ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to my teacher (Dr. Faisal Mohammed Abdalla Ali) who gave me the golden opportunity to do this wonderful project on the topic (DES SECURITY ENHANCEMENT USING GENETIC ALGORITHM, which also helped me to know about so many new things I am really thankful to him.

ABSTRACT

In symmetric cryptosystems a primary key is used to create a number of subkeys according to specified key scheduling algorithm; certain initial keys are weak keys. The initial value is split into two halves, and each half is shifted independently. If all the bits in each half are either 0 or 1, then the key used for any cycle of the algorithm is the same for all the cycles of the algorithm This can occur if the key is entirely 1s, entirely 0s, or if one half of the key is entirely 1s and the other half is entirely 0s.for this reason the design of a good key schedule is a crucial aspect of cipher design. In This research presents new algorithms that simplify the creation and expansion process of the encryption key of the DES algorithm, which is considered one of the most important elements in the process of encryption, by creating new key generator architectures that allows us to generate pseudorandom 16 different keys to be used in cryptographic, algorithm suitable for hardware or software implementations.These changes, based on genetic algorithm, Simulation study shows that the proposed technique gives a totally different group of pseudorandom subkeys each time we run the generator. Furthermore; comparison analyses between the proposed subkey generation process and the standard technique used in DES. The proposed method is then been evaluated and subjected to many randomness tests in order to measures it is strength. A file has been encrypted using proposed method and the standard technique used in DES, then the randomness of each one is been subjected to test using Statistical Test Suite (STS). The result show that the proposed method gives good result and can be used in future in many cipher for keys generation.

المستخلص

في نظم التشفير المتماثل يستخدم المفتاح الأساسي لإنشاء عدد من المفاتيح الفرعية وفقا لجدوله مفتاح محدده للخوارزميه؛ هنالك مفاتيح معينه تعتبر مفاتيح ضعيفة. يتم تقسيم القيمة الأولية للمفتاح إلى نصفين، ويتم إزاحة كل نصف بصوره مستقله. إذا كانت كل البتات في كل نصف إما 0 أو 1، في هذه الحاله المفتاح المستخدم في كل دوره من الخوارزميه هو نفس المفتاح المستخدم في كل دورات الخوارزميه يمكن أن يحدث هذا إذا كان المفتاح هوعباره عن واحدات او اصفار، أو إذا كان نصف المفتاح واحدات ، والنصف الآخر هو عباره عن اصفار .لهذا السبب ان تصميم جدولة مفاتيح جيده هو جانب هام من تصميم التشفير. في هذا البحث يتم تقديم خوارزميات جديدة لتبسط عملية إنشاء وتوسيع مفتاح التشفير لخوارزمية DES، الذي يعتبر واحدا من أهم العناصر في عملية التشفير، عن طريق إنشاء معمارية توليد جديدة للمفتاح الذي يسمح لنا لتوليد 16 مفتاح شبه عشوائي ومختلفة لاستخدامها في التشفير، خوارزمية مناسبة لتطبيقات العتاد والبرمجيات. هذه التغييرات، استنادا إلى الخوارزمية الجينية، وتبين الدراسة أن النموزج المقترح يعطي مجموعة مختلفة تماما من المفاتيح الفرعية شبه العشوائيه في كل مرة نقوم فيها بعملية توليد المفاتيح. وعلاوة على ذلك؛ مقارنة التحليلات بين عملية توليد الفرعي المقترح والتقنية القياسية المستخدمة في DES. ومن ثم تم تقييم النظام المقترحة وتعرض للكثير من الاختبارات العشوائية من أجل اختبار قوته. تم تشفير ملف باستخدام كل من النظام المقترح وألنظام القياسي المستخدم في DES، ثم اختبار عشوائية كل من الملفين باستخدام Statistical Test Suite(STS). النتيجة تدل على أن

الطريقة المقترحة تعطي نتيجة جيدة، ويمكن استخدامها في المستقبل في العديد من انظمة التشفير لتوليد المفاتيح الفرعية.

Glossary

block

A sequence of consecutive characters encoded at one time.

block length

The number of characters in a block.

cipher

An algorithm for performing encryption (and the reverse, decryption) - a series of well-defined steps that can be followed as a procedure. Works at the level of individual letters, or small groups of letters.

Ciphertext

A text in the encrypted form produced by some cryptosystem. The convention is for ciphertexts to contain no white space or punctuation.

cryptanalysis

The analysis and deciphering of cryptographic writings or systems.

cryptography

The process or skill of communicating in or deciphering secret writings or ciphers

P-value

The probability (under the null hypothesis of randomness) that the chosen test statistic will assume values that are equal to or worse than the observed test statistic value when considering the null hypothesis. The P-value is frequently called the “tail probability”.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES