الجمهورية العربية السورية
جامعة البعث
كلية العلوم
قسم الرياضيات

دراسة سلوكيات دالة النظائر الجمعية وتطبيقاتها في التشفير باستخدام نظام UNICODE

دراسة أعدت لنيل درجة الماجستير في التحليل الرياضي

إعداد الطالب : محمد حازم هامش الأنصاري
إشراف
أ . د . سامح العرجة
أ . د . محمد نور شمه

١٤٣٦هـ/٢٠١٥م

Syrian Arab Republic

Al-Baath University

Faculty Of Science

Department Of Mathematics

Studying Behavior Of Symmetric Additive Function And Its Application In Cryptography By UNICODE System

By

M .Hazem Hamesh Al ansari

Supervised By

Dr. Sameh Al arjeh

Dr. Muhammad Nour Shamma

١٤٣٦هـ

٢٠١٥م

دراسة سلوكيات دالة النظائر الجمعية وتطبيقاتها في التشفير باستخدام نظام UNICODE

الملخص

تقدم رسالتنا دراسة للتعرف على خواص وسلوكية دالة النظائر الجمعية بغية الاستفادة منها في تطوير الطرائق الكلاسيكية في التشفير وذلك من اجل الوصول إلى الأمان في تبادل المعلومات بين الشبكات الحاسوبية حيث إننا سنجد أن دالة النظائر الجمعية $\bar{F}(x) = (a\bar{x} + b)mod(n)$ ماهي إلا عبارة عن دمج بين طريقتين من طرائق التشفير الكلاسيكي وهما :

١. **شيفرة أتباش (Atbash cipher)**

٢. **شيفرة أفاين (AFFINE Cipher)**

حيث أنه يمكن ملاحظة ذلك من خلال العلاقات التالية :

طريقة Atbach تأخذ شكل الدالة : $f_1(x) = (n - x)mod(n)$

طريقة Affine تأخذ شكل الدالة : $f_2(x) = (ax + b)mod(n)$

ومنه تركيب الدالتين السابقتين سوف يعطي الدالة التالية :

$$\bar{F}(x) = f_2(f_1(x)) = (a(n - x) + b\ )mod(n) = (a\bar{x} + b)mod(n)$$

وهي عبارة عن دالة النظائر الجمعية التي سوف نقوم بدراسة سلوكياتها بشكل مفصل ومن ثم الاستفادة منها في تطوير الطريقة الألمانية ADFGVX في التشفير وذلك من خلال :

أولاً: عبر توسيع مصفوفة بوليبس لتصبح من الدرجة ١٦*١٦ وبذلك نشمل كل محارف نظام ASCII .

ثانياً: عبر الاستفادة من الدالة المصفوفية $f(x) = K_t\bar{X} + B$ في تطوير هذه الطريقة حيث إن ($K_t = P_t^{-1}KP_t, X, B$) مصفوفات لها شروط خاصة وهنا لابد من التنويه على ان هذه الدالة تعد تطوير لدالة هيل ولكن تم اضافة خاصية الانسحاب والدوران عليها لكي تصبح هذه الدالة اكثر امنا و قدرة على تشفير رسالة كاملة دفعة واحدة اعتماداً على حساب المصفوفات ذات المراتب العليا استنادا الى ترميز UNICODE وهذا ما يجعلها صعبة الاختراق الأمر الذي يحافظ على أمن المعلومات داخل النصوص والرسائل المبثوثة وجدير بالذكر إلى قابلية تطبيق هذه الطريقة حاسوبياً لتعطي نتائج سريعة و دقيقة .

Abstract

Introduction :
In our time, there is an urgent need for more use of cryptography because The world has become connected to each other via open networks, where is the use of these networks in the electronic transmission of information among ordinary people, or between private or public organizations therefore, great efforts has made from all over the world to find the best ways in which to exchange data confidentiality In the Second World War mathematics has become great attention in cryptography, as an example, Hans Rohrbach in Germany , Alan Mathison Turing in England And A.Adrin Albert in the United states

This research presents an analytical description of some classical methods of cryptography where we convert these methods to the functions , which give us the possibility to study the behaviors better and open the door to develop it in order to reach safety in the exchange of information between computer networks , Whereas the development of computational techniques and its entry in different Specialty of life like scientific , administrative, financial or military In addition to the proliferation of patch work systems, computing has become not limited to a geographical area, but include the whole hemisphere so this situation has led to the emergence of real risks caused by the illegal attempt to entry into the stored processed data in computers and transmitted with each other in order to get this information for different purposes or trying to change them or destroy them . we find through This research that the symmetric additive function is only composing between two classic method of cryptography the affine cipher and Atbash cipher .

This thesis is an attempt to identify the characteristics and behavioral of symmetric additive function in order to use it to develop methods of classical encryption in order to reach safety in the exchange of information between computer networks
where we find that the symmetric additive function are only an integration between two method the affine cipher and Atbash cipher
Where it can be seen through this relationships
$f_1(x) = (n - x) mod(n)$ Atbash cipher function
$f_2(x) = (ax + b) mod(n)$ affine cipher function
And from the composing of the previous two functions will give the following function: