جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة ديالى/كليةالعلوم/ قسم الرياضيات

بروتوكول المرور الثلاثي على نظام شفرة حقيبة الظهر المعدل

رسالة مقدمة

إلى/جامعة ديالى/كلية العلوم/ قسم الرياضيات كجزء من متطلبات نيل شهادة الماجستير في علوم الرياضيات

من قبل

طه عبد شلفون

المشرف

أ.م.د.رفعت زيدان خلف

1442هـ

2021م

Chapter One

General Introduction

Chapter One

General Introduction

1.1 Overview

Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries. It is a way to store and transfer data in a particular format so that only authorized persons capable of reading and processing [**1],[2**].Many types of cryptosystems have been invented, Knapsack Encryption Algorithm is the first algorithm for encrypting public key. It was developed by Ralph Markel and Martin E. Hellman in 1978 [**3**].Public-key encryption or asymmetric encryption is essentially depends on two types of keys [**4**]. Here, two mathematically related keys are used, private, and public key. Differently, symmetric key algorithms that use the same key for encrypting and decrypting the data [**5]**.With asymmetric encryption, anyone has the ability of encrypting a message using the public key of the intended receiver, but it is possible to decrypt that message encrypted, only by the use of the private key of the receiver. It is not mathematically feasible to find out a private key based on a public key. For that reason, keys can be shared for receiving transactions, meanwhile private key must remains secret, guaranteeing only the private key holder decrypts content and makes digital signature[**6**].

TPP is a concept of sending information that let the senders to securely sending messages to receiver using its key and the receiver decrypt the encrypted messages using its key as well [**7**].It is called TPP because receiver and sender make three ciphertext. Adi Shamir had firstly developed TPP in 1980[**8**].

The main concept of implementing this protocol is that both the sending and receiving parties have a private key to encrypt and a private key to decrypt [**9**].we proposed two methods to modify knapsack problem-based cryptography system using (TPP).

1.2 Related Work

1.**B.Oktaviana and A. Putera Utama**[**10**] **Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography**: This study combined the classical encryption algorithm with the modern encryption algorithm that can be used to protect /classified data. The theories covered two algorithms related to encryption, like TPP and Caesar Cipher ,but TPP is a method related to the mechanism of making the same algorithm run two times in both processes decryption and encryption. This technique does not share password during both decryption and encryption processes. Furthermore, Through the combination process of both TPP and traditional cryptography, the resulting ciphertext is ensured . The data sending process does not require to key-sharing with to the message sender, anymore. It is possible to use classical cryptography , but it can be susceptible to be attacked.

2.A. P. U. Siahaan[11]Three-Pass Protocol Concept in Hill Cipher Encryption Technique: Several techniques are introduced for dismantling the message, Hill Cipher (HC) employs the model of symmetric key. It is necessary to distribute this key to massage receiver to facilitate restoring the ciphertext into plaintext by the receiver. In the application of TPP in HC, plaintext cannot be converted immediately to ciphertext, and then the message is encrypted by using the second key. The ciphertext cannot be converted to the original one ; It is converted

into a dissimilar character's order. Therefore, it is possible to apply TPP in HC. Basically, this process will help senders provide more security for his/her data from interception. The technique of non-distributed key is safer than the regular technique where each participant is not required to exchange keys when performing a process like that. TPP is the optimum technique to provide more security to data/ information.

3. **A. Subandi, R. Meiyant i, and C. L. M. R. Sembiring [12] Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Keystream Generator Modification**:

The study shows the mechanism of implementing traditional algorithmVigenere Cipher by modifying the key and how to apply it in TPP that the sending party and receiving party are not required performing key sharing. The key modification of Vigenere Cipher, The research shows that by making adjustment to the keys, classical algorithm Vigenere Cipher can be more reliable than the standard Wigner encryption. This is due to modifying the keys that are created from a process that has been done. Therefore, when the length of the key is not equivalent to the plaintext length, the key would not be repeated but a function will generate it. This leads to generate more random keys instead of repeating the key, as in the algorithm of standard Vigenere Cipher.

4. **Dian Rachmawat, Amer Sharif, and Rosalia Sianipar [13] A combination of vigenere algorithm and one time pad algorithm in the three-pass protocol:** In this study, the cryptographic algorithms which used are Vigenere Cipher and One Time Pad. However, the security of both algorithms depends on the security of the algorithm key. Three-Pass Protocol is a scheme of work that lets two people exchange secret messages without doing a key exchange. So, both the symmetric

cryptographic algorithms combined on a TPP scheme. The purpose of the combination of two algorithms in the three-pass protocol is to secure the image message without exchange key process between sender and recipient. The results of the research and testing using Get Pixel pointed out that safeguarding the image file using the combination of Vigenere Cipher and One Time Pad algorithm restores the original image files intact. Therefore, it meets the parameters of the integrity of the data. The test results based on time parameter shows that time of the program execution process is directly proportional to the size of the image. The result is related with the formula which calculate every pixels of the image.

5. **Aqeel Aziz [14] New Approach of RSA Algorithm based on Three-Pass Protocol**: The proposed system used TPP method with the RSA cryptosystem by combining them. The main aim of the proposed algorithm is a secret message exchange between the sender and the receiver by using the RSA cryptosystem and they do not need to know the public key for each other. In addition, the implementation of this work shows that the security is improved and it is more efficient compared with the traditional RSA cryptosystem . Moreover, the new approach of RSA algorithm achieves success in sending the message securely without sharing any keys , this is the main point and the difference with the RSA algorithm. The new approach of RSA algorithm develops the security aspect; it is secure enough when compared to RSA, as it relied upon the factoring problem and sharing the public keys of both parties.

6. **R. Rahim [15]**A **Review on Cryptography Protocol for Securing Data :**This study applies systematic approach to protocol cryptography for security level and uses other algorithms to be combined with the

protocol. It is possible to use the cryptography protocol to handle problems related to key sharing occurring among the sending parties and receiving ones. Using Shamir's TPP with the Pohlig-Hellman algorithm can function very well.

1.3 Problem Statement

Knapsack Cipher is susceptible to a lot of attacks by attackers , and compromised through various application techniques by compromising algorithms that have vulnerabilities. This leads to weak insecure algorithms and thus unusable in most of the applications. This serious issue allows researchers and developers in the field of security to offer several solutions to alleviate the risks involved.

1.4 Aim of Thesis

To solve the above-mentioned problems, a system for improving the knapsack cipher was proposed, using two methods:

1- Rifaat method (TPP Implementation on modified Knapsack cipher).

2- Taha method (TPP Implementation on modified knapsack cipher with linear equations).

1.5 Thesis Outlines

Beside this chapter, the remaining parts of the thesis include the following chapters:

Chapter Two: Theoretical background

This chapter includes the mathematical background of the concepts adopted in the proposed system. Public key cryptosystems and encryption.

Chapter Three: Knapsack Cipher and TPP

In this chapter, the knapsack Cipher some related concepts and TPP is a concept of sending information.

Chapter Four: TPP Implementation on Modified Knapsack Cipher

This chapter involves studies and results, which are obtained from the system proposed as well as the results of the knapsack cipher and Implementation TPP.

Chapter Five: **Conclusion and Suggestion for Future Work*s***

This chapter presents conclusions from the results of the presented work and some suggestions for future works.

المستخلص

خوارزمية تشفير حقيبة الظهر(**Knapsack**) هي أول خوارزمية تشفير للمفتاح العام. يستخدم هذا النوع من نظام التشفير مفتاحين مختلفين لعملية التشفير وفك التشفير. معظم أنظمة تشفير (**Knapsack**) التي تم إدخالها حتى الآن ليست آمنة ضد الهجماتلوجود نقاط ضعف في تصاميم شفرة(**Knapsack**). بروتوكول ثلاثي المرورهو واحد من أنظمة التشفير الحديثة حيث عملية إرسال رسالة لا تحتاج إلى توزيع المفتاح بحيث كلا من المرسل و المستلم للرسالة لا يحتاج إلى معرفة بعضها البعض.

وبناء على ذلك، فإن الهدف الرئيسي من هذه الرسالة هو تنفيذ دراسة جديدة للجمع بين شفرة(**Knapsack**)، مع تشفير بروتوكول ثلاثي المرور الحديث.يمكن أن يكون بروتوكول ثلاثي المرور حلا لأنظمة الأمان التي تتطلب عملية أفضل عن طريق الجمع بين خوارزمية التشفير وغيرها كحل للمشكلة.

في هذه الرسالة استخدمنا طريقة بروتوكول ثلاثي المرور(**TPP**) مع نظام التشفير(**Knapsack**) من خلال الجمع بينهما، وهذا المزيج يسمح للمرسل والمستقبل لتبادل الرسائل بشكل آمن دون الحاجة إلى إرسال مفتاح عام لهم، وذلك لأن بروتوكول الجمع المقترح لديه هذه الخاصية، لذلك يتم تحسين أمن التكامل من خوارزمية (**Knapsack**). بالإضافة إلى ذلك ، يظهر تنفيذ هذا العمل أنه أكثر كفاءة في المقارنة مع نظام تشفير (**Knapsack**) التقليدي.