Ministry of Higher Education and
Scientific Research
University of Mosul
College of Computer Science and
Mathematics
Department of Computer Science

Robust Passwords Generate Based on Chaotic System with Genetic Algorithm

**A Thesis Submitted to the Council of the College of
Computer Science and Mathematics
University of Mosul
as a Partial Fulfillment of the Requirements
for the Degree of Higher Diploma
in
Computer Science**

Submitted by

Ehab Younis Mostafa Hassan

Supervised by

Assist. Prof. Dr. Saja Jasem Mohammed

2024 A.D. **1445 A.H.**

ABSTRACT

With the growing frequency of cyber-attacks and data breaches, the significance of robust passwords cannot be exaggerated. The use of password-generating software has been extensive in creating intricate passwords that pose cracking challenges, but it has some limits. An inherent issue with this kind of program is its tendency to produce passwords that are arduous to recall, prompting customers to either jot them down or use them again across several accounts. Text passwords have been the primary user authentication method used by many Internet services for a long time. By adhering to the suggested practice, users encounter the daunting challenge of creating and maintaining several site-specific and robust (i.e., not easily guessed) passwords.

An effective approach to tackling this issue is implementing a password generator. This technique operates on the client side and produces (and regenerates) robust, site-specific passwords as needed, with little user input. This thesis utilizes the logistic chaotic method, a significant pseudo-random source functioning as a pseudo-random number generator (PRNG), to produce a resilient text password. A genetic method is used to augment the feeble password that has been produced. Since our system operates in real-time, our generator does not store any user input/output in memory or keep any log. Our method ensures absolute privacy protection without any possibility of privacy breaches.

Many practical implementations with various user input values are applied to the proposed algorithm. All of the generated passwords are tested using the most popular websites. The high-test results ratio gives the generated password “very strong.” Time of execution was also an important thing to consider. The time increases in a linear relationship with the password length. That gives the proposed algorithm power to be used in many places where a very strong password is generated based on easy-to-remember user input characters.

وزارة التعليم العالي والبحث العلمي
جامعة الموصل
كلية علوم الحاسوب والرياضيات
قسم علوم الحاسوب

توليد كلمات مرور قوية بالإعتماد على نظام الفوضى والخوارزمية الجينية

رسالة مقدمة
الى مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل
كجزء من متطلبات نيل شهادة دبلوم عالي في
علوم الحاسوب

من قبل
ايهاب يونس مصطفى حسن

بإشراف
أ.م.د. سجى جاسم محمد

١٤٤٥ هـ
٢٠٢٤ م

الخلاصة

مع ازدياد وتيرة الهجمات الالكترونية واختراق البيانات، فأن اهمية استخدام كلمات المرور القوية لا غنى عنها، لهذا فقد تم التوسع في استخدام برامج توليد كلمات المرور الخاصة قوية والمعقدة لمواجهة تحديات ومصاعب الاختراق إلى حد معين، ومشكلة هذا النوع من البرامج هو ميلها إلى انشاء كلمات سر قد تكون صعبة الحفظ والاستراجاع، مما يدفع المستخدمين اما إلى كتابتها او استخدامها لعدة حسابات، لذلك فقد كانت كلمات السر المكتوبة والنصية هي الطريقة الأساسية المتبعة في الكثير من المواقع الالكترونية عبر الإنترنت ولمدة طويلة جدا. ولقد واجه المستخدمين الكثير من المشاكل في انشاء كلمات سر (صعبة التذكر) والحفاظ عليها.

الطريقة المثلى الفعالة في التعامل مع هذ المشكلة هي عبر استخدام برنامج مولد كلمات المرور وهذه الطريقة عملية من جانب المستخدم وتنتج كلمات سرية قوية تلبي الاحتياجات المطلوبة من خلال قيام المستخدم إدخال كلمات معينة او أرقام بسيطة سهلة التذكر وتم استخدم في هذه الرسالة الأسلوب الفوضوي اللوجستي (logistic chaotic method) وهو مصدر شبه عشوائي يعمل كمولد أرقام عشوائية زائفة (pseudo-random) لإنتاج كلمة مرور نصية مرنة. وقد يتطلب استخدام الخوارزمية الجينية (genetic method) لتقوية كلمات المرور الضعيفة والبدائية التي تم توليدها. وبما ان نظامنا يعمل في الوقت الحالي (real time)، فأن برنامج التوليد الخاص بنا لا يحفظ اي عملية إدخال او توليد كلمة مرور لأي مستخدم في ذاكرة الحفظ او في السجل.

ولقد تم تطبيق العديد من الطرق الفعالة مع الكثير من قيم مدخلات المستخدم على الخوارزمية المقترحة، وتم اختبار جميع كلمات المرور بأستخدام مواقع الويب الاكثر شهرة. فأن نسبة نتائج الاختبار العالية تمنح كلمة المرور المولدة التي تم إنشاؤها (قوية جدا). وقد تم ايضا الاخذ بنظر الاعتبار الوقت الذي استغرقته العملية. ويزداد الوقت في علاقة طرديا مع طول كلمة المرور. والتي تعطي الخوارزمية المقترحة القوة لكي ستم اعتمادها في الكثير من الاماكن (المواقع) حيث يتم توليد كلمات مرور قوية بالإعتماد على حروف والمدخلات سهلة التذكر والحفظ الخاصة بالمستخدم.