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

Cryptanalysis of Blowfish algorithm using LSTM deep learning

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

By

Raghad Layth Malallah Aziz

Supervised by

Lecture. Dr. Auday Hashim Saeed Al-Wattar

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

Abstract

Cryptanalysis is a very important field of assessing the security of encryption algorithms, especially in an era of rapid advancements in computing power. Regarding information security, it is essential to enhance cryptanalysis techniques continually. There are many methods and techniques used in cryptanalysis, including mathematical methods. The problem with the thesis is that the ability of these methods may be limited in terms of effort and accuracy of the results, meaning they do not give satisfactory results to the analyst or the attacker.

Therefore, in this thesis, an artificial intelligence (AI) algorithm is used to improve the cryptanalysis of block ciphers (Blowfish algorithm as a case study). This thesis proposes an intelligent model by using the LSTM structure as a basic learning layer in the proposed neural network to improve the analysis of Blowfish cryptography to enhance its security. This proposed neural network was trained using a dataset created with a size of 1218 KB of plaintext and ciphertext pairs.

After training, a training accuracy of 0.7076 was obtained, and a training loss of 1.2941 was considered a satisfactory result. Also four metrics were used to measure the performance of the smart model using a data set that is not visible to the model: Accuracy F1 score Recall Precision, the result was 71%. This thesis provides valuable insights into the application of AI algorithms for reinforcing the security of block ciphers. Additionally, the results inform potential enhancements to the Blowfish algorithm, increasing its resilience against attacks.

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

تحليل الشفرات لخوارزميات السمكة المنتفخة باستخدام التعلم العميق LSTM

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

من قبل

رغد ليث مال الله عزيز

بإشراف
د. عدي هاشم سعيد الوتار

1445 هـ 2024 م

الخلاصة

يعد تحليل التشفير مجالًا مهمًا جدًا لتقييم أمان خوارزميات التشفير، خاصة في عصر التقدم السريع في قوة الحوسبة. فيما يتعلق بأمن المعلومات، فمن الضروري تعزيز تقنيات تحليل الشفرات بشكل مستمر. هناك العديد من الأساليب والتقنيات المستخدمة في تحليل الشفرات، بما في ذلك الأساليب الرياضية. ومشكلة الأطروحة هي أن قدرة هذه الأساليب قد تكون محدودة من حيث الجهد ودقة النتائج، أي أنها لا تعطي نتائج مرضية للمحلل أو المهاجم.

لذلك، في هذه الأطروحة، قمنا باستغلال إمكانات خوارزميات الذكاء الاصطناعي (AI) لتحسين تحليل الشفرات لكتلة التشفير (خوارزمية السمكة المنتفخة كدراسة حالة). تقترح هذه الأطروحة نموذجًا ذكيًا باستخدام بنية LSTM كطبقة تعلم أساسية في الشبكة العصبية المقترحة لتحسين تحليل تشفير السمكة المنتفخة لتعزيز أمانها. تم تدريب هذه الشبكة المقترحة باستخدام مجموعة بيانات تم إنشاؤها بحجم 1218 كيلو بايت من أزواج النص العادي والنص المشفر.
وبعد التدريب تم الحصول على دقة تدريب قدرها 0.7076، واعتبرت خسارة التدريب البالغة 1.2941 نتيجة مرضية. تم استخدام أربعة مقاييس لقياس أداء النموذج الذكي باستخدام مجموعة بيانات غير مرئية للنموذج: الدقة، درجة F1، الدقة في الاستدعاء، وكانت النتيجة 71%. توفر هذه الأطروحة رؤى قيمة حول تطبيق خوارزميات الذكاء الاصطناعي لتعزيز أمن تشفير الكتل. بالإضافة إلى ذلك، تشير النتائج إلى التحسينات المحتملة لخوارزمية السمكة المنتفخة، مما يزيد من مرونتها ضد الهجمات.

يوفر هذا البحث رؤى قيمة حول تطبيق خوارزميات الذكاء الاصطناعي لتعزيز أمان تشفير الكتل. بالإضافة إلى ذلك، تشير النتائج إلى التحسينات المحتملة لخوارزمية السمكة المنتفخة، مما يزيد من مرونتها ضد الهجمات .