جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة ديالى/كلية العلوم/ قسم الرياضيات

صياغة جديدة لنظام التشفير Knapsack Problem بالاعتماد على الكسر المستمر و الرمز الاسطوري

رسالة مقدمة

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

من قبل

احمد عبدالرحمن محسن ابراهيم

بأشراف

أ.م. د. رفعت زيدان خلف

شوال /1442 مايو /2021

Chapter One

General Introduction

Chapter One

General Introduction

1.1 Overview

The great development in the field of the Internet and technology, in the modern world today and the increase in the number of devices that send and receive data, as well as the fact that there are many such devices that perform several functions without human intervention, has led to large data transmission processes. Definitely, these data contain sensitive data and personal information, so there is an urgent need to protect these data from attacks, and there are many ways to protect information. This can be overcome by cryptography-related sciences, which prevent any user to access the required information or sensitive data, except the personnel who have an authorization to do that. Basically, Cryptography can secure information through providing powerful protection to confidentiality issue and can provide protection to information concerning data authenticity and integrity[1][2].

The Cryptography term comes from Greek language, it is a compound word having two meanings : “Crypto” that means hidden and “grafia” which means writing [3]. Most importantly several types of these systems are invented , the most widely-known cryptosystem and the earliest public key cryptographic (PKC) system in the world , is proposed in1976, by Martin E. Hellman, American cryptologist Ralph C. Merkle (computer scientist) [4]. Cryptosystems are called (PKC) since two dissimilar keys are required in both decryption and encryption processes , the first key is to encrypt data , called the public-key, and the second key is to decrypt data , called the private -key and it is impossible to derive the decrypt key from the encrypt key. Most importantly, knapsack cryptosystem represents the earliest (PKCs), it is an additive number theory cryptosystem [5]. Since the history of proposing this technique in 1970s, several versions of this system have been proposed such as the multiplicative knapsack cryptosystem[6][7].Chor-Rivest knapsack cryptosystem [8][9],the Graham-Shamir knapsack [10], the Naccache-Stern Knapsack [11], and the Super-Pascal Triangle Knapsack [12].

Unluckily, the majority of knapsack cryptosystems that technicians are proposed, up to now, are not reliable enough concerning security aspect to resist cryptanalysis attacks.This type of attacks can overcome these systems due to the vulnerabilities existing in the cryptosystem designs.

During the early 1980s, Adi Shamir presented an approach to overcome (MHKC), this approach managed to decrypt encoded text in polynomial time needless to use the private key , he was able to break the MHKC ; it is considered the first cryptanalytic approach of this type [13].

Furthermore,Lovász László, Hendrik Lenstra and Arjen Lenstra invent algorithm by the use of a lattice reduction, which named the LLL Algorithm, the purpose of the algorithm for finding a shortest vector in a lattice [14].

The system of Merkle-Hellman knapsack problem (MHKP) is characterized to have some weaknesses, which includes : it is susceptible to attacks by the use of LLL algorithm [15]

To avoid the LLL algorithm attack, this thesis introduces the idea of using continuous fraction.

1.2 Related Works

This section reviews some of the previous studies and explains the different techniques that are used for developing the classification systems.

- M. Hellman and R. Merkle, (1978) [16] Hiding information and signatures in trapdoor knapsacks, concealing signatures and information in trapdoor knapsacks, the knapsack problem is an NP-complete combinatorial problem , which generally thought that this is , from a computational point of view, complicated to be solved. The knapsack problem is an NP-complete combinatorial problem that is strongly believed to be computationally difficult to solve in general. Specific instances of this problem that appear very difficult to solve unless one possesses "trapdoor information" used in the design of the problem are demonstrated. Because only the designer can easily solve problems, others can send him information hidden in the solution to the problems without fear that an eavesdropper will be able to extract the information. This approach differs from usual cryptographic systems in that a secret key is not needed. Conversely, only the designer can generate signatures for messages, but anyone can easily check their authenticity

- A. Shamir and R. Zippel, (1980) [17] On the security of the Merkle-Hellman cryptographic scheme (Corresp.), in IEEE Transactions on Information Theory, A version simplified of the Merkle-Hellman PKC can be broken. While their completely developed system appears to be capable of resisting cryptanalytic attacks we proposed, the result indicates partially in which the system's security aspect can be optimized. the Merkle-Hellman public-key cryptographic system is breakable. While their full-fledged system seems to be resistant to the cryptanalytic attack we propose, this result suggests some ways in which the security of their system can be further enhanced.

- A.Shamir, (1982)[18] A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem, the cryptographic security of the Merkle-Hellman cryptosystem has been a major open problem. In this paper, we show that the basic variant of this cryptosystem, in which the elements of the public key are modular multiples of a super- increasing sequence, is breakable in polynomial time. In 1976 Diffie and Hellman published their pioneering paper on public-key cryptography . Their paper speculated that such cryptosystems exist and surveyed their potential applications but did not describe actual implementations. In late 1976 and early 1977, the first two public-key cryptosystems were discovered. Since then many variants and a few new public-key cryptosystems have been proposed, but for a variety of reasons these first two systems continue to dominate the field. They have been extensively analyzed, and a number of cryptanalytic attacks have been proposed to try to break them. However, all these attacks are unlikely to succeed unless the cryptosystems are greatly simplified or their key sizes reduced. We describe the first cryptanalytic attack we know of that can break a full-size variant of one of these cryptosysterns in reasonable time and space complexities. The variant is known as the single-iteration Merkle-Hellman cryptosystem, and it is the simplest (and presumably the least secure) in the family of public-key cryptosystems proposed in Merkle and Hellman’s original paper. The cryptanalytic attack is not directly applicable to multi-iteration Merkle-Hellman cryptosystems, and thus the cryptographic security of these variants remains an open problem.

- B. Chor and R. Rivest,(1988) [19] Introduced a knapsack-type Public

Key Cryptosystem Based on arithmetic in Finite Fields, A new knapsack-type public key cryptosystem is introduced. The system is based on a novel application of arithmetic in finite fields, following a construction by Bose and Chowla. By appropriately choosing the parameters, one can control the density of the resulting knapsack, which is the ratio between the number of elements in the knapsack and their sue in bits. In particular, the density can be made high enough to foil "low-density" attacks against our system. At the moment, no attacks capable of "breaking" this system in a reasonable amount of time are known. In 1976, Diffie and Hellman introduced the idea of public key cryptography, in which two different keys are used: one for encryption and one for decryption. Each user keeps his decryption key secret while making the encryption key public, so it can be used by everyone wishing to send messages to him. A few months later, the first two implementations of public key cryptosystems (PKC‘s) were discovered: the Merkle-Hellman scheme and the Rivest-Shamir-Adelman (RSA) scheme. While no efficient attacks against number-theoretic PKC‘s are known, several knapsack-type PKC‘s have been shown to be insecure. Most of those systems have a concealed " superincreasing" sequence. Shamir made the first successful attack on the basic Merkle-Hellman system.Following his attack, other attacks against more complicated systems were proposed. In particular, Brickell found a way to break the general Merkle-Hellman scheme.

- Y. Boas, D. Rocha, Elt, (2020) [20] F2MH cryptographic system: Initial analyzing of an original endeavor for reviving Knapsack-based (PKC). Public-key cryptography is an ubiquitous building block of modern telecommunication technology. Among the most historically important types, the knapsack-based encryption schemes, from the early years of public-key cryptography, performed particularly well in computational resources (time and memory), and mathematical and algorithmic simplicity. Although their widespread adoption was readily curtailed by effective cryptanalyses to several different attempts, the question of whether or not there is any future for actual usage of knapsack based asymmetric encryption schemes, and all its potential advantages remains unsettled. The goal of this paper is to present a novel construction, which offer consistent security improvements on knapsack-based cryptography. We propose two improvements upon the original knapsack cryptosystem that address the most important types of attacks: the Diaphantine approximations based attacks and the lattice problems oracle attacks. The proposed defenses demonstrably preclude the aforementioned types of attacks the goal of this paper is to introduced a new architecture, which offers consistent security improvements over knapsack-based cryptography.

1.3 Problem Statement

Due to the tremendous development in the field of information and communication technology and the expansion of penetrations and attacks of stored and transmitted data, where encryption techniques appeared to achieve and preserve security, including the Merkel-Hellmann algorithm, but all technologies did not withstand the attack of the LLL algorithm, which adopts the concept of gram –Schmidt orthogonal, and there are other problems such as the length of cipher text.

1.4 Aim of Thesis

To solve the above-mentioned problems, a system for improving the Merkel-Hellmann algorithm was proposed, using the concept of continuous fraction, which is based on compressing the data and making it impenetrable by the LLL algorithm.

1.5 Thesis Outline

This thesis is contains five chapters, including chapter one, it contains the following chapters:

▪Chapter Two: (Scientific and Theoretical Background)

This chapter explains in detail background of basic mathematical concepts in linear algebra, orthogonal, Reduced basis for lattice, Gram Shmidt Orthogonal, and Concepts of Cryptography, Symmetric Cryptography, Asymmetric Cryptography, Cryptoanalysis.

▪Chapter Three :(Merkle-Hellman knapsack cryptosystem)

This chapter explain some type of Knapsack Problem,Ordinary Knapsack Problem, 0-1 Knapsack Problem and detail the background of Merkle-Hellman knapsack cryptosystem, also discusses LLL Algorithm, illustration example.

- **Chapter Four: (Results and Analysis)**

This chapter we give example to encryption text by Merkle-Hellman without use Continued Fraction and other example to encryption text by Merkle-Hellman with using Continued Fraction, and discusses the results and give the analysis for them.

- **Chapter Five:(Conclusions and Suggestions for Future Works)**

In this chapter we give some concluding remarks which are derived from the outputs of the conducted tests are given in this chapter; also we give some suggestions for future works are presented.

الملخص

تعد تقنية المعلومات من أهم مكونات العصر الحديث ، وتعرف بأنها عملية استخدام أجهزة الكمبيوتر لتخزين ونقل واسترجاع البيانات والمعلومات وتنفيذها. من المفاهيم التكنولوجية أهمها مفهوم نظم المعلومات الذي يعد من أهم عناصر تقنية المعلومات والذي يضم مجموعة من العناصر التكنولوجية التي تدل على أهمية نظم المعلومات في حياتنا وأهمها المهام .

في عالم الحوسبة ، التشفير هو تحويل البيانات من نموذج قابل للقراءة إلى نموذج مشفر لا يمكن قراءته أو معالجته إلا بعد فك تشفيره.

التشفير هو لبنة البناء الأساسية لأمن البيانات وهو الطريقة الأبسط والأكثر أهمية لضمان عدم سرقة معلومات نظام الكمبيوتر أو قراءتها من قبل شخص يريد استخدامها لأغراض شائنة.

يستخدم التشفير من قبل المستخدمين الأفراد والشركات الكبيرة. يتم استخدامه على نطاق واسع على الإنترنت لضمان أمان معلومات المستخدم المرسلة بين المتصفح والخادم.

من بين خوارزميات التشفير المهمة التي تم استخدامها في المراسلات خوارزمية Merkel-Hellmann ، لكنها تحتوي على نقاط ضعف لم تصمد أمام بعض الهجمات ، بما في ذلك الهجوم باستخدام خوارزمية LLL ، وهناك مجموعة من الأبحاث التي بدت لعلاج نقاط الضعف ، ولكن احتوت على نقاط ضعف أخرى ، بما في ذلك الوقت وطول النص المشفر والأمان.

في هذا الصدد ، تم اقتراح نظام تشفير لمعالجة نقاط الضعف في خوارزمية Merkle-Hellmann. النظام المقترح يعتمد على الكسر المستمر ، والذي يمنع هجوم LLL.

قدم النظام المقترح نظامًا عالي الكفاءة من خلال استخدام مقياس متوسط الأمان.