Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Diyala
College of Science
Mathematics Science Department

"Three Pass Protocol Implementation On Modified Knapsack Cipher"

A Thesis Submitted to
the University of Diyala / College of Science / Department of Mathematics,
InpartialFulfillmentoftheRequirementsfortheDegreeofMasterinMathematicsScience

By

Taha Abd Shalfon

Supervised By

Assistant Professor Doctor Rifaat Zaidan Khalaf

2021A.D. **1442A.H.**

سورة الأحزاب الآية٥٦

Dedication

To the martyrs of Iraq...

To my mother…

To my father…

To my wife…

To my sons...

To my brothers…

To my sisters…

Taha Al-Fuhairi

Supervisor's certification

We certify that this thesis entitled **“Three pass protocol implementation on modified knapsack cipher”** was prepared by **“Taha Abd Shalfon”** under our supervision at the University of Diyala Faculty of Science Department of Mathematics Science, as a partial fulfillment of the requirements needed to award the degree of Master of Science in Mathematics Science.

Signature:

Name: Dr. Rifaat Zaidan Khalaf

Title: Assist. Prof.

Date: / /2021

(Supervisor)

In view of the available recommendation, we forwarded this thesis for debate by the examination committee.

Signature:

Name: Dr. Lieth Abdullatif Majed

Title: Assist. Prof.

Head of Mathematics Science Department

Date: / /2021

Examination Committee Certification

We certify, as an examining committee, that we have read this thesis entitled "**Three pass protocol implementation on modified knapsack cipher**" and examined the student "**TahaAbdShalfon**" and found that the thesis meets the standard of a thesis for the degree of Master of Mathematic Science.

(Chairman)
Signature:
Name: Dr. Ayad A. Abdulsalam
Title: professor
Date: / /2021

(Member)
Signature:
Name: Dr. Faez Hassan Ali
Title: Assistant Professor
Date: / /2021

(Member)
Signature:
Name: Dr. Anwar nooruldeen imran
Title: Assistant Professor
Date: / /2021

(Member/Supervisor)
Signature:
Name: Dr. Rifaat Zaidan Khalaf
Title: Assistant Professor
Date:

Approved by the Dean of College of Science, University of Diyala

(The Dean)
Signature:
Name: Tahseen Hussein Mubarak
Title: professor
Date: / /2021

Linguistic Certification

This is certify that this thesis entitled "**Three pass protocol implementation on modified knapsack cipher**" was prepared by "**TahaAbdShalfon**" under my linguistic supervision. Its language was amended to meet the English style.

Signature:

Linguistic Supervisor: Dr. Fatima M. Aboud

Title: Assistant Professor

Date: / /2021

Scientific Certification

This is certify that this thesis entitled "**Three pass protocol implementation on modified knapsack cipher**" was prepared by "**TahaAbdShalfon**" under my Scientific supervision. It has been evaluated Scientifically, therefore, it is suitable for debate by examining committee.

Signature:	Signature:
Scientific supervisor:	Scientific supervisor:
Dr. Abdul Khaliq Owaid Mazeel	Dr. Alharith Abdulkareem Abdullah
Title: Assistant Professor	Title: Assistant Professor
Date: / /2021	Date: / /2021

ACKNOWLEDGMENTS

First of all, I thank God almighty, for granting me the ability and patience to do this work successfully and well. I will never forget anyone who helped and encourages me during my studies. Then I would like to express my sincere gratitude to my supervisor (Assistant Prof. Dr. Rifaat Z.Khalaf) for his valuable and profitable time, which he gladly provided through my full studies here with a welcoming heart. I appreciate his optimistic behaviour ,which has always encouraged me to my tough job.. After that, I would like to express my special thanks to the PhD instructors and the rest of all my faculty whose job has been to maintain improving my knowledge and broadening my views in a variety of ways. I also love to save thanks all my friends whose have provided me with useful feedback and pushed me forward.

Taha Al-Zuhairi

ABSTRACT

Knapsack Cryptosystem is the first public key encryption algorithm. This kind of cryptosystem uses two different keys for the encryption and decryption process. Most knapsack cryptosystems that have been introduced so far are not secure against cryptanalysis attacks. These cryptanalytic attacks find weaknesses in the designs of the knapsack cipher. Three Pass Protocol(TPP) is one of the modern encryption systems where the process of sending a message does not need to distribute the key so that both the recipient and the sender of the message do not need to know each other.

Accordingly, the main goal of this thesis is to implement a new study to combine the traditional knapsack cipher with the modern TPP encryption. TPP could be a solution for security systems that require a better process by combining a cryptographic algorithm and other as a solution to the problem.

In this thesis we used a three-pass protocol (TPP) method with the knapsack cipher by combining them, this combination allows senders and the receivers to exchange the messages securely without need to send a public key for them, because the proposed combination protocol has this property, so the integration security of the knapsack algorithm is improved. In addition, the implementation of this work shows that the security is improved and it's more efficient comparing with the traditional knapsack cipher.

Table of Contents

List of Figures

List of Tables

List of symbols and Abbreviations

Abbreviated Form	Full Form
Z	Integers Numbers
R	Real Numbers
*	Multiplication operation
+	Addition operation
⁄	Division operation
-	Subtraction operation
GCD	Greatest common divisor
Mod	Modulus
S	super increasing sequence of positive Integers
B	Sequence of public key
(s ,q ,r)	private key
M	Message
r_1	Multiplier for the sender (Alice)
r_2	multiplier for the recipient(Bob)
r_2^{-1}	Multiplier inverse for the recipient(Bob)
E_A	Encryption key (Alice)
E_B	Encryption key (Bob)
D_A	Decryption key (Alice)
D_B	Decryption key (Bob)
CT	Cipher text
PT	Plaintext
HC	Hill Cipher
RSA	Rivest Shamir and Adelman
U.T	Unwanted terms
W.T	Wanted terms
TPP	Three Pass Protocol
D	Determinant of matrix
Key_1^{-1}	Inverse of Key_1 matrix
Key_2^{-1}	Inverse of Key_2 matrix
$(\text{Cipher text})^T$	Transpose (Cipher text)

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.

Chapter Two

Theoretical Background

Chapter Two

Theoretical Background

2.1 Introduction

This chapter includes the basic theoretical aspects of recognition system in the mathematical background that we need used in this work and the definitions, concepts, and systems used in improving the discussed and also it presents the background for various necessary preprocessing issues and techniques that had been includes concepts of number theory and linear algebra with appraisal of cryptography and its types such as symmetric and asymmetric.

2.2 Mathematical background Terms

This section includes definitions and mathematical concepts that have been used in the public-key systems, especially in the knapsack cipher system.

Definition (2.1)Greatest common divisor (GCD)[16]: Let p and q be two integers , at least one of the integers cannot be zero .Greatest common divisor (GCD) of p and q is the positive integer denoted by d=gcd(p,q) satisfying :

1. d is divisible by p and q.
2. If c is divisible by p and q, then $c \leq d$.

Definition (2.2) Euclidean division: In arithmetic, Euclidean division or division with remainder is the process of dividing one integer integer (the dividend) by another (the divisor), in a way that produces a quotient and a remainder smaller than the divisor[17].

Definition (2.3) modulus (MOD): Given two positive number s*a* and *n*, *a* modulo *n* (abbreviated as *a* mod *n*) is the remainder of the Euclidean division of *a* by *n*, where *a* is the dividend and *n* is the divisor[**18**]. The modulo operation is to be distinguished form the symbol mod, which refers to the modulus [**19**](or divisor) one is operating form.

$a=n\,q+r$

$q=a/n$,*q*=quotient

$0 \le r < a$

$r=a \bmod n$

Definition (2.4)Coprime, Relatively prime: In number theory**,** If both *p* and *q* are two given integers they are called **coprime, relatively prime or mutually prime** if their greatest common divisor gcd(*p* ,*q*)=1.Consequently, any prime number that divides one of *p* or *q* does not divide the other**[20]**.

Definition (2.5)super- increasing : In mathematics, a sequence of real numbers that are positive ($S_1, S_2, \ldots, S_n$) can be called "super- increasing "if each sequence element would be bigger than the entre former elements' sum in sequence [**23**]. In formal context, it is possible to write this condition for all $n \geq 1$

$$s_{n+1} > \sum_{j=1}^{n} s_j \qquad \ldots(3.1)$$

Theorem(2.1)[20] : Let *p, q* and *s* are integers. when *p* is dividing *s*and *q*, then, *p* is dividing $q\,x + s\,y$ for each x and y .

Theorem(2.2) [20]: The Division Algorithm: Given an integers *p and q*, with $q > 0$, there are matchless integers *rand m* so that $p = q\,m + r$ with $0 \le r < qp$ is called the dividend, *m* the quotient, *q* the divisor and *r* represents the remainder.

Lemma(2.2.1) [20]: Let $p,q \in z^+$.when $p = q\ m\ + r$, then gcd(p, q) = gcd(q, r).

2.3 The Euclidean Algorithm[20]:

Input :a and b, $a \geq b$

Output: gcd of a and b ;

While $b \neq 0$ >o

$r = a$ mod b ;

$a=b$,$b=r$;

end

gcd=a ;

Theorem (2.3) (Euclidean algorithm) [20]: Let a, $b \in z^+$with $a \geq b$. Put $r_0 = a$ and$r_1 = b$. For each $j \geq 0$, apply the division algorithm to divide r_j by r_j+1 to obtain an integer quotient q_j+1 and remainder r_j+2, so that:

$r_j = r_j$+q_j+1 + r_j+2 with $0 \leq r_j$+2 < r_j+1.

This process terminates when a remainder of 0 is reached, and the last nonzero remainder in the process is gcd (a, b).

Theorem(2.4)[20]: Given two integers p and q are not both zero.Then, GCD of p and q is a linear combination. i.e. there are two integers m, n so that gcd$(p, q) = mp + nq$.

Theorem(2.5)[20]: Given two integers p and q, then $\frac{p}{gcd\ (p,q)}$, $\frac{q}{gcd\ (p,q)}$are relatively prime.

Euclidean's Lemma (2.6) [20]: When q and p are relatively prime and $p = xqs$ then p divides s.

2.2.1Algorithm: The multiplicative inverse of a mod $q(a^{-1}b)$

Input : Two non-negative integers a and b with $a \geq b$
Output : The multiplicative inverse of a mod b
Step 1: x=0; Step 2: do Step 3: $x = x + 1$ Step 4: $y = a * x$ Step 5: $y = y$ mod b Step 6: if $y = 1$ then Step 7: return x Step 8: while $x < b$

Example(2.1): Assume we have $p = 3$, $q = 32$, to compute a multiplicative inverse of **3** (mod 32) follow the following steps:

$3x = 1 - 32y$

$ax \equiv 1\ (mod\ b), 3x \equiv 1\ (mod\ 32)$

By using extended Euclidean algorithm:

$32 = 10 * 3 + 2$

$3 = 1 * 2 + 1$

Backwards substitution for two above steps:

$2 = 32 - 10 * 3$

$1 = 3 - 1 * 2$

$= 3 - 1 * (32 - 10 * 3)$

$= 3 - 32 + 10 * 3$

$= 11 * 3 - 32$

$11 * 3 = 1 + 32 \equiv 1 \ (mod\ 32)$

Satisfying to $3x \equiv 1 \ (mod\ 32)$:

$x = 11$is represents $p^{-1}q$.

2.4 System of linear equations

A system of linear equations (or linear system) is a finite collection of linear equations in same variables. For instance, a linear system of m equations in n variables $x_1, x_2, \ldots, x_n$ can be written as:

$a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1$

$a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2$

$\vdots$

$a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m$

A solution of a linear system is a tuple $(s_1, s_2, \ldots, s_n)$ of numbers that makes each equation a true statement when the values $s_1, s_2, \ldots, s_n$ are substituted for $x_1, x_2, \ldots, x_n$ respectively. The set of all solutions of a linear system is called the solution set of the system.

2.4.1 Types of Matrices

Different types of Matrices and their forms are used for solving numerous problems. Some of them are as follows:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

1) Row Matrix: A row matrix has only one row but any number of columns. A matrix is said to be a row matrix if it has only one row.

2) Column Matrix: A column matrix has only one column but any number of rows. A matrix is said to be a column matrix if it has only one column.

3) Square Matrix: A square matrix has the number of columns equal to the number of rows. A matrix in which the number of rows is equal to the number of columns is said to be a square matrix. Thus an m × n matrix is said to be a square matrix if m = n and is known as a square matrix of order n.

4) Rectangular Matrix: A matrix is said to be a rectangular matrix if the number of rows is not equal to the number of columns.

5) Diagonal matrix: A square matrix $B = [b_{ij}]_{m\times m}$ is said to be a diagonal matrix if all its non-diagonal elements are zero, that is a matrix $B = [b_{ij}]_{m\times m}$ is said to be a diagonal matrix if $b_{ij} = 0$, when $i \neq j$.

6) Scalar Matrix: A diagonal matrix is said to be a scalar matrix if all the elements in its principal diagonal are equal to some non-zero constant. A diagonal matrix is said to be a scalar matrix if its diagonal elements are equal, that is, a square matrix $B = [b_{ij}]_{n\times n}$ is said to be a scalar matrix if

- $b_{ij} = 0$, when $i \neq j$
- $b_{ij} = k$, when $i = j$, for some constant k.

7) Zero or Null Matrix

A matrix is said to be zero matrix or null matrix if all its elements are zero.

8) Unit or Identity Matrix

If a square matrix has all elements 0 and each diagonal elements are non-zero, it is called identity matrix and denoted by *I*.

Equal Matrices: Two matrices are said to be equal if they are of the same order and if their corresponding elements are equal to the square matrix $A = [a_{ij}]_{n \times n}$ is an identity matrix if:

- $a_{ij} = 1$ if $i = j$
- $a_{ij} = 0$ if $i \neq j$

We denote the identity matrix of order *n* by In. When the order is clear from the context, we simply write it as *I*.

9) Upper Triangular Matrix: A square matrix in which all the elements below the diagonal are zero is known as the upper triangular matrix.

10) Lower Triangular Matrix: A square matrix in which all the elements above the diagonal are zero is known as the upper triangular matrix.

2.4.2 Operations with Matrices

1) Matrix addition: If $A[a_{ij}]_{mxn}$ and $B[b_{ij}]_{mxn}$ are two matrices of the same Order then their sum $A + B$ is a matrix, and each element of that matrix is

the sum of the corresponding elements. i.e. $A + B = [a_{ij} + b_{ij}]_{mxn}$.

Example (2.2) : $\begin{bmatrix} 2 & 1 \\ -3 & 5 \end{bmatrix} + \begin{bmatrix} 7 & 9 \\ 4 & 13 \end{bmatrix} = \begin{bmatrix} 9 & 10 \\ 1 & 18 \end{bmatrix}$

2) Subtraction of Matrices:

If A and B are two matrices of the same order, then we define $A-B=A+(-B)$.

Example(2.3): Let $A = \begin{bmatrix} 6 & 3 \\ 1 & 5 \end{bmatrix}$ and $B = \begin{bmatrix} 5 & 2 \\ 4 & 4 \end{bmatrix}$ find $A - B, B - A$

$$A - B = \begin{bmatrix} 6 & 3 \\ 1 & 5 \end{bmatrix} - \begin{bmatrix} 5 & 2 \\ 4 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ -3 & 1 \end{bmatrix}$$

$$B - A = \begin{bmatrix} 5 & 2 \\ 4 & 4 \end{bmatrix} - \begin{bmatrix} 6 & 3 \\ 1 & 5 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 3 & -1 \end{bmatrix}$$

$$A - B \neq B - A$$

3) Scalar multiplication: A matrix can be multiplied by a scalar as follows. If $A = [aij]$ is a matrix and k is a scalar, then $kA=[ka_y]$.That is, the matrix kA is obtained by multiplying each entry of A by k.

4) Matrix multiplication: By far the most important operation involving matrices is matrix multiplication, the process of multiplying one matrix by another. The first step in defining matrix multiplication is to recall the definition of the dot product of two vectors. Let r and c be two n-vectors. Writing r as a 1 x n row matrix and c as an n x 1 column matrix, the dot product of r and c is

$$r.c = [r_1 r_2 \dots r_n].\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = r_1c_1 + r_2c_2 + \cdots + r_nc_n$$

Example (2.4) :

$$[-3 \quad 2 \quad 0 \quad -1 \quad -1\ ]\begin{bmatrix} -7 \\ -2 \\ 9 \\ -1 \\ 8 \end{bmatrix}$$=(-3)(-7)+(2)(-2)+(0)(9)+(-1)(-1)+(-1)(8)=10

Example (2.5) : Let$A = \begin{bmatrix} 1 & 0 & -3 \\ -2 & 4 & 1 \end{bmatrix}$ $and\ B = \begin{bmatrix} 2 & -1 \\ 3 & 0 \\ -5 & 2 \end{bmatrix}$

verify that

$$AB = \begin{bmatrix} 1 & 0 & -3 \\ -2 & 4 & 1 \end{bmatrix}\begin{bmatrix} 2 & -1 \\ 3 & 0 \\ -5 & 2 \end{bmatrix} = \begin{bmatrix} 17 & -7 \\ 3 & 4 \end{bmatrix}$$

$$BA = \begin{bmatrix} 2 & -1 \\ 3 & 0 \\ -5 & 2 \end{bmatrix}\begin{bmatrix} 1 & 0 & -3 \\ -2 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 4 & -4 & -7 \\ 3 & 0 & -9 \\ -9 & 8 & 17 \end{bmatrix}$$

$AB \neq BA$

2.4.3 The inverse of a matrix: Let *a* be a given real number. Since 1 is the multiplicative identity in the set of real numbers, if a number *b* exists such that

ab=*ba*=1,then b is called the reciprocal or multiplicative inverse of a and denoted a^{-1} (or $1/a$). The analog of this statement for square matrices reads as follows. Let *A* be a given *n x n* matrix. Since $I = I_n$ is the multiplicative identity in the set of n x n matrices, if a matrix *B* exists such that :*AB*=*BA*=*I*

then B is called the (multiplicative) inverse of A and denoted A^{-1} (read A inverse).

Example (2.6): If $A = \begin{bmatrix} 2 & 3 \\ 5 & 8 \end{bmatrix}$ then $A^{-1} = \begin{bmatrix} 8 & -3 \\ -5 & 2 \end{bmatrix}$

Since $A\,A^{-1} = \begin{bmatrix} 2 & 3 \\ 5 & 8 \end{bmatrix}\begin{bmatrix} 8 & -3 \\ -5 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

And $A^{-1}A = \begin{bmatrix} 8 & -3 \\ -5 & 2 \end{bmatrix}\begin{bmatrix} 2 & 3 \\ 5 & 8 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

2.4.4 Solving Systems of Linear Equations Using Matrices

Matrices are useful for solving systems of equations. We have seen how to write a system of equations with an augmented matrix, and then how to use row operations and back-substitution to obtain row-echelon form. Now, we will take row-echelon form a step farther to solve a 3 by 3 system of linear equations. The general idea is to eliminate all but one variable using row operations and then back-substitute to solve for the other variables.

Example (2.7): Solve the system of linear equations using matrices.

$x - y + z = 8$

$2x+3y - z = -2$

$3x - 2y - 9z = 9$

Solution: First, we write the augmented matrix.

$$\begin{bmatrix} 1 & -1 & 1 & 8 \\ 2 & 3 & -1 & -2 \\ 3 & -2 & -9 & 9 \end{bmatrix}$$

Next, we perform row operations to obtain row-echelon form.

$$-2R_1 \quad + \quad R_2 = \quad R_2 \rightarrow \begin{bmatrix} 1 & -1 & 1 & 8 \\ 0 & 5 & -3 & -18 \\ 3 & -2 & -9 & 9 \end{bmatrix}$$

$$-3R_1 \quad + \quad R_3 = \quad R_3 \rightarrow \begin{bmatrix} 1 & -1 & 1 & 8 \\ 0 & 5 & -3 & -18 \\ 0 & 1 & -12 & -15 \end{bmatrix}$$

The easiest way to obtain a 1 in row 2 of column 1 is to interchange R_2 and R_3

interchange R_2 and R_3 $\rightarrow \begin{bmatrix} 1 & -1 & 1 & 8 \\ 0 & 1 & -12 & -15 \\ 0 & 5 & -3 & -18 \end{bmatrix}$

Then

$$-5R_2 + R_3 = R_3 \rightarrow \begin{bmatrix} 1 & -1 & 1 & 8 \\ 0 & 1 & -12 & -15 \\ 0 & 0 & 57 & 57 \end{bmatrix}$$

$$\frac{-1}{57} R_2 = R_3 \rightarrow \begin{bmatrix} 1 & -1 & 1 & 8 \\ 0 & 1 & -12 & -15 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

The last matrix represents the equivalent system.

$x - y + z = 8$

$y - 12z = -15$

$z = 1$

Using back-substitution, we obtain the solution as (4,−3,1).

Example (2.8): Solve the system of linear equations using matrices.

- x + y + z = 6
- 2y + 5z = −4
- 2x + 5y − z = 27

Solution:

They could be turned into a table of numbers like this:

$$\begin{array}{ccccc} 1 & 1 & 1 & = & 6 \\ 0 & 2 & 1 & = & -4 \\ 2 & 5 & -1 & = & 27 \end{array}$$

We could even separate the numbers before and after the "=" into:

$$\begin{array}{ccc} 1 & 1 & 1 \\ 0 & 2 & 5 \\ 2 & 5 & -1 \end{array} \quad \text{And} \quad \begin{array}{c} 6 \\ -4 \\ 27 \end{array}$$

Now it looks like we have 2 Matrices.

In fact we have a third one, which is [x y z]:

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 5 \\ 2 & 5 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 6 \\ -4 \\ 27 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 5 \\ 2 & 5 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x + y + z \\ 2y + 5z \\ 2x + 5y - z \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 5 \\ 2 & 5 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 6 \\ -4 \\ 27 \end{bmatrix}$$

Like this: Ax=B

where

A is the 3x3 matrix of *x* ,*y* and *z* coefficients

X is *x* ,*y* and *z* ,*and B is* 6 , -4 ,27

Then (as shown on the inverse of a Matrix page) the solution this :

$X = A^{-1}B$

It means that we can find the values of *x*, *y* and *z* (the *X* matrix) by multiplying the inverse of the *A* matrix by the *B* matrix

So let's go ahead and do that:

First , we need to find the inverse of the *A* matrix (assuming it exists)

Using the matrix calculator we get this :

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 5 \\ 2 & 5 & -1 \end{bmatrix}^{-1} = \frac{1}{-21}\begin{bmatrix} -27 & 6 & 3 \\ 10 & -3 & -5 \\ -4 & -3 & 2 \end{bmatrix}$$

Then multiply A^{-1} by B (we can use the Matrix Calculator again):

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \frac{1}{-21}\begin{bmatrix} -27 & 6 & 3 \\ 10 & -3 & -5 \\ -4 & -3 & 2 \end{bmatrix}\begin{bmatrix} 6 \\ -4 \\ 27 \end{bmatrix} = \frac{1}{-21}\begin{bmatrix} -105 \\ -63 \\ 42 \end{bmatrix} = \begin{bmatrix} 5 \\ 3 \\ -2 \end{bmatrix}$$

And we are done the solution is : x=5 ,y=3 ,z=-2

2.5 Cryptosystems Overview

Cryptographic algorithms play an important role in securing information through many paths of communication. These algorithms have a great significance and usefulness for senders and receivers to perform various missions when using network. Furthermore , by using such algorithms , it is possible to perform many tasks , especially in regard with encrypting , decrypting, authenticating data/ information and providing protection to communications and information from any threat carried out by intruders. Technically speaking, these algorithms can be divided into symmetric algorithms and asymmetric algorithms, which are designed to achieve security metrics for the categories listed can be illustrated as in figure (2.1).

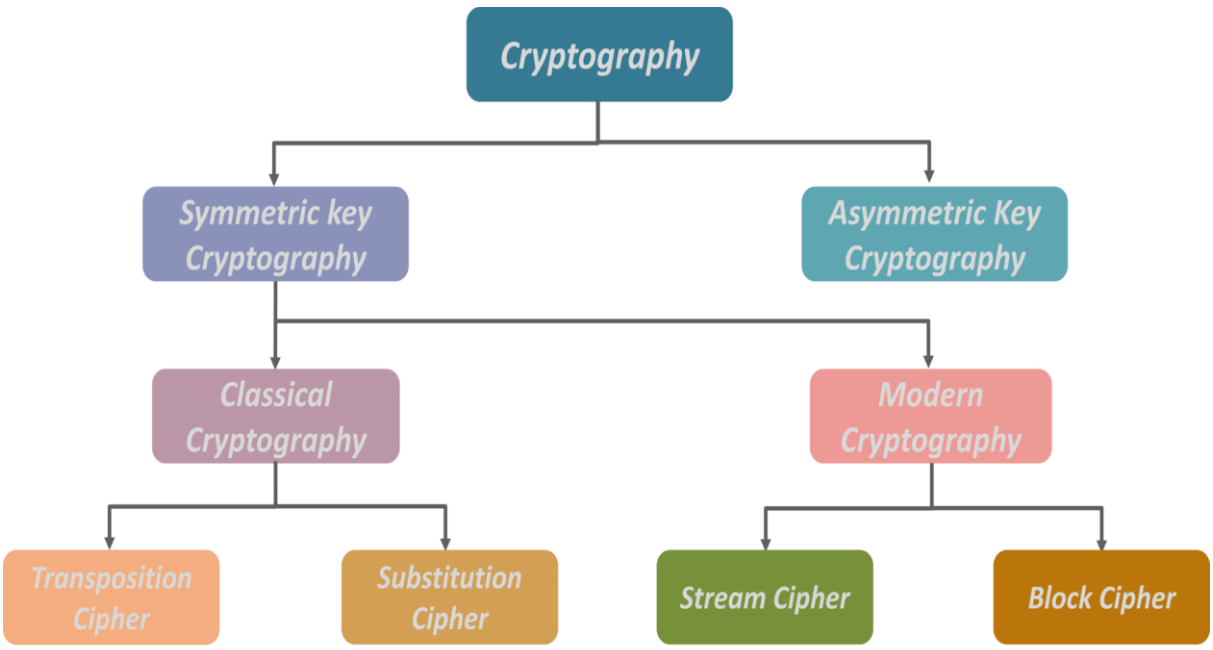

Figure (2.1) classified Cryptographic Algorithms

Figure (2.2) shows the encryption security categories. The cryptographic algorithms' five basic objectives are to ensure that data and information secured enough from malicious attackers .

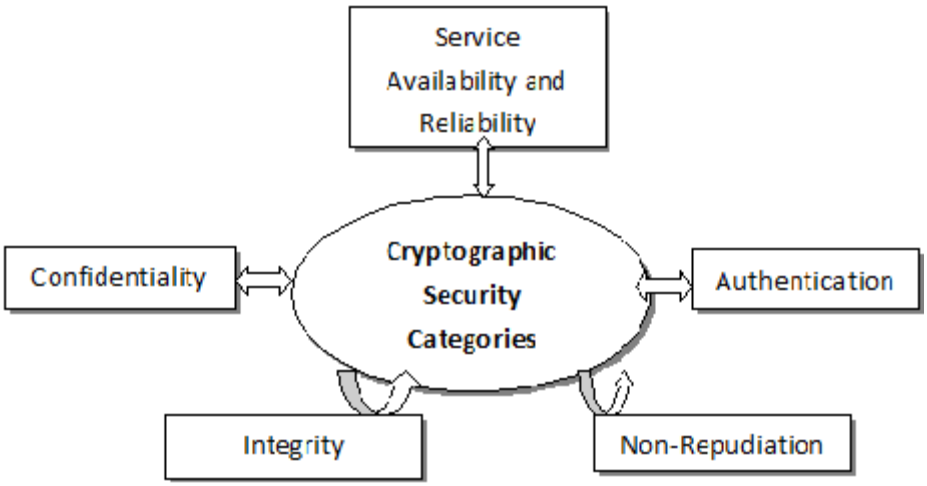

Figure 2.2: Cryptographic Security Categories

Chapter Three

Knapsack Cipher and three pass protocol

Chapter Three

Knapsack Cipher and TPP

3.1 Introduction

This chapter contains an introduction to the mathematical form of the knapsack cipher with a detailed example and the basics of Markel-Hellman. Finally, a detailed explanation to three pass protocol, with security and authentication

3.2 Knapsack Problem Introduction

The knapsack problem can be used as public key cryptosystem[**3**] and this encryption needs two different keys. One is for Encrypting, which is called public key, and the other is for decrypting process, which is called private key[**4**]. In this system of knapsack, decryption key cannot be found from encryption key. Knapsack is described as a given set of items where each of them has a weight and value. Therefore, total weight is less than some given weight and total value is as large as possible. Studying knapsack problem has started since 1897. The name "knapsack problem" goes back to the mathematician's early works, Tobias Danzig, (1884–1956), its name indicates to the common problems when packing the most expensive or useful items without having to overweight the luggage.

3.3 Knapsack Cryptosystem

The security of knapsack cryptosystem are whose depend upon the robustness of the knapsack cipher. These types of systems are still not very popular since simple versions of those algorithms have not

offered much confidentiality[3]. Moreover, the best-known knapsack encryption system is the Merkle-Hellman Public Key, which was one of the earliest public key encryption systems and was published by Ralph Merkle and Martin Hellman in 1978**[4].**Hellman invented the first knapsack cipher system. Since the original Merkel-Hellman knapsack system was proposed, there have been many variations of the cipher system suggested. However, as expected many cryptanalysis attacks have been found to defeat such ciphers. A polynomial time attack was published by Adie Shamir in 1984. As a result, this is now considered insecure. All knapsack cryptosystems are an attempt to hide the basis of the knapsack using smart transformations and transformations that distinguish one knapsack cryptosystem from another and by means of which the attempt is made to defeat the various crypto analytic techniques. Each knapsack cryptosystem has its own special technique for defeating the various known cryptanalytic techniques.

3.3.1 Basic Markel-Hellman Knapsack Cryptosystem

The Merkel and Hellman suggested this idea using the elements of the public key are modular multiples of super increasing sequence, to construct knapsack cipher system as the following:

Step(1) Selecting block of size *n* as a super-increasing sequence of positive integers [**23**].

Step(2) Choose random integer q , q>$\sum_{i=1}^{n} Si$.

Step(3) Choose a random integer r such that gcd (r ,q)=1.

Step(4) Calculate sequence $B = (b_1, b_2, \ldots, b_n)$ where $bi = rsi \bmod q$…(3.1) private key is (s ,q ,r) and Public-key is B.

3.3.2 Encryption Process

Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography[26]. Let m be contains an n-bit message consisting of bits $m_1,m_2,\ldots,m_n$ Where m_i is in the binary form, then the text of the message is multiplied by the public key to convert it to the cipher text.

$C=\sum_{i=1}^{n} mi\ bi$,(C is the ciphertext) …(3.2)

Knapsack cryptosystem can provide a brilliant way to create public key and private key.

Encryption has been a longstanding way for sensitive information to be protected. Historically, it was used by militaries and governments.

In modern times, encryption is used to protect data stored on computers and storage devices, as well as data in transit over networks.

3.3.3 The Complete Algorithm for the Knapsack Cipher

```
Knapsack (v, w, n, W)
for (w=0 to W)V[0,w]=0;
for(i=1 to n)
for(w=0 to W)
if ((w[i]≤w) and (v[i]+v[i-1,w-w[i]]> v[i-1,w]))
v[i,w]=v[i]+ v[i-1,w-w[i];
keep[I,w]=1;
else
v[I,w]=v[i-1,w];
keep[I,w]=0;
k=W
for(i=n do w n to1)
if(keep[I, k]= =1
```

output I;

k=k-w[i];

return v [n,W] ;

Example (3.1) take the message **"TAHA"**

Suppose that the user employs the super increasing sequence S=(3,5,11,20,41), taking q=85 and r=44,each knapsack item is multiplied by a and reduced modulo m to produce the public key in listed enciphering key . As shown in the table (3.1)

44x3mod 85=47

44x5 mod 85=50

44x11mod 85=59

44x20 mod 85=30

44x41 mod 85=19

The public key B=(47,50,59,30,19)

The letters of the message must be converted to the corresponding correct setting, and then to the binary as in table (3.1)

Table (3.1) : The letters and the corresponding binary numbers

Letter	Integers corresponding to Letters	Binary equivalent	Letter	Integers corresponding to Letters	Binary equivalent
A	1	00001	N	14	01110
B	2	00010	O	15	01111
C	3	00011	P	16	10000
D	4	00100	Q	17	10001
E	5	00101	R	18	10010
F	6	00110	S	19	10011
G	7	00111	T	20	10100
H	8	01000	U	21	10101
I	9	01001	V	22	10110
J	10	01010	W	23	10111
K	11	01011	X	24	11000
L	12	01100	Y	25	11001
M	13	01101	Z	26	11010

T=10100

A= 00001

H=01000

A=00001

Then the binary numbers corresponding to the letters of the message are multiplied by the public key to be encrypted.

10100(47,50,59,30,19)=1*47+0*50+1*59+0*30+0*19=106

00001(47,50,59,30,19)=0*47+0*50+0*59+0*30+1*19=19

01000(47,50,59,30,19)=0*47+1*50+0*59+0*30+0819=50

00001(47,50,59,30,19)=0*47+0*50+0*59+0*30+1*19=19

Binary code $A_i=(a_1,a_2,a_3,a_4,a_5)$, $C_i=A_i*B$ then C=(106,19,50,19).Table (3.2) cipher text using knapsack algorithm.

Table (3.2) :The knapsack encrypt

Letters	Integers Corresponding To letters	Binary	Knapsack	Cipher text "C.T"
T	20	10100	10100(47,50,59,30,19)	106
A	1	00001	00001(47,50,59,30,19)	19
H	8	01000	01000(47,50,59,30,19)	50
A	1	00001	00001(47,50,59,30,19)	19

3.3.4 Decryption Process

Decryption: is to take the encrypted texts and convert them back to plaintext, which can be read or understood weather by human or computer. Moreover, it is possible to explain how data is manually decrypted or by using the proper codes or keys to converting it into plaintext. To demonstrate this, we take the previous example to decipher it. The decryption process is done as follows:

1) We find r^{-1}, which is multiplicative inverse of a mod q such that $r \times r^{-1} \bmod q = 1$

r=44 , mod85

Input r=44,q=85

Output 29,since(44x29)mod85=1

29 is modulo inverse of 44(under 85)

2) multiplying 29 with each block of cipher text , taking modulo 85.

29x106 mod 85=14Then, we will have to make the sum of 14 from the values of private key (3, 5, 11, 20, 41) i.e 3+11=14 , making that corresponding bits 1 and others 0 which is 100100. Similarly,

29 x 19 mod85 = 41

41=00001=A

And, 29x50 mod85 = 5

5 = 01000 =H

And,29x19mod85=41

41=00001=A

The result of this steps in this example as in the table(3.3)

Table (3.3) : The knapsack decryption

Cipher text(C.T)	multiply by r^{-1}modq	The resulting	Compared with S=(3,5,11,20,41)	Plain text(P.T)
106	106x29 mod 85	14	10100	T
19	19x29 mod 85	41	00001	A
50	50x29 mod 85	5	01000	H
19	19x29 mod 85	41	00001	A

When the Knapsack Algorithm is used in public key cryptography, the idea is to create two different knapsack problems. One is easy to solve, the other

not. Using the easy knapsack, the hard knapsack is derived from it. The hard knapsack becomes the public key. The easy knapsack is the private key. The public key can be used to encrypt messages, but cannot be used to decrypt messages. The private key decrypts the messages. Note this in figure (3.1)

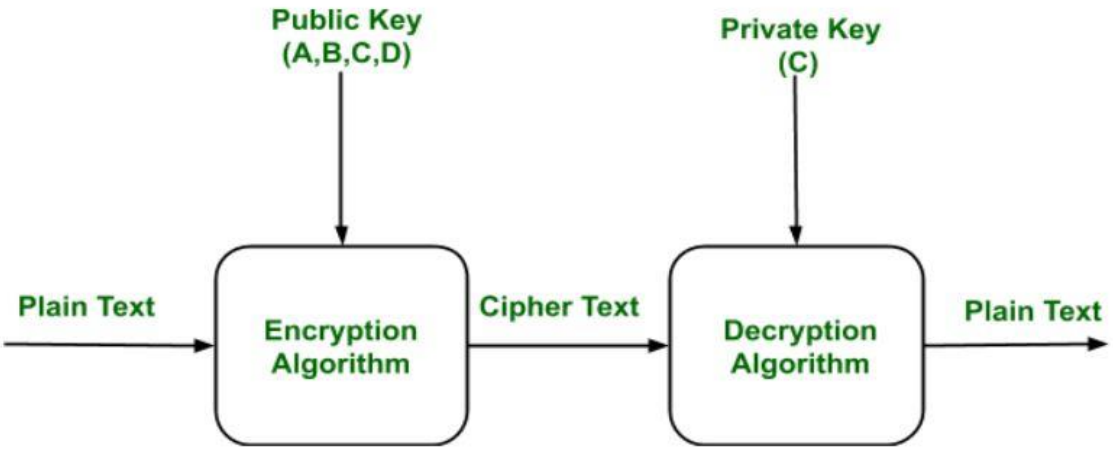

Figure (3.1): The Implementation Of Encryption and Decryption Keys of Knapsack

3.4 Three Pass Protocol(TPP)

In cryptography TPP of sending information/data is a framework allowing the senders to securely sending messages to receiver needless to perform the process of exchanging key between the two parties. Encrypt function E and decrypt function D are used by this protocol. The encrypt function employs an encrypt key E for changing message (plain-text) m to a ciphertext= $E_A(m)$. For each encryption key E, there would be a decrypt key D allowing to retrieve the messages by the use of the function of decryption D(E(m))=m, the functions of decryption and encryption can often be the same . Both decryption and encryption functions should have the properties of any message m, any key of encryption E with consistent

decrypt key D and any independent key of encryption E, $D_A (E_B(E_A (m)))$ $=E_B(m)$, to be appropriate to TPP .To put it in another way. Even if although a second encryption is performed using the key k, it must be possible to eliminate the first encryption using key E. This can occur by the mean of using a commutative encryption. it is an order-independent encryption, i.e. it fulfills $E_B(E_A(m))$ to the whole keys of encryption B and A the whole messages m. it also satisfies $D(E_B(E_A (m)))$ $=D(E_A(E_B(m)))$ [**25**].

TPP Algorithm is as the follows:

1) The sending party selects a private key of encrypting E_A and a matching key of decrypting D_A. The sending party, by the use of key E_A, can encrypt the message m and send the message encrypted E_A (m) to the receiving party .

2) The receiving party selects a private key of encrypting E_B and a matching key of decrypting D_B. The receiving party , by the use the key E_B , can encrypt the 1^{st} message $E_B(E_A$ (m))) and send back the message double- encrypted to the sending party .The sending party , by the use of the key D_A , can decrypt the 2^{nd} message due to the property of commutative abovementioned $D_A(E_B(E_A$ (m)))= $E_B(m)$, encrypting massage using only private key of the receiving party . The sending party can send this to the receiving party . therefore , the receiving party is capable of decrypting the message by the use of key D_B, to be precise, $D_B(E_B(m))=m$ the original message. The TPP process can be illustrated in figure(3.3).

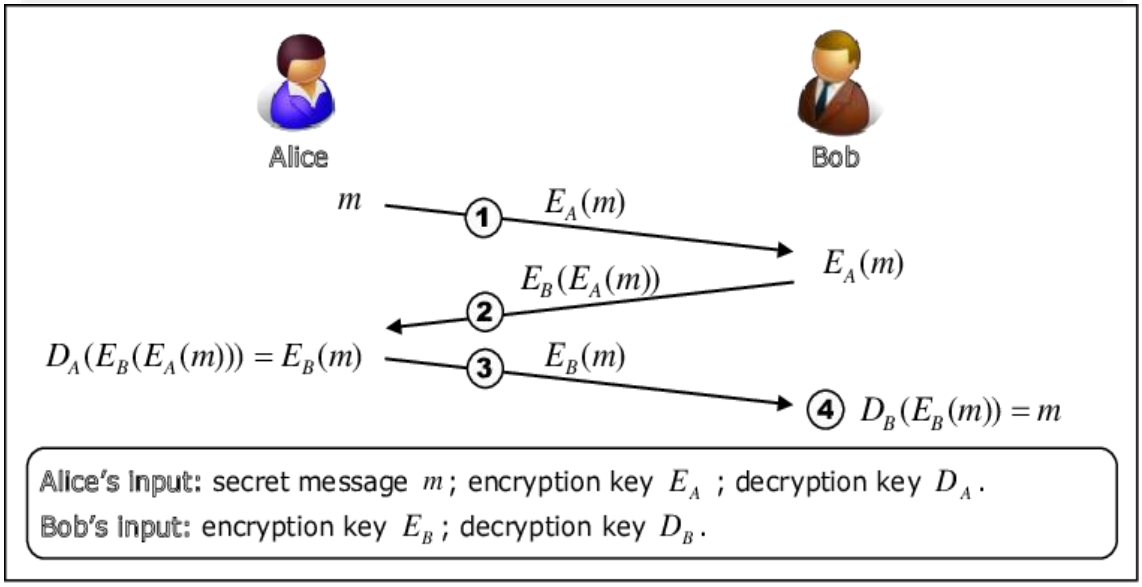

Figure (3.2): Three Pass Secret Exchange Protocol

3.5 Security of TPP

Data Security is essential in the process of sending messages one of the most common used data is cryptographic security. However, it is possible to divide cryptography to classical and modern cryptography[**26**].TPP can be categorized as a modern technique of cryptography . TPP cannot be secure enough unless it fulfills the most essential requirement ,namely , attacker's incapability of detecting any information related massage *m* from the three massages that are transmitted E(s ,m) , E(r, E(s ,m)) and E(r ,m). See figure (3.3).

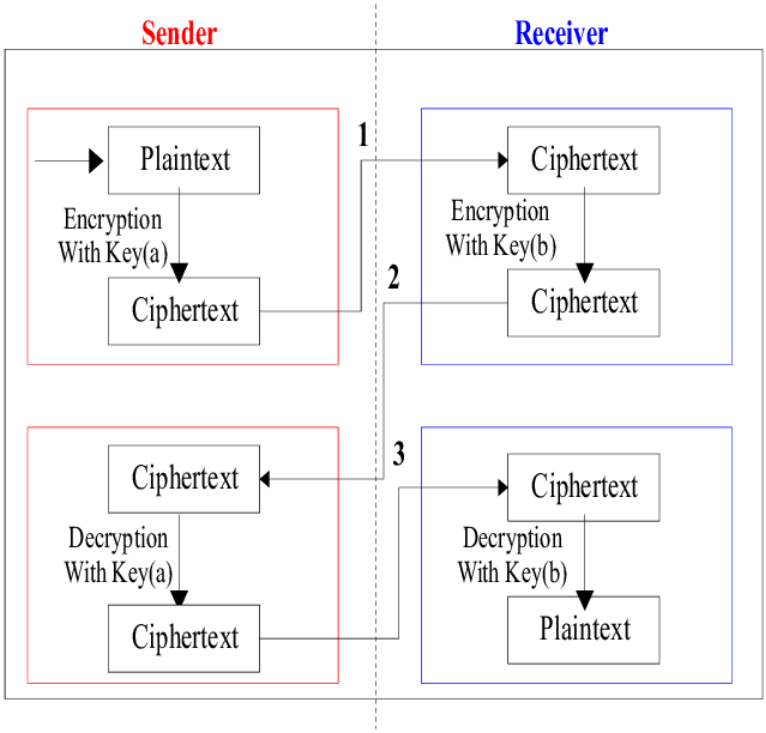

Figure (3.3): Three Pass Protocol Process Scheme

Note that the whole processes that involve the private key of the sending party *s* and *t* were conducted by the sending party ,and the whole processes that involve the private key of the receiving party *r* and *q* were conducted by the receiving party , therefore ,the sender and the receiver does not needs knowing the keys of the other party.

3.6 Authentication TPP Implementation

Authentications the process of proving an assertion, that is to say, a process of recognizing a user's identity, like a user identity of computer system. Unlike identification, which represents the process indicating identity of an individual or thing, authentication is the verification process of this identity[**27**]. It may require checking documents related to personal identity, the website authenticity using a digital certificate [28], determinant-ion artifact age by the use of carbon dating, or making sure

that document are not bogus.TPP , as above-explained, provides no authentication **[29]**.

Therefore, with no extra authentication, the protocol can be susceptible to malicious attacks such as (MitM) attack if the attacker is capable of generating false messages, or intercepting and replacing the original messages transmitted.

3.6.1 TPP Implementation on Caesar Cipher

Security of data is needed in the process of sending messages [**30**]. Cryptographic security is one of the frequently used data. Classical cryptography is an algorithm that uses a key for secure data and the process is very easy to use. However, it is already old fashioned because it is considered weak in data security. where the Caesar Cipher algorithm that is by changing the position of the initial letter of the alphabet or also called ROT algorithm [**31**].This technique is also known as a single cipher alphabet. The core of these cryptographic algorithms is shifting towards all the characters in plaintext with the same shift value. The steps taken to establish ciphertext with Caesar Cipher is Determine the magnitude of the shift characters used in forming the ciphertext to plaintext and Redeeming the characters in plaintext into ciphertext with based on a predetermined shift.

The main goal to use classical Caesar cipher algorithm with TPP is to strengthen the security of the data[**32**].

Example(**3.2**) In this example we demonstrated the implementation TPP in Caesar's algorithm, using the following steps:

1) We put an incoming text " REMEMBER THE PRIVATE PASSWORD" as a plaintext.

2) The shifts value is 5.

3) The encryption process takes two times.

4) First time, the sender conducts massage encryption.

5) Second time, the receiving party conducts massage encryption when a massage reaches. Table (3.4) illustrates this process.

Table (3.4): The first round of encryption using Caesar Cipher

PT	R	E	M	E	M	B	E	R
CT_1	W	J	R	J	R	G	J	W
PT	T	H	E					
CT_1	Y	M	J					
PT	P	R	I	V	A	T	E	
CT_1	U	W	N	A	F	Y	J	
PT	P	A	S	S	W	O	R	D
CT_1	U	F	X	X	B	T	W	I

6) In Table (3.5) we will notice the process of encrypting incoming text happens by the use of Caesar Cipher. And the process of encrypting will produce “WJRJRGJW YMJ UWNAFYJ UFXXBTWI” as the cipher text.

Table (3.5): The 2'nd round of encryption using Caesar Cipher

CT_1	W	J	R	J	R	G	J	W
CT_2	A	N	V	N	V	K	N	A
CT_1	Y	M	J					
CT_2	C	Q	N					
CT_1	U	W	N	A	F	Y	J	
CT_2	Y	A	R	E	J	C	N	
CT_1	U	F	X	X	B	T	W	I
CT_2	Y	J	B	B	F	X	A	M

7) Table (3.6) illustrates the 2nd round of the encrypting process by the use shift value 4. The last cipher text is "ANVNVKNA CQN YAREJCN YJBBFXAM" .It is the final set of the process of encrypting. For reading the message, the sender and the receiver should decrypt the last cipher text two times .

Table (3.6) : The 1st round of decryption using Caesar cipher

CT_2	A	N	V	N	V	K	N	A
CT_3	V	I	Q	I	Q	F	I	V
CT_2	C	Q	N					
CT_3	X	L	I					
CT_2	Y	A	R	E	J	C	N	
CT_3	T	V	M	Z	E	X	I	
CT_2	Y	J	B	B	F	X	A	M
CT_3	T	E	W	W	A	S	V	H

7) Table (3.7) show the 1st process of decrypting . It continues producing the format of cipher text because the text is not readable .This cipher text requires to be sent to the receiving party over again to be totally readable . Table (3.7) illustrates the final process of decrypting to the whole process.

Table (3.7): The 2'nd round of decrypting using Caesar cipher

CT_3	V	I	Q	I	Q	F	I	V
PT	R	E	M	E	M	B	E	R
CT_3	X	L	I					
PT	T	H	E					
CT_3	T	V	M	Z	E	X	I	
PT	P	R	I	V	A	T	E	
CT_3	T	E	W	W	A	S	V	H
PT	P	A	S	S	W	O	R	D

Classical cryptography considered the 1st generation of cryptography dealing with the mechanism of making text(s) unreadable, but , based upon the algorithm it follows ,its system is characterized of having vulnerability regarding any malicious data attacks. Furthermore ,through the combination process of both TPP and traditional cryptography, the resulting ciphertext can be protected . The data sending process does not require to key-sharing the message sender. Despite of being susceptible to various types of attacks, some people still use classical cryptography.

3.6.2 TPP Concept in Hill Cipher (HC)

Lester Hill , the American mathematician, invented Hill Cipher (HC) in 1920s [**34**] and it was widely -known algorithm because it is simple and of highly throughputs [**35**]. It uses matrices in encryption, the smallest matrix to use is 2x2 mod 26 can be produced in the cipher text by providing key as the determinant, we can use a matrix larger than 2x2, but our difficulty lies in finding the inverse of that matrix. In HC , we could , randomly, choose the integers (A = 0, B = 1, …, Z = 25), for keys beforehand , But, the provided key ,occasionally, won't work. that occurs when decrypting the cipher text back to plaintext . Produced plaintext is dissimilar from the original message, there for before selecting encryption keys in advance , we must test that if it contains the right determinant. And if it does, it is possible to apply the inverse key on the cipher text when decryption happens. It is necessary to send the key to someone in charge of decrypting massages since we use it as a password for modifying massage. It is imperative to distribute the keys, and at that moment a third party may intervene to intercept the text and can be broken.

TPP is the most common method to minimize attacks by interceptors[**36**]. When applying this algorithm, it is very necessary to modify the matrix formula, there are some modifications to Hill Cipher parts for making the two algorithms function together. in this system, either sending party or receiving party encrypts and decrypts by using his own keys matrix separately , with no need to share these keys with the other party , an attacker cannot obtain the key because the two parties keep them securely. Therefore, transmission of the information using this technique can be more secured.

Example(3.3): The description of a TPP method will be shown in HC

Choose Plaintext :STOP:

$\begin{pmatrix}18 & 14\\19 & 15\end{pmatrix}$ ...(1)

Key $_1$:$\begin{pmatrix}3 & 6\\4 & 9\end{pmatrix}$ key of Sender

Key $_2$:$\begin{pmatrix}3 & 2\\3 & 5\end{pmatrix}$ key of receiver

Inverse key: Now, we can prove that the provided keys are invertible.

Key $_1$:$\begin{pmatrix}3 & 6\\4 & 9\end{pmatrix}$

Determinant : (3 * 9- 6* 4) mod 26 =3

(D ≠ 0 and D ≠ Even)

3^{-1}mod 26=9

9* $\begin{pmatrix}9 & -6\\-4 & 3\end{pmatrix}$mod 26 =$\begin{pmatrix}81 & -54\\-36 & 27\end{pmatrix} mod\ 26 = \begin{pmatrix}3 & 24\\16 & 1\end{pmatrix}$= Key_1^{-1}…(2)

Key 2 :$\begin{pmatrix}3 & 2\\3 & 5\end{pmatrix}$

Determinant : (3*5-3*2) mod 26 =9

(D ≠ 0 and D ≠ Even)

9^{-1}mod 26=3

3$\begin{pmatrix}5 & -2\\-3 & 3\end{pmatrix} mod 26 \begin{pmatrix}15 & -6\\-9 & 9\end{pmatrix} mod\ 26 \begin{pmatrix}15 & 20\\17 & 9\end{pmatrix}$=$Key_2^{-1}$ …(3)

it is possible to use Key_1andKey_2 as the key pair in Hill Cipher.

Encryption (1)

$C_1=K_1*P$

C_1 =: $\begin{pmatrix}3 & 6\\4 & 9\end{pmatrix} * \begin{pmatrix}18 & 14\\19 & 15\end{pmatrix} = \begin{pmatrix}12 & 2\\9 & 9\end{pmatrix}$

(Cipher text(1)) ^{T} $=\begin{pmatrix}12 & 9\\ 2 & 9\end{pmatrix}$(4)

Encryption (2)

$C_2=K_2*C_1$

(Cipher text(1)) ^{T} $=\begin{pmatrix}12 & 9\\ 2 & 9\end{pmatrix}$

Cipher text (2) : $\begin{pmatrix}3 & 2\\ 3 & 5\end{pmatrix} * \begin{pmatrix}12 & 9\\ 2 & 9\end{pmatrix}$

(Cipher text (2)) ^{T} $=\begin{pmatrix}14 & 20\\ 19 & 20\end{pmatrix}$final encryption(5)

Decryption(1)

(C_2) ^{T} $=\begin{pmatrix}14 & 20\\ 19 & 20\end{pmatrix}$

Cipher text (3) : $\begin{pmatrix}3 & 24\\ 16 & 1\end{pmatrix} * \begin{pmatrix}14 & 20\\ 19 & 20\end{pmatrix}$

$C_3=K_1^{-1}C_2$

(Cipher text (3)) ^{T} $=\begin{pmatrix}4 & 9\\ 20 & 2\end{pmatrix}$(6)

Decryption(2)

(Cipher text (3)) ^{T} $=\begin{pmatrix}4 & 9\\ 20 & 2\end{pmatrix}$

$P=K_2^{-1}C_3$

Plaintext: $\begin{pmatrix}15 & 20\\ 17 & 9\end{pmatrix} * \begin{pmatrix}4 & 9\\ 20 & 2\end{pmatrix}$

Plaintext = $\begin{pmatrix}18 & 19\\ 14 & 15\end{pmatrix}^{T}$

$$(\text{Plaintext})^{T} = \begin{pmatrix} 18 & 14 \\ 19 & 15 \end{pmatrix} \quad ...(7)$$

$(\text{Plain text})^{T}$ represents the ultimate result of the decrypting process of the two methods. Each party is required to make two phases of computation where the sending party performs the decryption and decryption processes .

Table (3.8) illustrates the entire tasks of decryption and encryption operations, The sentence is "STOP".

Table (3.8): Sample of TPP In Hill Cipher

No	PT	CT1	CT2	CT3	P
1	18	12	14	4	18
2	19	9	20	9	19
3	14	2	19	20	14
4	15	9	20	2	15

3.6.3 TPP Implementation in Vigenere Cipher

Vigenere Cipher is a method for encoding the text of the alphabet. It uses a simple poly- alphabetic substitution form. It is a cipher based on replacement, using several substitution letters [**36**]. The Vigènere code is a poly alphabetic replacement cipher. It is published by a French diplomat (and also a cryptologist), Blasé de Vigènere, in the 16th century, 1586. It was first explained by Gavan Batista in the year1533, as it is written in the book La Citra del Sig. This algorithm was broadly known 200 years later and was called the code Vigènere. It was used during the civil war in America, and the Confederate Army used the Vigènere code in the

American social War. Babbage and Kasiski productively broke the vigènere code in the mid-19th century [**36**]. This kind of encryption algorithm is very well known because it is easy to know and apply. Mathematically, the equation below illustrates the encryption and decryption process Vigenere Cipher Which C represents cipher text, P represents plaintext, K represents Key, and D represents Decryption process and E represents Encrypting process.

Example (3.4) : Supposing that the plaintext " LET ME HELP YOU" with the key word "TAHA" then, according to the table (3.9) of vigènere cipher , the illustration below shows the encrypting process :

Table(3.9) : Vigenere Cipher to Encrypt

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

P: E K: A

K: A C: E

C: E P: E

For the process of decryption, with vigènere cipher table the same key is used, then plaintext resulting from comparing cipher text with keys, the alphabet is corresponding to the cipher text and the key, then the alphabet is plaintext .

Cipher text :EEA MX HLLI AVU

Key word : TAHA TAHATAHA

Plaintext : LET ME HELP YOU

The disadvantage of Vigenere cipher algorithm is when the length of key is not bigger than the length of the plaintext , the key would be repeated , since it would probably create the same encrypted text having the same length of the same plaintext. Kasiski examination (Kasiski method) is a method that breaks Vigenere Cipher , it collects the same characters of cipher text for calculating the distance for finding a number of the key length, After performing this, the following phase is to determine what the key words to use in brute-force search [**12**].

Dissimilar encryption word, it is dissimilar when decrypting without modifying the key, it is possible to encrypt the word " LET" as the word " EEA", then " ME" is equivalent to MX . This will be a vulnerability for cryptanalyst to perform cryptanalysis using Kasiski methods . Through making modification of the key, Kasiski method is more challenging to implement.

Example(3.5) (of TPP):

Let the message "LET ME HELP YOU" and key of the sender "TAHA" and key's owned by the recipient "ABED"

First Encryption by Sender:-

Plaintext :LET ME HELP YOU

Sender Key :TAHA FGQM REDX

First Cipher text: EEAM JNUX GCRR

Second encryption by recipient:-

First Cipher text : EEAM JNUX GCRR

Recipient Key : ABED XDWQ OPGS

Second cipher text :EFEPGQQNURXJ

First decryption by sender :-

Second cipher text: EFEP GQQN URXJ

Sender key :TAHA FGQM REDX

Third cipher text :LFXP BKAB DNUM

Second decryption by recipient:-

Third cipher text :LFXP BKAB DNUM

Recipient Key :ABED XDWQ OPGS

Plaintext :LET ME HELP YOU

3.6.4 TPP on RSA

RSA is an asymmetric encryption algorithm , known also as Public-key cryptography, that modern computers widely are using for encrypting and decrypting data /messages and to secure data transmission processes. Asymmetric algorithm is characterized of having two a pair of key , it uses dissimilar key in process of encrypting and decrypting[**38**]. This is simply because one of the two keys can be given to anyone without exploiting the security of the algorithm[**39**]. Therefore, it is not always suitable for every application [**40**]. To hold up the security of the asymmetric algorithm that is more secure than symmetric algorithm . a new model is proposed that combines one of the symmetric algorithms , which is RSA cryptosystem with the modern cryptography protocol. This protocol is called TPP. The structure of the protocol allows the asymmetric algorithms to send encrypted messages without distributing a public key. We will support the security of the RSA cryptosystem in the process of sending messages. The investigational results are discussed with the security and it proves that the approach functions well , and it is secure, RSA is one of the public key encryption forms. In RSA public-key encryption system, participants create their own public and secret key with the following procedures [**41].**In public-key cryptography system, the key of encryption is public and different from the key of decryption , which it should remain hidden. RSA users create and publish a public key relying upon two big prime numbers, and auxiliary value. It is very imperative to keep these numbers secret. Moreover, it is possible to anyone to encrypt messages, by using the public key, but it is impossible to decrypt massages unless he /she knows the prime numbers**.** The RSA security aspect relies on the presumed difficulty of factoring large

integers, the "factoring problem". To Break the encryption RSA is widely known as the problem of RSA**[42].**

There are dissimilar kinds of attacks on the RSA like: Guessing private key (d), Searching the Message Space, Common Modulus, Cycle Attack, Low Exponent, Finally Factoring, and Faulty Encryption, The variable N, that factors the public- key and it looks as the optimum method to crack RSA. Encryption algorithm relies on its power in some aspects. Each algorithm possesses certain features of mismatch heavily dependent on key encryption, that relies on the arrangements of, denounce" it tries to integrate the key with the texts of certain deviations.

The algorithm of RSA depends on the variable N, which consists of multiplication process to each of the P and q, which depends upon finding the variable d. Variable d is the higher value of n, variable d increases its volume, the higher values of p and q the value of d raises. This refers that the algorithm relies upon adopting the prime numbers since these numbers create a key d, relying on p and q are already prime numbers[**43**]. An interesting cryptographic protocol is the three pass protocol. The protocol is utilized in a lot of applications[**44]**,[**45**].The protocol announces that privacies could be achieved with no advance distributions of the secret key or public key. The protocol suggests that senders and receivers are connected by classical channels that guarantees that the opponents cannot be able of breaking or tampering a message but it allows the opponents to read all messages that have been sent over links. The senders and receivers are pretended to have secret-keys encryption systems which their encrypting functions E_k have the commutative properties for all plaintexts P and all keys k_s and k_R, $E_{k_s}(E_{k_R}(P))$ ...(1)

This means that the results of dual encryptions are the same whether senders first key k_s or key k_R or vice versa .The step that shows the mechanism of classical TPP Protocols explained below :

Sending party and receiving party select in a random way, their private secret keys, k_s and k_R, respectively.

The sending party encrypts P using key k_s , and then sending the resulting to receiver.

$C_1=Ek_s(P)$ ...(2)

The receiver receives C_1, deals with C_2 as plaintext and encrypted C_3 using receiver key k_R. The receiving party send the resulting back to senders.

$C_2= Ek_R(C_1)=Ek_R(Ek_s(P))$ …(3)

When receiving C_2 by the sending party , and decrypting C_2 using key k_s. Due to the commutative properties, this remove the previous encryptions by k_s and the result is.

$C_3=E^{-1}_{Ks}(Ek_R(E_{Ks}(P)))= E^{-1}_{Ks}(E_{Ks}(Ek_R(P)))= Ek_R(P)$ …(4)

Then, the sending party is sending C_3 back to receiver. The receiving party receiveC_3, and decrypting C_3 using key k_R to get plaintext P, which is sent successfully by the sender. in short, the plaintext delivers securely in a two boxes to the receivers, the receivers utilizing two keys for opening the two boxes without sharing keys for opening the two boxes, the entire steps related to the classical TPP illustrated in figure (3.5).

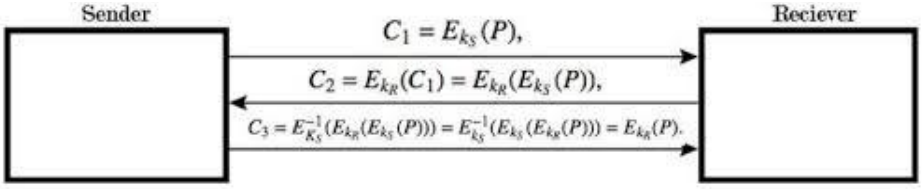

Figure (3.4): Three Pass Protocol with RSA

Chapter Four

Three Pass Protocol Implementation On Modified Knapsack Cipher

Chapter Four

TPP Implementation on Modified Knapsack Cipher

4.1 Introduction

Encryption is the process that scrambles readable text so it can only be read by the person who has the secret code, or decryption key. It helps provide data security for sensitive information. Therefore, the security of cryptographic systems and the hiding of information is related to the method of generating the keys of these systems. As a result, this thesis presents "Three pass Protocol implementation on modified knapsack Cipher" as a mathematical method for generating the keys in a proposed secure system.

4.2 Rifaat Method (TPP Implementation on Modified Knapsack Cipher)

In this method we used a three-pass protocol (TPP) with the knapsack cipher by combining them, this combination allows senders and the receivers to exchange the messages securely without need to send a public key for them, because the proposed combination protocol has this property.

The following steps are explaining the proposed new approach:

Step(1) Alice chooses a super increasing set "S_1" , multiplier$a_1$and modulus $m_1$and computing the public key$T_1$and she Encrypts the message as shown in the table (4.1) and sends first cipher text "$C.T\ 1$" to Bob.

Step(2) Bob chooses a super increasing set"S_2" , multiplier a_2 and modulus $m_2$andcomputing the public keyT_2 and $\sum_{i=1}^{n} T_2^i = \sum_{i=1}^{n} a_2 s_i$, $n \in N$, and hecomputing the cipher text "$C.T\ 2$" by

Encryption the cipher text "$C.T$ 1" secondly, and he send the cipher text "$C.T$ 2" to Alice.

Step(3) Alice takes the following steps:

1) Determines the number of elements of the recipient's public key by converting the second encrypted text into binary.

2) Compares the numbers of message element with the numbers of public key elements and adds a number of zeros to the left to message elements to ensure matching in case of unequal.

3) Identifies the items in the public key that match the 1 in the message and resends it .i.e(Alice Determine the Unwanted terms "U. T" and Wanted terms "W. T" and send the wanted terms to Bob, as showing in table (4.3).

Step(4) Bob calculates the plain text by using the wanted terms, as showing in table (4.4).

To illustrate this technique, use example(4.1)

Example(4.1)

Let the plaintext be message " TAHA ABED SHALFON " with length L=15.

Step(1) Alice chooses the set $S_1 = (2,3,6,12,24)$ and multiplier$a_1 = 5,$ and modulus$m_1 = 49$

Step(2) Alice computing the public key as follows:

2x5 mod49 =10

3x5 mod49 =15

6x5 mod 49=30

12x5 mod 49=11

24x5 mod49=22

The public key T_1= (10,15,30,11,22)

Then the message as in binary code:

1010000001010000000100001000100010100100100110100000000101100
001100111101110

Knapsack contain five weights so we needs to split the message into groups of five. This correspond L=15 set of weights with totals as follows:-

10100 (10,15,30,11,22)=10+0+30+0+0=40

00001(10,15,30,11,22)=0+0+0+0+22=22

01000(10,15,30,11,22)=0+15+0+0+0 =15

00001(10,15,30,11,22)=0+0+0+0+22= 22

00001(10,15,30,11,22)=0+0+0+0+22 = 22

00010(10,15,30,11,22)=0+0+0+11+0=11

00101(10,15,30,11,22) =0+0+30+0+22= 52

00100(10,15,30,11,22) =0+0+30+0+0=30

10011(10,15,30 11,22)=10+0+0+11+22=43

01000(10,15,30,11,22)=0+15+0+0+0=15

00001(10,15,30,11,22)=0+0+0+0+22=22

01100(10,15,30,11,22)=0+15+30+0+0=45

00110(10,15,30,11,22)=0+0+30+11+0=41

01111(10,15,30,11,22)=0+15+30+11+22=78

01110(10,15,30,11,22)=0+15+30+11+0=56

So the message that is sent will be in the following form:-

(40,22,15,22,22,11,52,30,43,15,22,45,41,78,56).This is called encrypted text, see table (4.1).

Table (4. 1): First Encryption Process

Letters	**Integers Corresponding to Letters**	**Binary**	**First Cipher text "C.T$_1$"**
T	20	10100	40
A	1	00001	22
H	8	01000	15
A	1	00001	22
A	1	00001	22
B	2	00010	11
E	5	00101	52
D	4	00100	30
S	19	10011	43
H	8	01000	15
A	1	00001	22
L	12	01100	45
F	6	00110	41
O	15	01111	78
N	14	01110	56

Step(3) Alice encrypt the message as in Table (4.1)

Step(4) In first pass protocol ,Alice send the first cipher text $C.T1 =$ (40,22,15,22,22,11,52,30,43,15,22,45,41,78,56) to Bob.

Step(5) Bob converts the cipher text it received to binary and then chooses super increasing set "S_2",

$S_2 = (1,2,4,11,19,39,81)$multiplier $a_2 = 7$ and modulus $m_2 = 173, a_2^{-1} = 99$

and calculate the public key T_2

1x7mod173=7

2x7mod173=14

4x7mod173=28

11x7mod173=77

19x7mod173=133

39x7mod173=100

81x7mod173=48

Then the public key T_2=(7,14,28,77,133,100,48)

$$and \sum_{i=1}^{7} T_2^i = \sum_{i=1}^{7} a_2 s_i = 407$$

Step(6) Bob performs the second encryption of the encryption text (C.T_1)it receives

0101000(7,14,28,77,133,100,48)=14+77=91

0010110(7,14,28,77,133,100,48)=28+133+100=261

0001111(7,14,28,77,133,100,48)=77+133+100+48=358

0010110(7,14,28,77,133,100,48)=28+133+100=261

0010110(7,14,28,77,133,100,48)=28+133+100=261

0001011(7,14,28,77,133,100,48)=77+100+48=225

1101000(7,14,28,77,133,100,48)=14+77+100=191

0011110(7,14,28,77,133,100,48)=28+77+133+100=338

0101011(7,14,28,77,133,100,48)=14+77+100+48=239

0001111(7,14,28,77,133,100,48)=77+133+100+48=358

0010110(7,14,28,77,133,100,48)=28+133+100=261

0101101(7,14,28,77,133,100,48)=14+77+133+48=272

0101001(7,14,28,77,133,100,48)=14+77+48=139

1001110(7,14,28,77,133,100,48)=7+77+133+100=317

0111000(7,14,28,77,133,100,48)=14+28+77=119

Second encryption ($C.T_2$)=(91,261,358,261,261,225,191,338,239,358,261, 272,139,317,119).

He encrypted the first cipher text "$C.T_1$" secondly Table (4.2).

Table (4.2): Second Encryption process

First Cipher text "C.T $_1$"	Binary	Second Cipher text "C.T $_2$"
40	0101000	91
22	0010110	261
15	0001111	358
22	0010110	261
22	0010110	261
11	0001011	225
42	0101010	191
30	0011110	338
43	0101011	239
15	0001111	358
22	0010110	261
45	0101101	272
41	0101001	139
78	1001110	317
56	0111000	119

Step(7) In second pass protocol, Bob sends the "C.T 2" to Alice.

Step(8) Alice Determine the Unwanted terms and Wanted terms. This is done by comparing the elements of the message with the elements of the recipient's public key and choosing what is required in the message as shown in Table (4.3).

Table (4.3): Determine the Unwanted terms and Wanted terms

Letters	Integers Correspo -nding to Letters	Binary "B1"	First Cipher text "C.T 1"	Binary "B2"	Comparing	Unwanted terms and Wanted terms
T	20	10100	40	0101000	0010100 0101000	$a_2s_3 + a_2s_5 = \left(\sum_{i=1}^{7} a_2s_i\right) - a_2s_1 - a_2s_2 - a_2s_4 - a_2s_6 - a_2s_7$
A	1	00001	22	0010110	0000001 0010110	$a_2s_7 = \left(\sum_{i=1}^{7} a_2s_i\right) - a_2s_1 - a_2s_2 + a_2s_3 - a_2s_4 - a_2s_5 - a_2s_6$
H	8	01000	15	0001111	0001000 0001111	$a_2s_4 = \left(\sum_{i=1}^{7} a_2s_i\right) - a_2s_1 - a_2s_2 + a_2s_3 - a_2s_5 - a_2s_6 - a_2s_7$
A	1	00001	22	0010110	0000001 0010110	$a_2s_7 = \left(\sum_{i=1}^{7} a_2s_i\right) - a_2s_1 - a_2s_2 + a_2s_3 - a_2s_4 - a_2s_5 - a_2s_6$
A	1	00001	22	0010110	0000001 0010110	$a_2s_7 = \left(\sum_{i=1}^{7} a_2s_i\right) - a_2s_1 - a_2s_2 + a_2s_3 - a_2s_4 - a_2s_5 - a_2s_6$
B	2	00010	11	0001011	0000010 0001011	$a_2s_6 = \left(\sum_{i=1}^{7} a_2s_i\right) - a_2s_1 - a_2s_2 + a_2s_3 - a_2s_4 - a_2s_5 - a_2s_7$
E	5	00101	42	0101010	0000101 0101010	$a_2s_5 + a_2s_7 = \left(\sum_{i=1}^{7} a_2s_i\right) - a_2s_1 - a_2s_2 - a_2s_3 - a_2s_4 - a_2s_6$
D	4	00100	30	0011110	0000100 0011110	$a_2s_5 = \left(\sum_{i=1}^{7} a_2s_i\right) - a_2s_1 - a_2s_2 - a_2s_3 - a_2s_4 - a_2s_6 - a_2s_7$
S	19	10011	43	0101011	0010011 0101011	$a_2s_3 + a_2s_6 + a_2s_7 = \left(\sum_{i=1}^{7} a_2s_i\right) - a_2s_1 - a_2s_2 - a_2s_4 - a_2s_5$
H	8	01000	15	0001111	0001000 0001111	$a_2s_4 = \left(\sum_{i=1}^{7} a_2s_i\right) - a_2s_1 - a_2s_2 - a_2s_3 - a_2s_5 - a_2s_6 - a_2s_7$
A	1	00001	22	0010110	0000001 0010110	$a_2s_7 = \left(\sum_{i=1}^{7} a_2s_i\right) - a_2s_1 - a_2s_2 + a_2s_3 - a_2s_4 - a_2s_5 - a_2s_6$

L	12	01100	45	0101101	0001100 0101101	$a_2s_4 + a_2s_5 = \left(\sum_{i=1}^{7} a_2s_i\right) - a_2s_1 - a_2s_2 - a_2s_3 - a_2s_6 - a_2s_7$
F	6	00110	41	0101001	0000110 0101001	$a_2s_5 + a_2s_6 = \left(\sum_{i=1}^{7} a_2s_i\right) - a_2s_1 - a_2s_2 - a_2s_3 - a_2s_4 - a_2s_7$
O	15	01111	78	1001110	0001111 1001110	$a_2s_4 + a_2s_5 + a_2s_6 + a_2s_7 = \left(\sum_{i=1}^{7} a_2s_i\right) - a_2s_1 - a_2s_2 - a_2s_3$
N	14	01110	56	0111000	0001110 0111000	$a_2s_4 + a_2s_5 + a_2s_6 = \left(\sum_{i=1}^{7} a_2s_i\right) - a_2s_1 - a_2s_2 - a_2s_3 - a_2s_7$

Step(9) In third three pass protocol, Alice sends the wanted terms "W.T" to Bob.

Step(10) Bob restores plaintext by using the wanted terms as in Table(4.4)

Table (4.4): Recover the Plaintext

Wanted terms "W.T"	$(\mathbf{W.T})\mathbf{a_2^{-1}}\ \mathbf{mod\ m_2}$
$\left(\sum_{i=1}^{7} a_2 s_i\right) - a_2 s_1 - a_2 s_2 - a_2 s_4 - a_2 s_6 - a_2 s_7 = 407 - 7 - 14 - 77 - 100 - 48 = 161$	$(161)(99) \bmod 173 = 23$
$\left(\sum_{i=1}^{7} a_2 s_i\right) - a_2 s_1 - a_2 s_2 + a_2 s_3 - a_2 s_4 - a_2 s_5 - a_2 s_6 = 407 - 7 - 14 - 28 - 77 - 133 - 100 = 48$	$(48)(99) \bmod 173 = 81$
$\left(\sum_{i=1}^{7} a_2 s_i\right) - a_2 s_1 - a_2 s_2 + a_2 s_3 - a_2 s_5 - a_2 s_6 - a_2 s_7 = 407 - 7 - 14 - 28 - 133 - 100 - 48 = 77$	$(77)(99) \bmod 173 = 11$
$\left(\sum_{i=1}^{7} a_2 s_i\right) - a_2 s_1 - a_2 s_2 + a_2 s_3 - a_2 s_4 - a_2 s_5 - a_2 s_6 = 407 - 7 - 14 - 28 - 77 - 133 - 100 = 48$	$(48)(99) \bmod 173 = 81$
$\left(\sum_{i=1}^{7} a_2 s_i\right) - a_2 s_1 - a_2 s_2 + a_2 s_3 - a_2 s_4 - a_2 s_5 - a_2 s_6 = 407 - 7 - 14 - 28 - 77 - 133 - 100 = 48$	$(48)(99) \bmod 173 = 81$
$\left(\sum_{i=1}^{7} a_2 s_i\right) - a_2 s_1 - a_2 s_2 + a_2 s_3 - a_2 s_4 - a_2 s_5 - a_2 s_7 = 407 - 7 - 14 - 28 - 77 - 133 - 48 = 100$	$(100)(99) \bmod 173 = 39$
$\left(\sum_{i=1}^{7} a_2 s_i\right) - a_2 s_1 - a_2 s_2 - a_2 s_3 - a_2 s_4 - a_2 s_6 = 407 - 7 - 14 - 28 - 77 - 100 = 181$	$(181)(99) \bmod 173 = 100$
$\left(\sum_{i=1}^{7} a_2 s_i\right) - a_2 s_1 - a_2 s_2 - a_2 s_3 - a_2 s_4 - a_2 s_6 - a_2 s_7 = 407 - 7 - 14 - 28 - 77 - 100 - 48 = 133$	$(133)(99) \bmod 173 = 19$
$\left(\sum_{i=1}^{7} a_2 s_i\right) - a_2 s_1 - a_2 s_2 - a_2 s_4 - a_2 s_5 = 407 - 7 - 14 - 77 - 133 = 176$	$(176)(99) \bmod 173 = 124$
$\left(\sum_{i=1}^{7} a_2 s_i\right) - a_2 s_1 - a_2 s_2 - a_2 s_3 - a_2 s_5 - a_2 s_6 - a_2 s_7 = 407 - 7 - 14 - 28 - 133 - 100 - 48 = 77$	$(77)(99) \bmod 173 = 11$
$\left(\sum_{i=1}^{7} a_2 s_i\right) - a_2 s_1 - a_2 s_2 + a_2 s_3 - a_2 s_4 - a_2 s_5 - a_2 s_6 = 407 - 7 - 14 - 28 - 77 - 133 - 100 = 48$	$(48)(99) \bmod 173 = 81$
$\left(\sum_{i=1}^{7} a_2 s_i\right) - a_2 s_1 - a_2 s_2 - a_2 s_3 - a_2 s_6 - a_2 s_7 = 407 - 7 - 14 - 28 - 100 - 48 = 210$	$(210)(99) \bmod 173 = 30$
$\left(\sum_{i=1}^{7} a_2 s_i\right) - a_2 s_1 - a_2 s_2 - a_2 s_3 - a_2 s_4 = 407 - 7 - 14 - 28 - 77 - 48 = 233$	$(233)(99) \bmod 173 = 58$
$\left(\sum_{i=1}^{7} a_2 s_i\right) - a_2 s_1 - a_2 s_2 - a_2 s_3 = 407 - 7 - 14 - 28 = 358$	$(358)(99) \bmod 173 = 150$
$\left(\sum_{i=1}^{7} a_2 s_i\right) - a_2 s_1 - a_2 s_2 - a_2 s_3 - a_2 = 407 - 7 - 14 - 28 = 310$	$(310)(99) \bmod 173 = 69$

Bob compares 23 with (1,2,4,11,19,39,81) , 23=4+19 This means putting one under each of 4 and 19 and the rest are zero to get 0010100 = T in the same way

48x99mod173=81 by comparison ,we get 00001=A

77x99mod173=11 , 01000=H

48x99mod173=81 , 00001=A

48x99mod173=81 , 00001=A

100x99mod173=39 , 00010=B

181x99mod173=100 , 00101=E

133x99mod173=19 , 00100=D

176x99mod173=124, 10011=S

77x99mod173=11 , 01000=H

48x99mod173=81, 00001=A

210x99mod173=30, 01100=L

233x99mod173=58, 00110=F

358x99mod173=150, 01111=O

310x99mod173=69, 01110=N

The plain text "TAHA ABED SHALFON"

4.3 Taha Method (TPP Implementation On Modified Knapsack Cipher With Linear Equations)

This method combines knapsack Cipher and modern cryptographic algorithms and through the encoded texts between the sender and the receiver, we create linear equations and used the Gaussian Elimination method(GEM) to solve them and through it we reached the recipient's public key and we were able to encode messages on it and return it, which facilitated the task of the future in deciphering them. The steps of this method can be described as follows:

Step (1) Alice choose a super increasing S_1 and private encryption key a_1 and computing T_1 and encrypt his message m with key and send it to receiver.

Step (2) Bob chooses a super increasing S_2 and private encryption key(a_2) and corresponding decryption key T_2 and encrypt the first message with key and sends the doubly encrypted message back tothe sender.

Step (3) Alice creates linear equations through the first and second encoders, and they are solved in a GEM and finds the recipient's public key and encrypts his message on it and resends it.

Step (4) Bob uses the inverse of his private key to decode the message and compare the result with his group, thus obtaining the plain text.

4.4 Testing And Implementations

To illustrate this technique we take the following example :

Example(4.3.1) the message " Taha Abed Shalfon "

First : the sender (Alice) chooses the set

$S_1 = (2,3,6,12,24)\ multiplier\ a_1 = 5, and\ \ modulus\ m_1 = 49$

And computing the public key T_1={10,15,30,11,22}

Encrypted text. (40,22,15,22,22,11,52,30,43,15,22,45,41,78,56)

Third : he encryption the message as in Table 4.1

Forth :In first pass protocol ,Alice send the first cipher text $C.T\ 1 =$ (40,22,15,22,22,11,52,30,43,15,22,45,41,78,56) to Bob.

Fifth : Bob converts the cipher text it received to binary and then chooses super increasing

$$S_2 = (1,2,4,11,19,39,81)\ \ multiplier a_2 = 7\ \ and\ modulus\ m_2 = 173, a_2^{-1} = \ \ 99$$

$and\ calculate$ the public keyT_2=(7,14,28,77,133,100,48)

sixth :Bob encryption the first cipher text ($C.T_1$)secondly "(Table 4.2)" =($C.T_2$)=(91,261,358,261,261,225,175,338,239,358,261, 272,139,317,119)

Seventh :In second pass protocol, Bob sends the "C.T 2" to Alice. Alice through the first and second encoders ,creates thy following equations and makes them in a Gaussian method of elimination

$C.T_1$=(40,22,15,22,22,11,52,30,43,15,22,45,41,78,56)

$C.T_2$=(91,261,358,261,261,225,175,338,239,358,261,272,139,78,119)

40= 0101000 → 91……. (1)

22= 0010110 → 261…….(2)

15= 0001111 → 358.....(3)

22= 0010110 → 261……..(4)

22= 0010110 → 261…….....(5)

11= 0001011→ 225……..(6)

52= 0110100 → 175……..(7)

30= 0011110 → 338…….....(8)

43=0101011 → 239…….....(9)

15 =0001111→ 358.....(10)

22 =0010110 → 261.....(11)

45 =0101101→ 272…….....(12)

41= 0101001 → 139.....(13)

78= 1001110 → 317…….....(14)

56= 0111000 → 119……...(15)

Compute equations(3) and (6)

$a_2s_4+a_2s_5+a_2s_6+a_2s_7$=358…..(3)

$a_2 s_4+a_2s_6+a_2s_7$=225……(6)

---

a_2s_5=133

Compare equations (6) and (9)

$a_2s_4+a_2s_6+a_2s_7$=225.....(6)

$a_2s_2+a_2s_4+a_2s_6+a_2s_7$=239……(9)

$a_2\ s_2=14$

We substitute in equation (1)to find a_2s_4

$a_2s_2+a_2s_4=91$

$a_2\ s_4 =91-14=77$

We substitute $a_2s_2+a_2s_4$ in equation(13)

$a_2s_2+a_2s_4+a_2s_7=139$…….(13)

$14+77+a_2s_7=139$

$a_2s_7=48$

Then we substitute in equation (7)

$a_2s_2+a_2s_3+a_2s_5=175$…….(7)

$14+a_2s_3+133=175$

$a_2s_3=28$

Then we substitute in the equation (11)

$a_2s_3+a_2s_5+a_2s_6=261$……(11)

$28+133+ a_2s_6=261$

$a_2s_6=100$

Substitute in equation (14)

$a_2s_1 +a_2s_4+a_2s_5+a_2s_6=119$….(14)

$a_2s_1+77+133+100=317$

$a_2s_1=7$

so have obtained the public key of the receiver

=(7,14,28,77,133,100,48)

After that can send the message as follows :

Alice encrypts the message on the recipient's public key and then resends the message

0010100(7,14,28,77,133,100,48)=28+133=161

0000001(7,14,28,77,133,100,48) =48

0001000(7,14,28,77,133,100,48) =77

0000001 (7,14,28,77,133,100,48) =48

0000001(7,14,28,77,133,100,48) =48

0000010(7,14,28,77,133,100,48) =100

0000101(7,14,28,77,133,100,48)=133+48 = 181

0000100(7,14,28,77,133,100,48) =133

0010011(7,14,28,77,133,100,48)=28+100+48=176

0001000(7,14,28,77,133,100,48) =77

0000001(7,14,28,77,133,100,48)=48

0001100(7,14,28,77,133,100,48)77+133=210

0000110(7,14,28,77,133,100,48)=133+100=233

0001111(7,14,28,77,133,100,48)=77+133+100+48=358

0001110(7,14,28,77,133,100,48)=77+133+100=310

This is the text that Alice sends to Bob

(161,48,77,48,48,100,181, 133,176,77,48,210,233,358,310)

Bob multiplies this encrypted text by his own key and compares the result with his group, resulting the plain text as in the first method.

Chapter Five

Conclusions and Suggestions for Future Works

Chapter Five

Conclusions and Suggestions for Future Works

5.1. Introduction

This chapter includes a review of the most important conclusions reached through the application of the proposed method (TPP implementation on modified knapsack cipher) as well as a set of proposed actions for future work.

5.2 Conclusions

Recently, many new knapsack-based cryptosystems were proposed . The basic operations of all these cryptosystems are super increasing sequences and modular multiplications, which is the same as the basic Merkle-Hellman cryptosystem . In this thesis we presented a study on the three pass protocol to amend the knapsack cipher and the results were obtained:

1- This study has linked between the knapsack problem with three pass protocol implementation methods ,the purpose of which is to enhance data security.

2- In this study, the knapsack problem was modified and we introduced two methods were in this field so that they applied .

3-This research distinguished the possibility of sending the message between the sender and the recipient without any prior information between the two parties, or exchanging keys or sharing them except for the encryption method suggested in this work.

5.3 Suggestions for Future Works

The three pass protocol does not provide any authentication. Hence, without any additional authentication the protocol is susceptible to a man-in-the-middle attack if the opponent has the ability to create false messages, or to intercept and replace the genuine transmitted messages. So this thesis needs authentication, we Suggest that in the future.

References

[1] N. Sharma ,Prabhjot and H. Kaur, "A Review of Information Security using Cryptography Technique," International Journal of Advanced Research in Computer Science, vol. 8, no.4Special Issue, 2017.

[2] Safee ullah Soomro, Mohammad Riyaz Belgaum, Zainab Alansari, "Review and Open issues of Cryptographic Algorithms in Cyber Security" Conference Paper • DOI": 10.1109/iCCECE46942.8941663 August 2019.

[3] N. Vinothini, "Asymmetric Key Cryptography using Merkle-Hellman Knapsack Method and Genetic Algorithm "Journal of Computer Engineering and Applications, Vol. XII, Issue I, Jan. 18, 2018.

[4] Dwi Liestyowati**,** "Public Key Cryptography" Journal of Physics Conference Series 1477:052062, March 2020

[5] A.P.U. Saharan, "RC4 Technique in Visual Cryptography RGBI mage encryption", Journal of Computer Science and Engineering ,vole ,3 ,no.7,2016**.**

[6] Anurag Rawal, Gaurav, Hitesh, Khanna, GaganjotKaur, "Cryptography: Symmetric vs Asymmetric Encryption", Journal of Embedded Systems and Processing Volume 3 Issue 3 , Page 1-5 © MAT Journals 2018.

[7] Robbi Rahim, Ali Ikhwan, "Study of Three pass protocol on data Security", International Journal of Science and Research (IJRS) 5(11), November 2016.

[8]Rubin, Frank. "Device, system and method for fast secure message encryption without key distribution", No. 7,907,723. 15 Mar. 2011.

[9] Kanamori, Y. &Yoo, S."Quantum Three Pass Protocol Key Distribution Using Quantum Super position State", International Journal of Network Security Application, 2009.

[10]Boni Oktaviana, "Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography" IOSR Journal of Computer Engineering 18(4),P(26-29) , 2016.

[11] A. P. U. Siahaan, “Three-Pass Protocol Concept in Hill Cipher Encryption Technique,” Journal of Science and Research, vol. 5, no. 3, 2016.

[12] A. Subandi and R.Meiyanti,"Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Key stream Generator Modification", Journal Advances in Science Technology and Engineering Systems Vol, 2,No,5,1-5, 2017.

[13] Dian Rachmawat, Amer Sharif, and Rosalia Sianipar, "A combination of vigenere algorithm and one time pad algorithm in the three-pass protocol", Journal MATEC Web of Conferences197(13):03008,2018.

[14] Aqeel Azez "New Approach of RSA Algorithm based on Three-Pass Protocol" Journal of Engineering and Applied Sciences 14(21):7913-7916, 2019.

[15]R. Rahim."A Review on Cryptography Protocol for Securing Data" Journal of Physics, The 1st International Conference on Engineering and Applied Science ,Madiun, Indonesia Volume 1381012041,2019.

[16] Eric Lehman, Frank Thomson Leighton, Albert R. Meyer" Mathematics for Computer Science" Samurai Media Limited, Mar 8, 2017.

[17] Fraleigh, John B. A First Course in Abstract Algebra (5th ed.), Addison-Wesley, ISBN 978-0-201-53467-2, 1993.

[18] Lindsay N. Childs "Cryptology and Error Correction: An Algebraic Introduction and Real-World Applications" Springer Undergraduate Texts in Mathematics and Technology ISBN 978-3-030-15453-0,2019.

[19] William E."Modern Cryptography: Applied Mathematics for Encryption and Information Security" Springer Nature, Technology & Engineering , Dec 19, 2020.

[20] David M. Burton "Elementary Number Theory" ISBN 978-0-07-338314-9 McGraw-Hill Education, 2010.

[21] Peter Szabó and Katarína Gombíková."System of linear equations - infinite solutions" MATLAB File Exchange, Journal math works 2020.

[22]Yadanar Mon, Lai lai win kyi, “performance comparison of Gaussian elimination and gauss Jordan”, International Journal of Computer & Communication Engineering Research (IJCCER), Information Technology Department,02- march, 2014.

[23]Richard A. Mollin, "An Introduction to Cryptography" Journal Discrete Mathematical& Applications,2000.

[24] Nigel P. Smart "Cryptography Made Simple", Journal Springer International Publishing, Nov 20, 2015.

[25] A. P. U. Siahaan, “Factorization Hack of RSA Secret Numbers” International Journal of Engineering Trends and Technology,2016.

[26] Moll in, “An Introduction to Cryptography”, Second Edition, Taylor & Francis Group, 2007.

[27] Ola Salman, Sarah Abdallah ,Imad H. Elhajj, Ali Chehab ,Ayman Kayssi, "Identity-Based Authentication Scheme for the Internet of Things", IEEE Symposium on Computers and Communication (ISCC),American University of Beirut1107, 2020.

[28] Mahfouz, Ahmed; Mahmoud, Tarek M.; Eldin, Ahmed Sharaf "A survey on behavioral biometric authentication on smart phones". Journal of Information Security and Applications. **37**: 28–37, 2017.

[29] M. Reza Dan M. A. Bud man, “Simulcast Panamanian File Teaks Menggunak an Algorithm Massey-Omura,” Journal Dulia Technologic Informasi,2012.

[30]B. Bazith Mohammed, “Automatic Key Generation of Caesar Cipher” Journal of Engineering Trends and Technology, vol. 6, no.6,2013.

[31] Sanchez, J., Correa, R., Buena, H., Arias, S. and Gomez, H., "Encryption techniques: A theoretical overview and future proposals" in Third International Conference on eDemocracy&eGovernment, March 2016.

[32]Y. Kanamori Dan S.-M. Yoo, “Quantum Three-Pass Protocol: Key Distribution Using Quantum Super Position States,” International Journal of Network Security & Its Applications,2009.

[33] Davies, Robert B," Exclusive OR (XOR) and hardware random number generators" , Retrieved 28 August 2013.

[34] A. A. Khalaf, M. S. A. El-karimdan H. F. A. Hamed, “A Triple Hill Cipher Algorithm Proposed to Increase the Security of Encrypted Binary Data and its Implementation Using FPGA,” ICACT Transactions on Advanced Communications Technology, 2016.

[35] B. Forouzan, "Cryptography and Network Security" New York, NY, USA: McGraw-Hill, 2006.

[36] Andini Dani Achmad, Ayu Aryista Dewi, Muhammad Roy Purwanto3, Phong Thanh Nguyen, Imam Sujono , "Implementation of Vigenere Cipher as Cryptographic Algorithm in Securing Text Data Transmission" , Journal of Critical Reviews ISSN- 2394-5125 Vol 7, Issue 1, 2020.

[37] Andysah Putera Utama Siahaan " Three Pass Protocol Concept in Hill Cipher Encryption Technique", Seminar National Aplikasi Technology Informasi(SNATi),Yogyakarta,6 Augusts, 2016.

[38] William, Stallings. "Computer Security: Principles And Practice". Pearson Education India, 2008.

[39] William Stallings, “Cryptography and network security: principles and practices”, Pearson Education India, 2006.

[40] Bellare, Mihir, Alexandra Boldyreva, and Silvio Micali. "Public-key encryption in a multi-user setting: Security proofs and improvements" International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2000.

[41] Elaine Barker "Framework for Designing Cryptographic Key Management Systems" DIANE Publishing, 2011.

[42] Casteivecchi, Davide, “Quantum-computing pioneer warns of complacency over Internet security”, October 30, 2020.

[43]Elbaz, Limor, and Hagai Bar-El. "Strength assessment of encryption algorithms" ,2000.

[44] Alharith A. Abdullah, Rifaat Z. Khalaf, and Mustafa Riza, "A realizable quantum three-pass protocol authentication based on hill-cipher algorithm "Mathematical Problems in Engineering, (2015).

[45] Alharith Abdulkareem Abdullah "Modified Quantum Three Pass Protocol Based on Hybrid Cryptosystem" (2015).

Publications

[1] Rifaat Z. Khalaf, Ahmed A. Muhsin, Taha A. Shalfon**,** "Secure Knapsack Problem Based on Continued Fraction" Turkish Journal of Computer and Mathematics Education(TURCOMAT),Trabzon University, e-ISSN 1309-4653,14/ March/2021.

[2] Taha A. Shalfon "Three-Pass Protocol Implementation on Knapsack Problem based on Linear Equations" sponsored by IEEE of IEEE Iraq section in the 1st ABYLON INTERNATIONAL AND SCIENCE (BICITS'21) March 28-29,2021.

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.

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