't have problem to solve the puzzle in a short period of time.

3.4.5 CRYPTIC Feedback

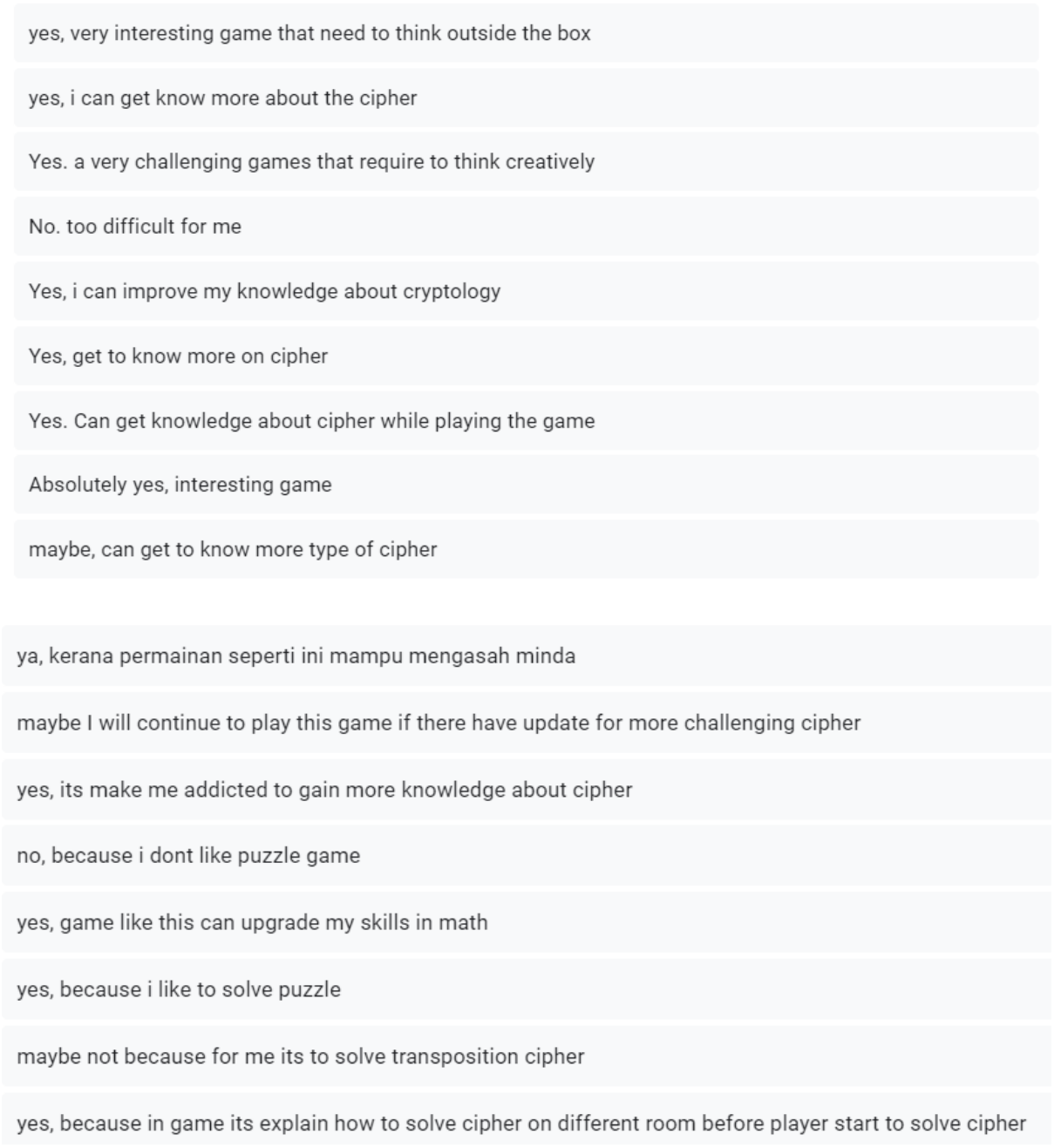

Figure 17: CRYPTIC Feedback from Player

In this section, we received good feedback which is most of them answer yes and want to play again. As we can see, they got interested in cipher after playing our CRYPTIC. Its shows that platform like video game can attract student to like about cipher.

3.4.6 Input Respondent Get from CRYPTIC

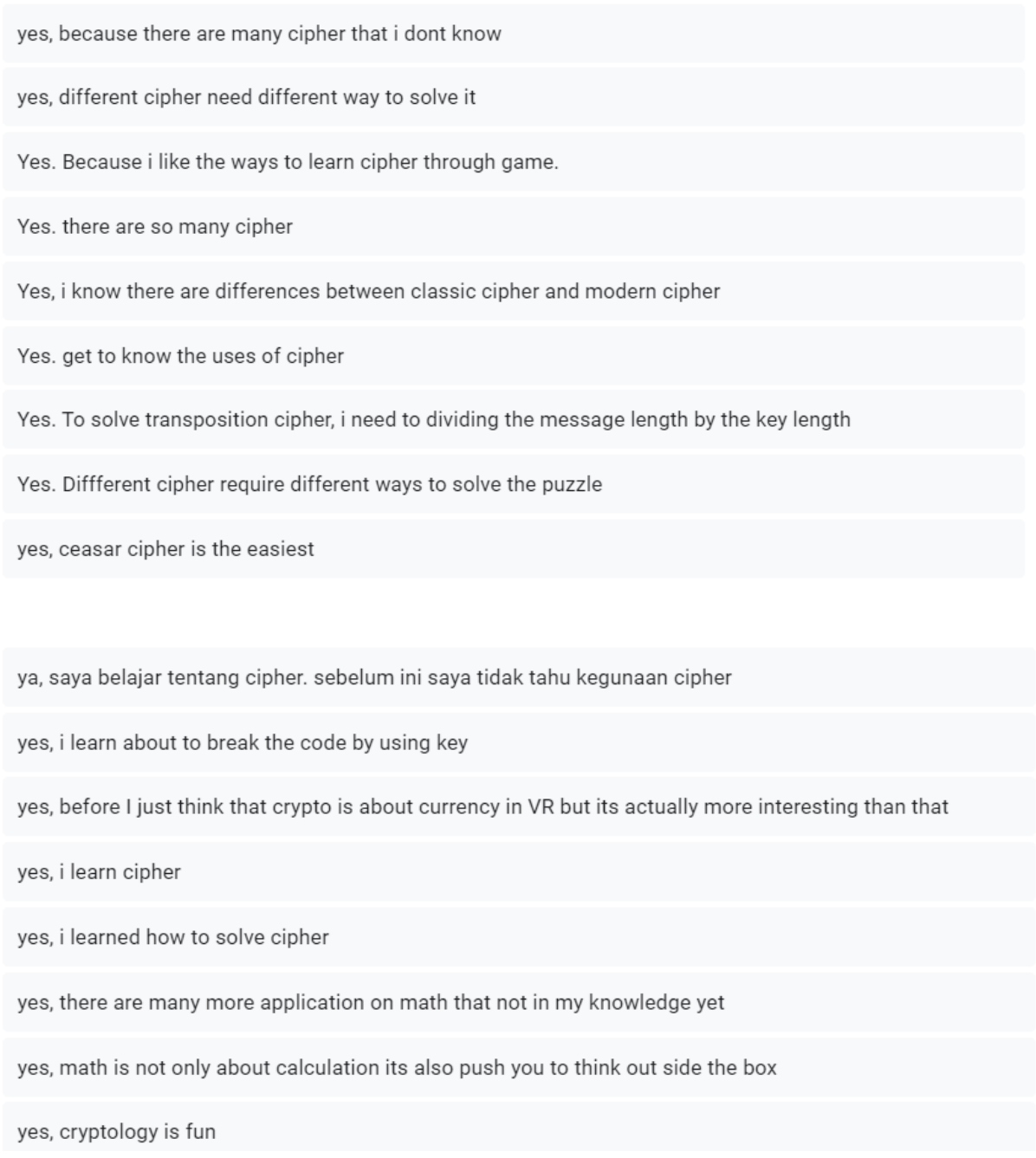

Figure 18: Input Player Get from Playing CRYPTIC

In this section, we asked about new things they learned and were able to use it in real life after playing the Cryptic game. We got a lot of positive responses. Most of the respondents just discover the exact meaning of cipher. We can see they managed to finish the game a get a good score.

4. Conclusion and Recommendations

This chapter summarizes the entire project and its achievement. It gives details on the success of every objective mentioned in Chapter 1. Other than discussing the final achievements of the study, it also discusses the limitations of the project. Lastly, there are recommendations given for future works that could be improved by other researchers.

4.1 Conclusion

In conclusion, the project succeeds to achieve all the objectives written. The first objective is to show the high-level mathematical ideas behind cryptographic games and the use in real life. The factors were identified during all the respondent finished the game even some of them take a much time to solve the cipher puzzle. In addition, they do well in Cryptic game and got interested to explore more on mathematical game.

The second objective is to introduce the concept of cipher in the mathematics of the cryptography and grow the talent pool to the cybersecurity industry. The data was collected from google form. The data before playing the games state that many of the respondent didn't know much about cipher and cyber security. In addition, platform like video game that will influence student to get know in detail about cipher and it uses in real life. Then, after playing the game, most of the respondent's state that there has learned something new like what is cipher, relationship between cipher and cyber security and the important of have cryptography knowledge in the 21st century. Its shows that all the respondents get the idea we put in the video game.

The third objective also has been successfully achieved. The objective is to create computer games to let the student learning interactively. In this IT era, we know that student nowadays like to play game. So, to make them to know details about cipher is by creating a video game. They can play the game while learning something new. Then, the data shows that we are achieve our target student to play and give feedback about Cryptic game.

4.2 Recommendations

There are several modifications that can be made from this study. This CRYPTIC game is in 2D so this game can probably be made in 3D. some respondents encouraged developers to increase the level of difficulty in the game and diversify the types of ciphers. Aside from classical cryptography, perhaps the developer could combine other cryptographic components such as RSA, Huffman code, and so on.

Acknowledgement

The authors would like to thank to Department of Mathematics Faculty of Computer and Mathematics Sciences, Universiti Teknologi MARA for supporting this project.

References

Adam, A. (2021, August 2). *Enigma | Definition, Machine, History, Alan Turing, & Facts | Britannica*. https://www.britannica.com/topic/Enigma-German-code-device

Ben, F. (2016, October 6). *Crack the Code! Make a Caesar Cipher - Scientific American*. https://www.scientificamerican.com/article/crack-the-code-make-a-caesar-cipher/

Bernama. (2019, October 24). *Isu kebocoran data membimbangkan: CyberSecurity - Sinar Harian*. https://www.sinarharian.com.my/article/53797/BERITA/Nasional/Isu-kebocoran-data-membimbangkan-CyberSecurity

Bernama. (2021, May 1). *Ramai pengguna internet tidak peduli kepentingan keselamatan siber - Cybersecurity Malaysia | Astro Awani*. https://www.astroawani.com/berita-malaysia/ramai-pengguna-internet-tidak-peduli-kepentingan-keselamatan-siber-cybersecurity-malaysia-295878

Collin, F. (2017, May 26). *cochranmath / Transposition Ciphers*. http://cochranmath.pbworks.com/w/page/118045167/Transposition%20Ciphers

Cryptography Definition & Meaning - Merriam-Webster. (n.d.). Retrieved August 15, 2022, from https://www.merriam-webster.com/dictionary/cryptography

Eric, G. (2017, April 11). *data encryption | cryptology | Britannica*. https://www.britannica.com/technology/data-encryption

Kathleen, R. (2021, September). *What is Cryptography? Definition from SearchSecurity*. https://www.techtarget.com/searchsecurity/definition/cryptography

Maneesh Kumar, S. (2021, October 4). *Difference between Substitution Cipher Technique and Transposition Cipher Technique - GeeksforGeeks*. https://www.geeksforgeeks.org/difference-between-substitution-cipher-technique-and-transposition-cipher-technique/

Simmons, G. J. (2017, August 16). *substitution cipher | cryptology | Britannica*. https://www.britannica.com/topic/substitution-cipher

Sudhir, K. (2018, January 28). *GDLC [Game Development Life Cycle]*. http://www.unity3dtechguru.com/2018/01/gdlc-game-development-life-cycle.html