الجمهورية العربية السورية
جامعة البعث
كلية العلوم
قسم الرياضيات

دراسة أعدت لنيل درجة الماجستير في التحليل الرياضي

دراسة سلوكيات دالة النظائر الضربية وتطبيقاتها في التشفير

إعداد الطالب
أحمد عرابي الأحمد

إشراف
أ.د.سامح العرجة
أ.د.محمد نور شمه

١٤٣٦ هـ / ٢٠١٥ م

Syrian Arab Republic

Al-Baath University

Faculty of Sciences

Department of Mathematics

Studying behavior of symmetric product function and its applications in cryptography

A study perpared to have the degree of master in mathematical analysis

By the student :

Ahmad Orabi Al ahmad

By Supervision Of :

D. Sameh Arjh

D. Mohammad Nour Shamma

ملخص الدراسة

تتلخص الرسالة هذه في تطوير طريقة فيجينير الكاملة في التشفير وذلك من خلال :

1- الاعتماد على ترميز الآسكي المضاف إليه عنصر مما يجعل عدد عناصره 257 (عدداً أولياً) وبالتالي تكون جميع الأعداد الأصغر منه أولية نسبياً معه ، والاعتماد على طريقة فيجينير الكاملة في التشفير .

2- دراسة سلوكيات دالة النظائر الضربية لتطبيقها في التشفير .

3- استخدام دالة النظير الضربي $F(X)=\left(AX^{*}+B\right)\mathbf{mod}\,257$ عناصرها (A,X,B) مصفوفات لها شروط خاصة بحيث تصبح قادرة على تشفير رسالة كاملة دفعة واحدة اعتماداً على حساب المصفوفات ذات المراتب العليا ، مما يجعلها صعبة الكسر الأمر الذي يحافظ على أمن المعلومات داخل النصوص والرسائل المبثوثة .

4- قابلية تطبيق هذه الطريقة حاسوبياً على Maple لتعطي نتائج سريعة وكبيرة .

مقدمة : هدف (التشفير) الحفاظ على سرية الرسائل المبثوثة عبر قنوات الاتصال المختلفة كالراديو والهاتف والجوال والبريد الإلكتروني والحكومات الإلكترونية ...إلخ.

هناك طرائق عديدة للتشفير نذكر منها التشفير بطريقة فيجينير الكاملة والتي قمنا بتطويرها لتصبح ملائمة للمتغيرات الحديثة ، كما استخدمنا دالة النظير الضربي $F(X)=\left(AX^{*}+B\right)\mathbf{mod}\,257$ بالإضافة إلى طريقة فيجينير الكاملة.

قبل شرح هذه الطريقة سوف نذكر بعض المفاهيم والتعاريف ذات الصلة.

This master summarizes the development of Viginier full method in cryptography. Our method is based on :

1 –*Coded Ascci added to it an element which makes the number of marks* 257 *, a prime number and the all smaller numbers of* 257 *are relatively prime with it , and depending on Viginier full method in cryptography·*

2 –*Studying behavior of symmetric product function to apply it in cryptography.*

3 –*Using of symmetric product function* $f(X) = \left(AX^{*} + B\right)$ *such that A,X and B are specified matrixes where as it become able to cipher a full message all at once , depending on the calculation of matrixes of high orders which makes it difficult to decipher , the thing which keeps the safety of information inside the texts and delivered messages .*

4 –*Its ability to apply by using computers on Maple to provide effective results.*

Introduction **:** *the goal of the* (*cryptography*) *is to preserve the confidentiality of messages delivered via various channels of communications* (*radio , telephone , mobile ,e-mail and e-government*) *etc.*

There are many ways to cryptography such as Viginier full method , We develop this method to be suitable for modern variable On the other hand , we use a symmetric product function $f(X) = \left(AX^* + B\right)$ *in addition to the Viginier full method in cryptography.*

Before explaining this method , we have to cite some of concepts and definitions.