

**Resource Allocation in Multihop**

**Cellular Networks**

**Submitted by: Xxx Xxx**

**Matriculation Number: xxxxxxx**

**Supervisor: Xxxx  
Co-supervisor: Xxxx**

### School of Electrical & Electronic Engineering

A final year project report presented to the Nanyang Technological University

in partial fulfilment of the requirements of the degree of

Bachelor of Engineering

**20xx**

# Table of Contents

[Abstract ***(not more than one page)*** i](#_Toc197854799)

[Acknowledgements **(optional)** ii](#_Toc197854800)

[Acronyms **(optional)** iii](#_Toc197854803)

[Symbols **(optional)** i](#_Toc197854803)v

[List of Figures v](#_Toc197854805)

[List of Tables v](#_Toc197854806)i

[Chapter 1 Introduction 1](#_Toc197854807)

[1.1 Organisations 1](#_Toc197854810)

[Chapter 2 Literature Review](#_Toc197854807)  ……………………………………............................................. ..2

[2.1 xxx 2](#_Toc197854808)

[2.2 xxx 2](#_Toc197854809)

[Chapter 3 xxx](#_Toc197854807)……………………………………………............................................. 3

[3.1 xxx 3](#_Toc197854808)

[3.2 xxx 3](#_Toc197854809)

(More chapters are usually required and can be inserted here)

[Chapter 4 Conclusions and Future Work…………………………………………….... 4](#_Toc197854807)

[4.1 Conclusions 4](#_Toc197854808)

[4.2 Recommendatin in Future Work 4](#_Toc197854809)

References ……………………………………………………………………………………………. 5

Appendix ***(optional)***………………………………………………………………………………… 6

# Abstract

Xxxx …

# 

# Acknowledgements (optional)

First of all, I would like to express my sincere thanks and great gratitude to my parents. …

Xxx Xxx

November 2009

# Terminology

|  |  |
| --- | --- |
| Cryptography  Encryption  Plaintext  Ciphertext  Cipher  Symmetric Key Encryption  Asymmetric Key Encryption  Steganography  Stream Cipher  Block Cipher  Period of a cipher | Cryptography is the science or study of techniques of secret writing [1]. It protects messages and communications by encoding them so only authorized users can read and interpret their true meaning. The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing" [2].  In computer science, cryptography refers to the use of deterministic encryption algorithms which are derived from mathematical concepts to establish secure data transactions [3].  Encryption is the process of transforming human-readable information into unintelligible text. This process uses one or more encryption algorithms and a specified key to encode messages. Decryption is the reverse process.  Plaintext refers to human-readable messages.  Ciphertext refers to encoded, unintelligible messages. Decryption of ciphertext generates plaintext.  a system of writing that most people cannot understand, so that the message is secret; a code [1]. In the digital era, cipher is more widely-known as the algorithm of computerized encryption and decryption. A cipher defines a series of steps or instructions to be followed to encode or decode a message. In many cases, it also uses an encryption or decryption key [3]. The key may be generated by itself, another cipher or environmental variables.  Symmetric key encryption uses the same key for encryption and decryption [4].  Asymmetric Key Encryption uses a public key, which is readily accessible to anyone, and a private key which is known only to the user. Each public key has a corresponding private key. Data encrypted with a public key can only be decrypted by its corresponding private key, and vice versa. Thus, only the user can read the encrypted message. The user can also leave a digital signature on his data by encoding it with the private key [5].  Steganography is a cryptography technique which hides the secret message within other mediums, such as another message, picture or video. The secret message is not transformed, but rather blended into its wrapping medium [6].  A stream cipher encrypts a stream of data. Encryption occurs at bit level or byte level. Encryption key varies with every bit or byte.  A block cipher encrypts a block of data at one time. It outputs an equal-length block of ciphertext. The size of a block may vary in different ciphers. Typically, a block size of 64 or 128 bits is used [7].  Period of a cipher is the number of encryption operations a cipher must perform before the output of the cipher repeats. |

# Acronyms (optional)

|  |  |
| --- | --- |
| RC4  AES  NTU  WPA  HTML5  CSS | Rivest Cipher 4  Advanced Encryption Standard  Nanyang Technological University  WiFi Protected Access  HyperText Markup Language  Cascading Style Sheets |

# Symbols (optional)

Xxxx Xxxxx

# List of Figures

[Figure 1.1: Proposed architecture. 10](#_Toc197854900)

# List of Tables

[Table 2‑1: t1. 30](#_Toc197854967)

# Introduction

Cryptography – the science or study of secret writing – has been a revolving topic of interest for thousands of years. The use of encryption techniques dated as far back as 4000 years ago, when an ancient Egyptian scribe used a simple substitution cipher in his drawings on the walls of a tomb. Caesar’s cipher, one of the most well-known and easiest encrypting method, was invented by Julius Caesar to protect military intelligence during the time of the Roman Republic [1]. Another famous wartime cipher was the Enigma machine. Unlike its 1900-years-older predecessor, the Enigma machine was a sophisticated version of polyalphabetic substitution cipher with 10114 possible configurations, therefore extremely difficult to break in its time. Coming into the modern era, the invention of Internet and the widespread of computers have enabled people to perform more and more activities online. As an increasing amount of information has been produced in or sent over the Internet, cryptography has been used to establish secure data transactions.

Modern cryptography mainly consists of symmetric key encryption, asymmetric key encryption and steganography [1]. In symmetric key encryption, the message sender and the recipient share one key, also called private key, for enciphering and deciphering. The private key must be exchanged prior any data transaction [8]. Asymmetric key encryption, also called public-key cryptography, was invented in the 1970’s because people needed a method to exchange the secret key safely without meeting each other in the physical world [5]. Steganography is the art of concealing a message within another message in plain sight.

Over the years, many symmetric key encryption algorithms have been developed to protect privacy and commerce. They mostly fall into two categories: stream cipher and block cipher. The main difference between them is that encryption occurs at bit level or byte level in a stream cipher, while in a block cipher it occurs at block level -- the size of a block of data depends on the exact block cipher used. A stream cipher takes in a stream of plaintext and outputs a stream of ciphertext dynamically. Examples of stream ciphers are one-time-pad, Linear Feedback Shift Register and RC4. A block cipher encrypts one chunk of data at once, and then outputs an equal-length block. Typically, a block size of 64 or 128 bits is used. Blowfish, RC5 and AES are some popular block ciphers [9].

In computer science, cryptography has been an important topic of study and research. Many academical institutions have opened courses about cryptography alone, or about cybersecurity in which cryptography is inevitably introduced to the students. In NTU, the School of Computer Science and Engineering offers course CZ/CE4024 – Cryptography and Network Security to undergraduates who are interested in how basic cryptography algorithms work and their application in real-world information security systems [10]. Some ciphers mentioned before, such as AES and RC4, are also explained in detail in this course. To facilitate the understanding of the basic enciphering algorithms and illustrate how specific ciphers work, this course has web demonstrations of various ciphers [11]. These web demos transform text descriptions of ciphers into interactive animations, and give users the opportunity to participate in each step of encryption. However, not every encryption algorithm taught in this course has a web demo. One example is RC4, which is simple yet efficient – a good example of stream cipher design. This caused need for its web demo implementation.

This report documents the implementation process of the RC4 web demo for course CZ/CE4024– Cryptography and Network Security. Target users of this web demo are computer science and engineering undergraduates. It is assumed that users understand basic computer science and mathematical concepts such as vector, pseudocode and encryption key. The report explores the mathematics used in RC4 design, justifies the true randomness of encryption key generated by RC4, and explains the functionality of the web demo and how it has been written using HTML, JavaScript, jQuery and Web Animations API. Limitations and potentials of web animation techniques touched in the demo are analyzed as well.

## Organisations

The body of this report includes five chapters. Chapter 1 introduces the background information of RC4 and explains the motivations behind its web demo implementation. Chapter 2 describes the inner workings of RC4 in detail and reviews past works done to illustrate RC4 in graphics and animations. Chapter 3 walks the reader through the implementation step by step and shares insights on its limitations and room for improvement. Chapter 3 also introduces a range of animation techniques provided in JavaScript, jQuery and Web Animation API. Chapter 4 cross-validates the output of the RC4 demo with other similar works. It then proceeds to compare their pros and cons. Chapter 5 concludes the report and share recommendations.

# Literature Review

## RC4 algorithm

RC4 is a stream cipher designed for RSA Security and named after its designer Ron Rivest. Its algorithm uses a key of adjustable length (range of length is from 1 to 256 bytes), and produces pseudo-random bytes through a random permutation. The period of this cipher has been estimated to be above 10100. RC4 is remarkably simple and runs very quickly in software. Due to its simplicity and high speed, it has become widely-used in many applications, such as Wi-Fi Protected Access (WPA) and Kerberos [9].

There are two parts of RC4: Initiation of S, and Stream Generation. In the first part, state vector S and a temporary vector T are initialized as shown in the pseudocode:

for i = 0 to 255 do

S[i] = i;

T[i] = K[i mod keylen];

K stands for key. It is a user-input key and has an adjustable length. Elements of K are used to fill in the elements of vector T. If K is shorter than 256 bytes, it would be repeated as many times as needed to fill out T. Values of vector S is initialized in an ascending order in the range of 0 to 255: S[0] = 0, S[1] = 1, …, S[254] = 254, S[255] = 255.

Next, vector S is permuted according to values of vector T. K is no longer useful in subsequent operations. The permutation pseudocode is presented below:

j = 0;

for i = 0 to 255 do

j = (j + S[i] + T[i]) mod 256;

Swap (S[i], S[j]);

Starting from S[0] to S[255], each vector S element is swapped with another S element the index of which is the value of j. The value of j is determined by vector T.

The second part generates a byte k by selecting one element from the 255 elements of S. Afterwards S is permutated once so that the next round of k-selection uses a different S. The pseudocode below illustrates the permutation:

i, j = 0;

while (true)

i = (i + 1) mod 256;

j = (j + S[i]) mod 256;

swap (S[i], S[j]);

t = (S[i] + S[j]) mod 256;

k = S[t];

It starts with the permuted vector S from the second stage. The cipher loops infinitely through vector S. For each S[i], a j value is calculated according to its value and the value of the previous j. S[i] and S[j] are then swapped, changing the configuration of vector S. Sum of values of S[i] and S[j] is used as an index which points another element in vector S. Value of this element S[ S[i] + S[j] ], is the pseudo-random byte output of RC4.

## Past works done to visualize RC4

There are a few visualizations of RC4 found on the Internet. They are either in the form of videos or in the form of applications. Below are screenshots of two RC4 simulation videos:

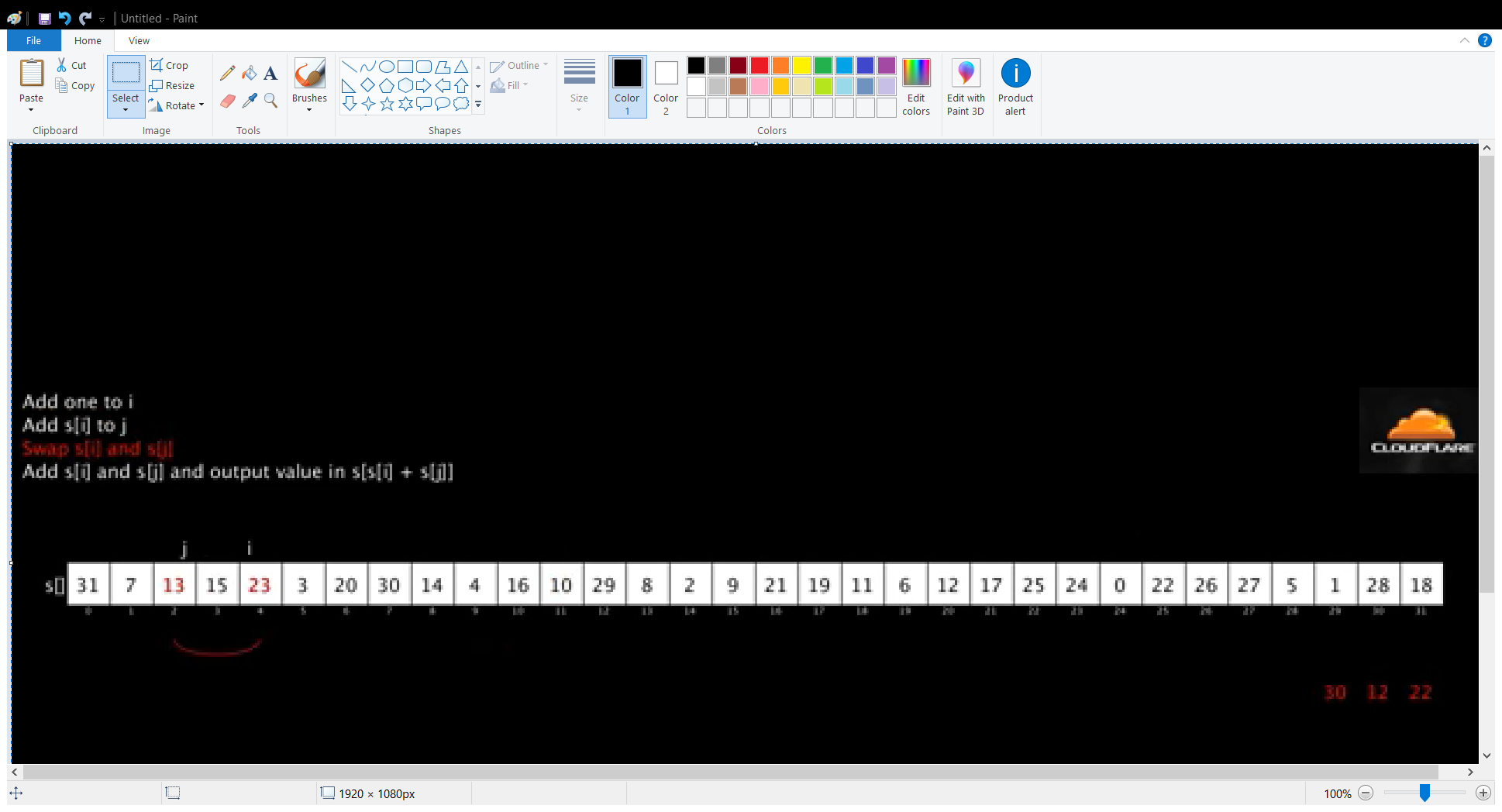


Figure 1. YouTube video “RC4 Algorithm” showing the ‘swap’ operation of RC4 algorithm [12].

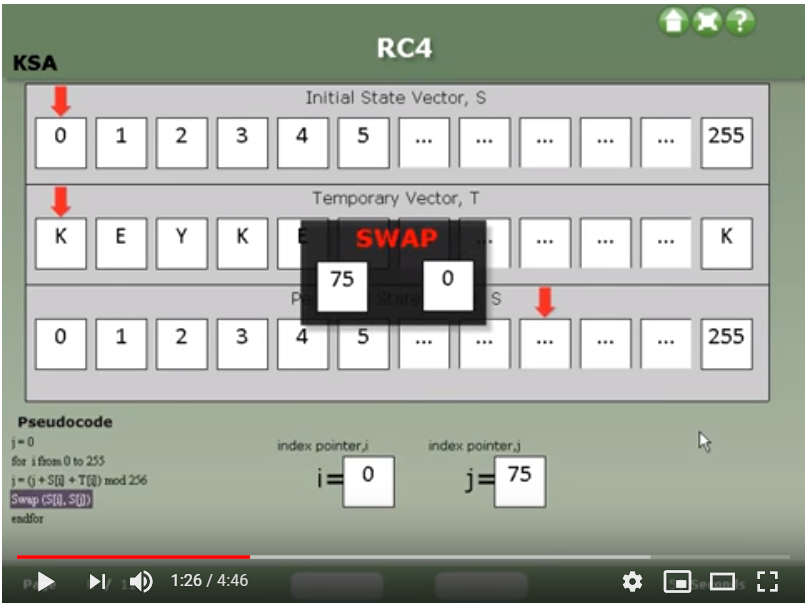
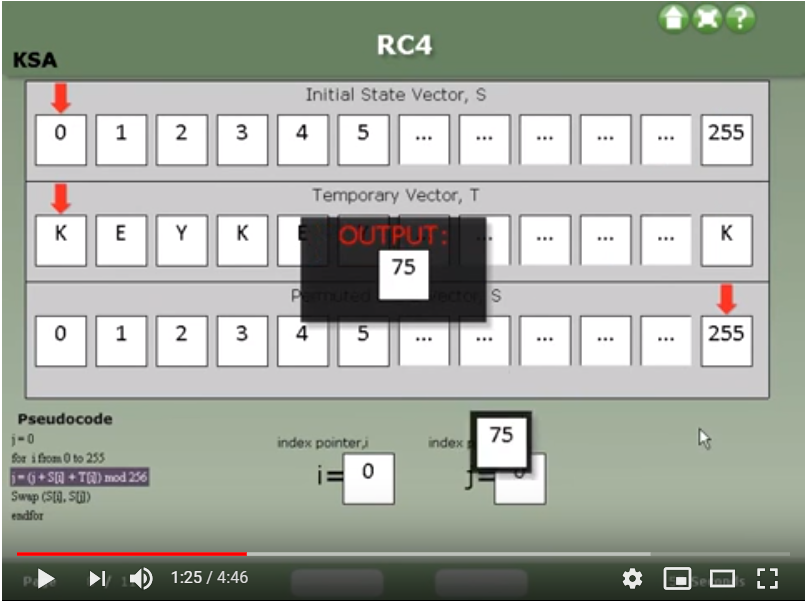
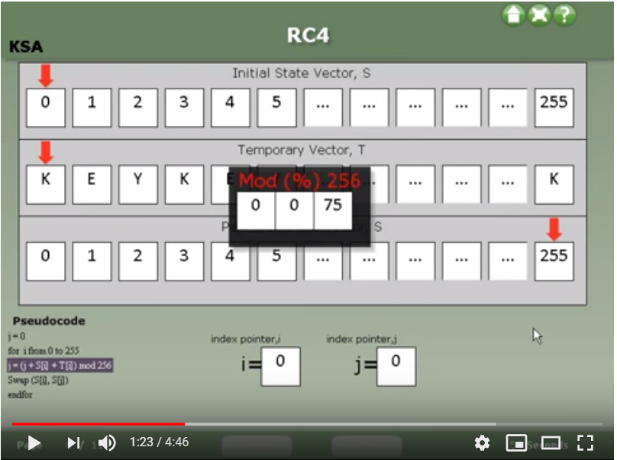
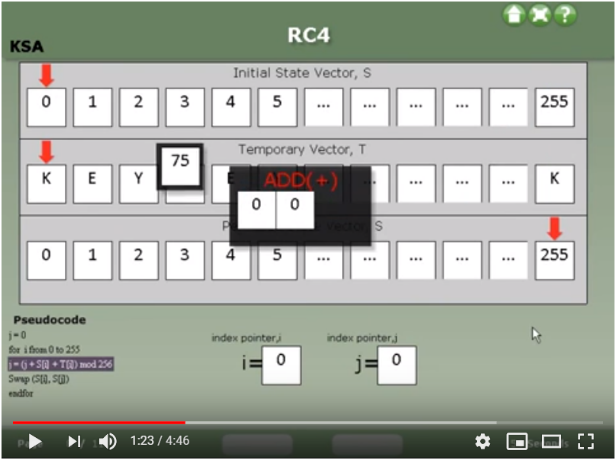


Figure 2(a), (b), (c), (d). YouTube video named “RC4 security algorithm” [13].

In general, these videos display the pseudocode of RC4 operation on one side and put animation section in the center. For each step, the corresponding pseudocode is highlighted in a different color, and then the operation is performed. Figure 2 is an example of a video showing the four steps of the Initial Permutation of vector S. Video format of RC4 visualization is straightforward and easy to understand. However, its encryption key value and plaintext is prefixed, lacking interactivity.

The other format is application. Two applications were found to truly simulate every step of RC4 algorithm. One application was developed by Vishwas Gagrani (YouTube account name). the video shown in Figure 2 is an introductory recording of his application with a given key and plaintext. This application used to be freely available on Google Play but was removed at some point of time in 2018 [13]. Another application was never made available to the mass, only presented in a conference paper [14]. In addition to RC4 algorithm, this application also implements ASCII conversion of key and plaintext. Figure 3 shows this function:

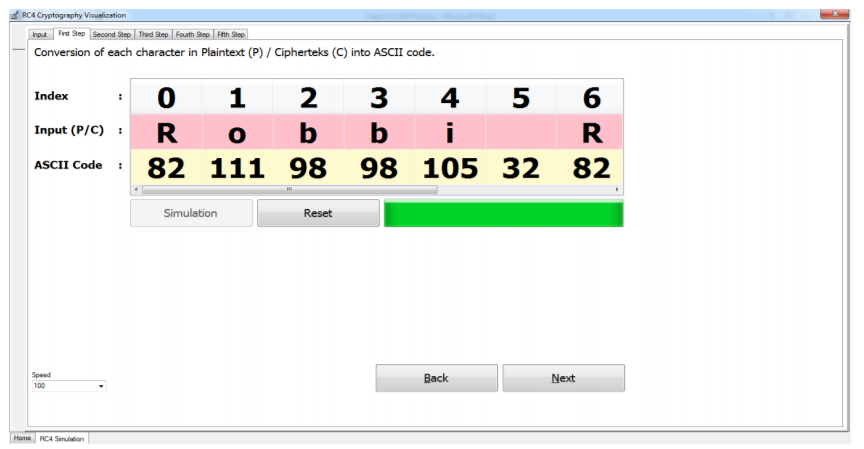
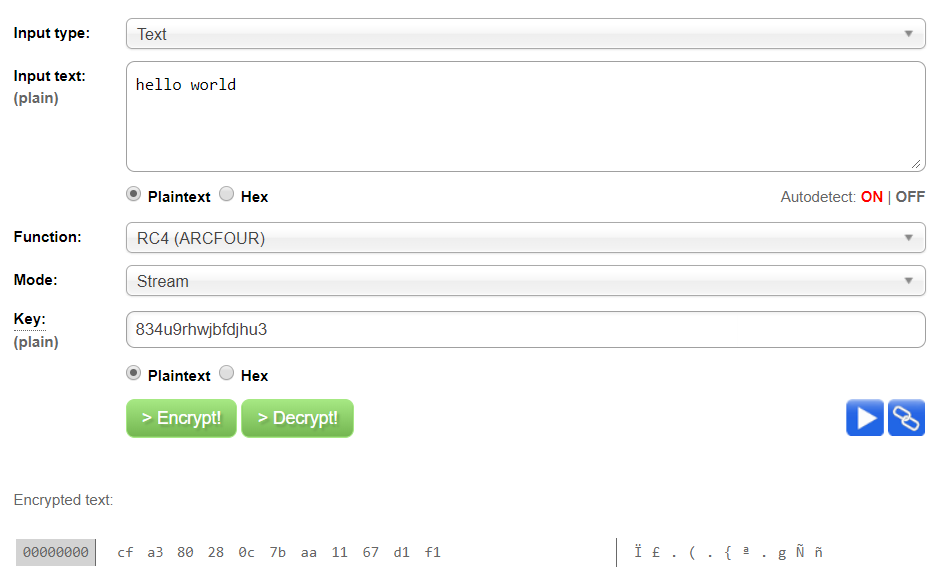


Figure 3. ASCII conversion of plaintext.

Other than videos and applications, there are many webpage simulations of RC4. However, they do not show the internal operations between input and output. Figure 4 below gives an example.

Figure 4. Webpage simulation of RC4 [15].

To summarize past works done on RC4 visualization, some videos and applications are helpful RC4 simulations for people who want to gain a solid, detailed understanding of RC4. Unfortunately, the videos are non-interactive with little explanation to aid learning, and the applications are not accessible to the NTU community. This caused a need for an interactive RC4 simulation to be developed and made available to not only NTU students but also everyone who are interested in cryptography.

# Implementation of RC4 Web Demonstration

## General structure

The web demo (demonstration) has four sections: Introduction, Stage 1, Stage 2 and Stage3.

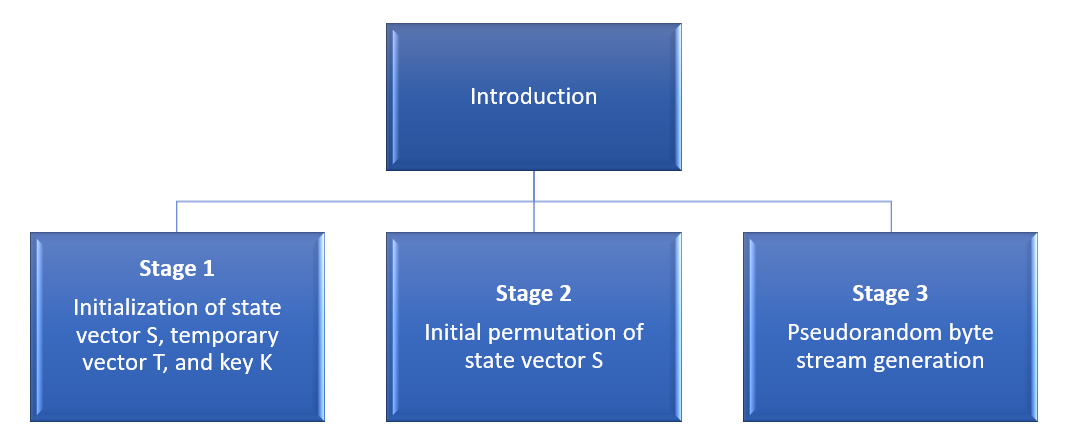


Figure 5. structure of web demo.

Introduction section gives the reader a brief overview of RC4. RC4 algorithms can be divided into three sub-sections, hence the three stages. The division of RC4 process is not an industrial practice, but rather a choice made during implementation in order to make RC4 easier to comprehend. The first two stages correspond to the first part described in 2.1 RC4 algorithm; the third stage corresponds to the second part. Below are screenshots of the four sections.

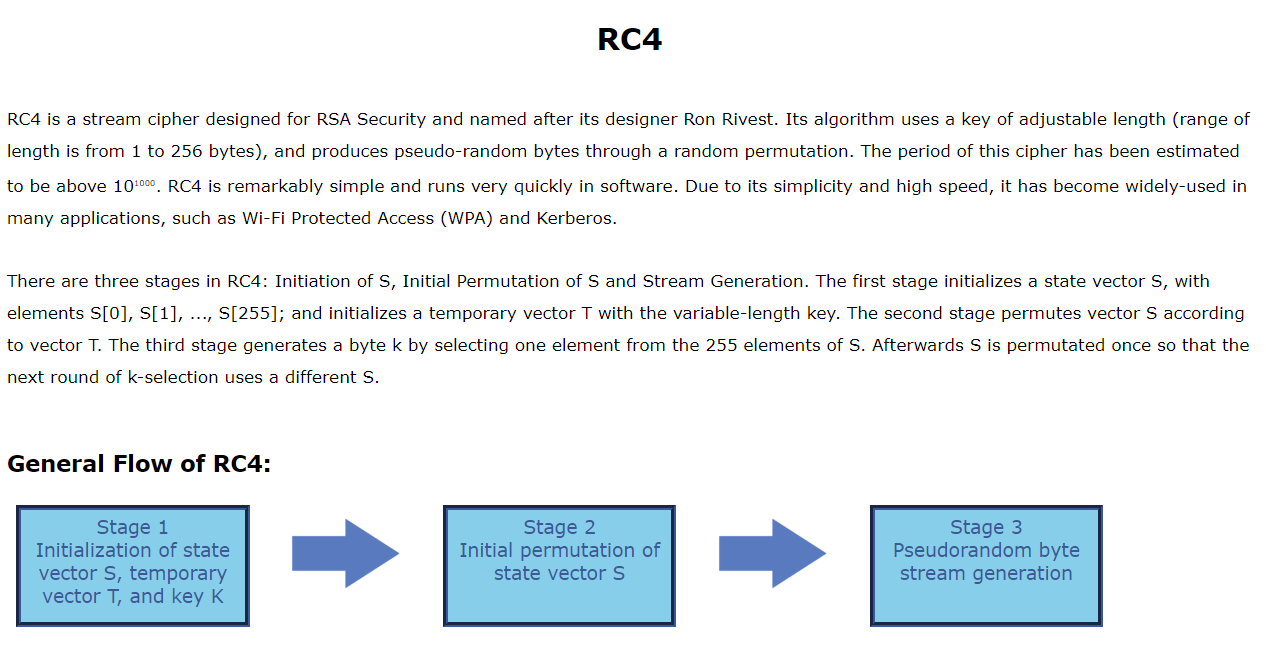


Figure 6. Web demo section 1.

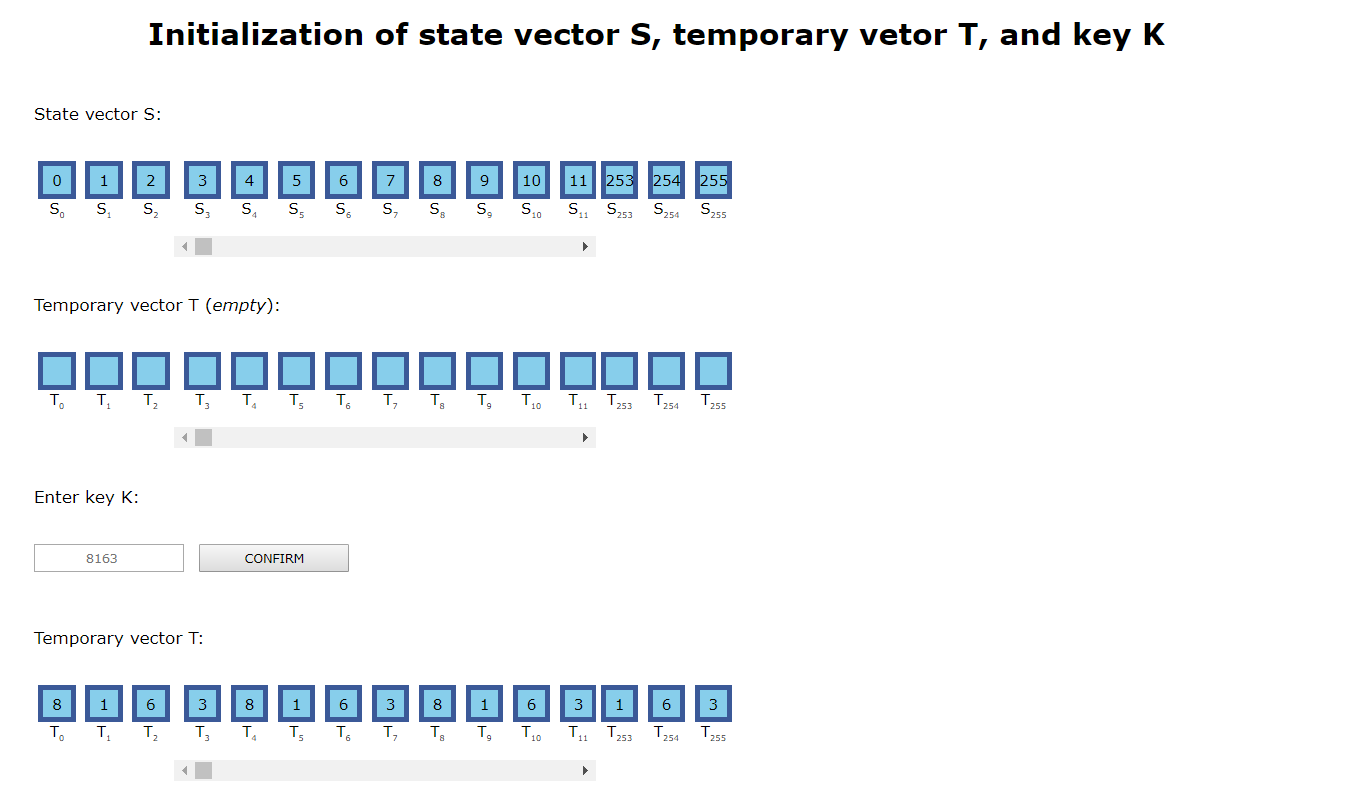


Figure 7. Web demo section 2.

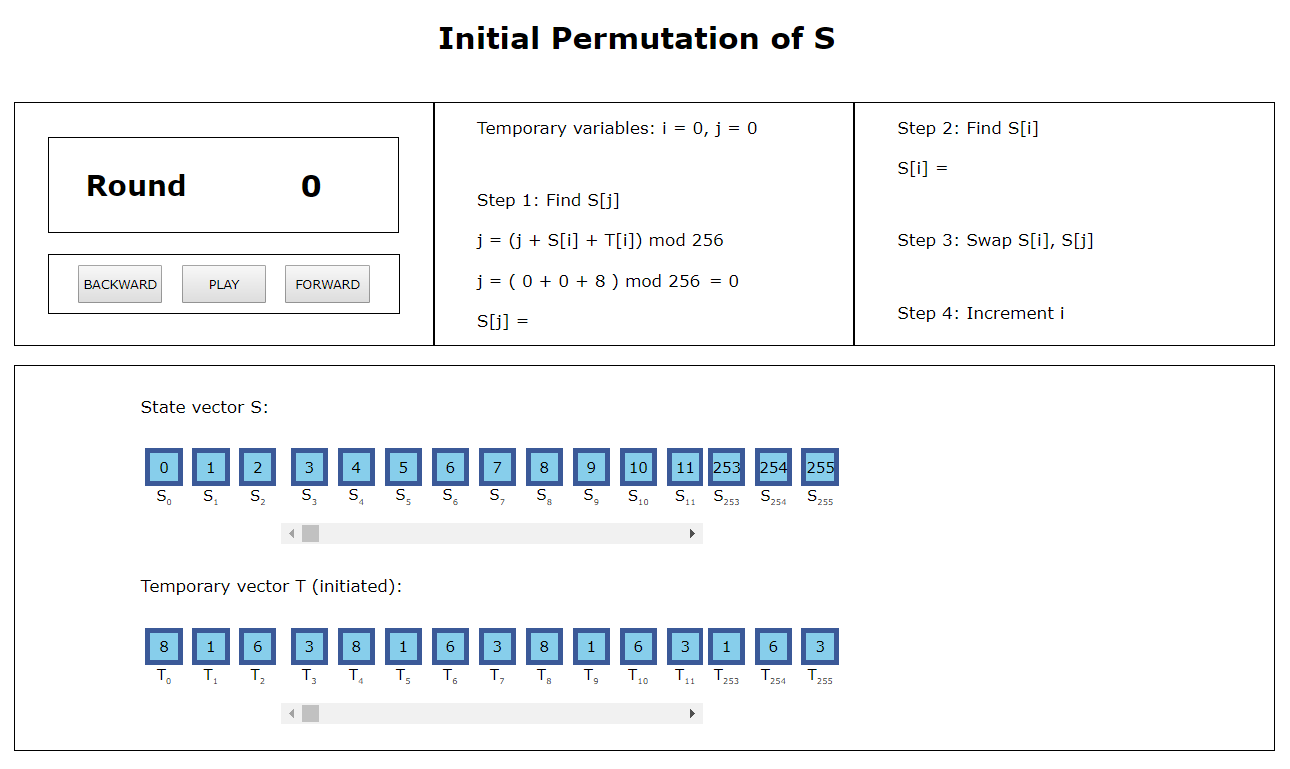


Figure 8. Web demo section 3.

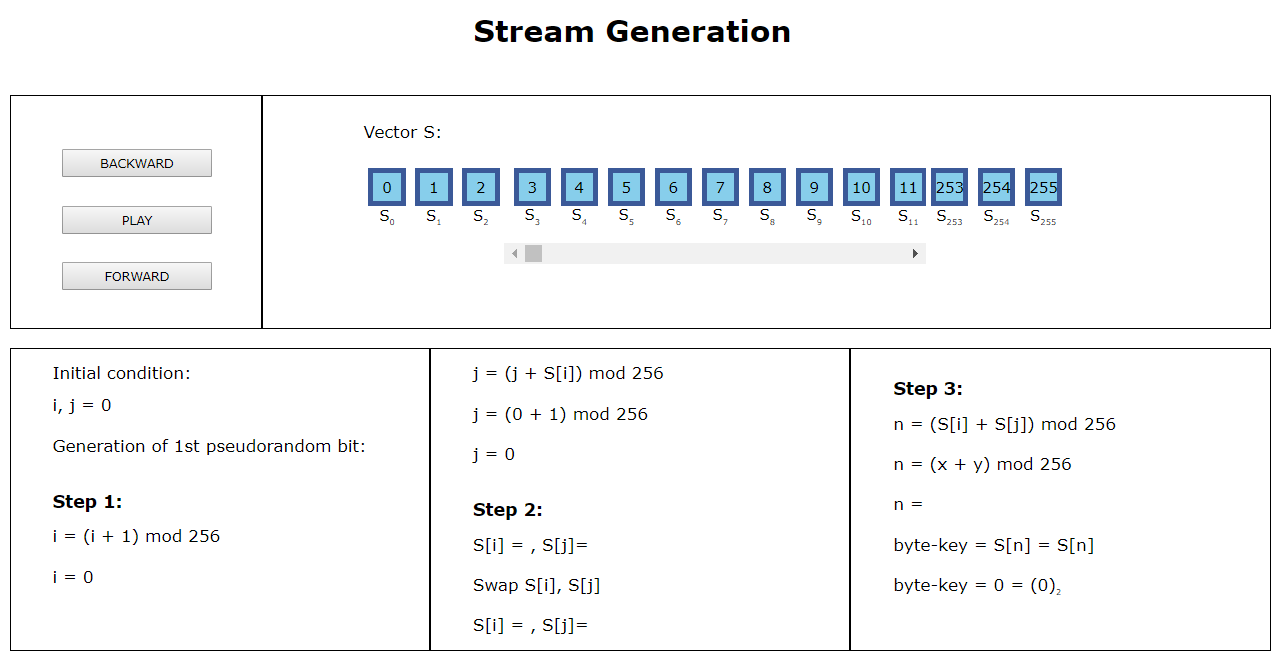


Figure 9. Web demo section 4.

The text and its styling in the webpage are created using HTML5 and CSS. An external CSS style sheet is used to keep the webpage document clean and simple, while making it easy to control its overall CSS style.

## xxx

# Chapter 4

**Conclusions and Future Work**

# 4.1 Conclusions

…

# 4.2 Recommendation in Future Work

# …References

|  |  |
| --- | --- |
| [1] | "Dictionary.com Definitions Cryptography," [Online]. Available: https://www.dictionary.com/browse/cryptography. [Accessed 17 November 2018]. |
| [2] | M. Rouse, "Definition cryptography," [Online]. Available: https://searchsecurity.techtarget.com/definition/cryptography. [Accessed 16 November 2018]. |
| [3] | N. G. McDonald, "Past, Present, And Future Methods Of Cryptography And Data Encryption". |
| [4] | W. Stallings, Cryptography and Network Security Principles and Practices, 4th ed., vol. I, Prentice Hall, 2005, p. 30. |
| [5] | "Public Key Cryptography," International Business Machines Corporation, [Online]. Available: https://www.ibm.com/support/knowledgecenter/en/SSB23S\_1.1.0.13/gtps7/s7pkey.html. [Accessed 16 November 2018]. |
| [6] | "Steganography," Merriam-Webster, Incorporated, [Online]. Available: https://www.merriam-webster.com/dictionary/steganography. [Accessed 16 November 2018]. |
| [7] | W. Stallings, Cryptography and Network Security Principles and Practices, 4th ed., vol. I, Prentice Hall, 2005, p. 64. |
| [8] | "Symmetric Cryptography," International Business Machines Corporation, [Online]. Available: https://www.ibm.com/support/knowledgecenter/SSB23S\_1.1.0.13/gtps7/s7symm.html. [Accessed 18 November 2018]. |
| [9] | W. Stallings, Cryptography and Network Security Principles and Practices, 4th ed., vol. I, Prentice Hall, 2005, pp. 23-194. |
| [10] | A. Datta, "CryptoIntroduction," Singapore, 2018. |
| [11] | A. Datta, "Random Cryptography Demos," Nanyang Technological University, 2018. [Online]. Available: http://pdcc.ntu.edu.sg/sands/cryptodemos/#fh5co-tab-feature-vertical7. [Accessed 18 November 2018]. |
| [12] | jgrahamc, "RC4 Algorithm". |
| [13] | M. Asaad, "RC4 Security Algorithm". |
| [14] | "Cipher," Cambridge University Press, [Online]. Available: https://dictionary.cambridge.org/dictionary/english/cipher. [Accessed 16 November 2018]. |

|  |  |
| --- | --- |
| [1] | "Dictionary.com Definitions Cryptography," [Online]. Available: https://www.dictionary.com/browse/cryptography. [Accessed 17 November 2018]. |
| [2] | M. Rouse, "Definition cryptography," [Online]. Available: https://searchsecurity.techtarget.com/definition/cryptography. [Accessed 16 November 2018]. |
| [3] | N. G. McDonald, "Past, Present, And Future Methods Of Cryptography And Data Encryption". |
| [4] | W. Stallings, Cryptography and Network Security Principles and Practices, 4th ed., vol. I, Prentice Hall, 2005, p. 30. |
| [5] | "Public Key Cryptography," International Business Machines Corporation, [Online]. Available: https://www.ibm.com/support/knowledgecenter/en/SSB23S\_1.1.0.13/gtps7/s7pkey.html. [Accessed 16 November 2018]. |
| [6] | "Steganography," Merriam-Webster, Incorporated, [Online]. Available: https://www.merriam-webster.com/dictionary/steganography. [Accessed 16 November 2018]. |
| [7] | W. Stallings, Cryptography and Network Security Principles and Practices, 4th ed., vol. I, Prentice Hall, 2005, p. 64. |
| [8] | "Symmetric Cryptography," International Business Machines Corporation, [Online]. Available: https://www.ibm.com/support/knowledgecenter/SSB23S\_1.1.0.13/gtps7/s7symm.html. [Accessed 18 November 2018]. |
| [9] | W. Stallings, Cryptography and Network Security Principles and Practices, 4th 编辑, 卷 I, Prentice Hall, 2005, pp. 23-194. |
| [10] | A. Datta, "CryptoIntroduction," Singapore, 2018. |
| [11] | A. Datta, "Random Cryptography Demos," Nanyang Technological University, 2018. [Online]. Available: http://pdcc.ntu.edu.sg/sands/cryptodemos/#fh5co-tab-feature-vertical7. [Accessed 18 November 2018]. |
| [12] | jgrahamc, "RC4 Algorithm". |
| [13] | M. Asaad, “RC4 Security Algorithm”. |
| [14] | "Cipher," Cambridge University Press, [Online]. Available: https://dictionary.cambridge.org/dictionary/english/cipher. [Accessed 16 November 2018]. |

**Appendix (optional)**