ISSN: 2410-7727

واجهة تخطيطية لمحاكاة خوارزمية التشفير S-DES

Graphical Interface for Simulation of Encryption Algorithm S-DES

د. إسماعيل إبراهيم الأحمد*

* جامعة الأندلس للعلوم والتقنية، اليمن، صنعاء، ism116620@gmail.com.

ISSN: 2410-7727

ISSN: 2410-7727

واجهة تخطيطية لمحاكاة خوارزمية التشفير S-DES

الملخص:

إن من أشهر خوارزميات التشفير الحديثة هي الخوارزمية القياسية لتشفير البيانات (DES) Data Encryption Standard. ونظرا لأن الخوارزمية DES تتعامل مع مفتاح طوله 64 bits، وكل مقطع من النص الأصلي Plaintext بطول 64 bits يمر خلال 16 دورة تشفير، فإنه يصعب تتبع سير عملياتها أثناء تعليمها أو تعلمها؛ لذا فقد تم استخدام نموذج لخوارزمية مبسطة من الخوارزمية DES وتدعى (S-DES) Simplified DES، ذات مفتاح عام طوله 10 bits ومقطع للنص الأصلي Plaintext طوله 8 bits وتعمل خلال دورتين فقط.

ولتسهيل فهم عمل الخوارزمية S-DES فقد صممت واجهة مرئية مدعمة بمخططات تساعد المستخدم على فهم وتتبع خطوات عملية التشفير وفك الشفرة، وقد تم تمثيل عمليتي التشفير وفك الشفرة للخوارزمية S-DES باستخدام لغة البرمجة المرئية فيجوال بيسك، بحيث تظهر جميع المدخلات والمخرجات على المخطط المرئي لمختلف مراحل عمل الخوارزمية S-DES بوضوح. وقد نُفذ هذا النظام وتم فحصه من خلال عينات مختلفة من البيانات وكانت جميع النتائج صحيحة وموزعة على مخطط الواجهة بشكل صحيح لجميع مراحل عمل الخوارزمية S-DES، كما تم تجربته من خلال تدريس مقرر أمن المعلومات في جامعة الأندلس لمجموعات مختلفة من الطلبة، ولاقى قبولاً وارتياحاً كبيرين من قبل الطلبة نظراً لسهولة استخدامه وفهمه.

الكلمات المفتاحية: واجهة تخطيطية، التمثيل البرمجي، الخوارزمية DES، الخوارزمية S-DES، التشفير، فك الشفرة.

Abstract:

One of the most popular modern algorithms is Data Encryption Standard (DES). Since the algorithm DES uses a key length of 64 bits, and each block of the plaintext with a length of 64 bits goes through 16 rounds, it is difficult to track its operations while it is being taught or learned. Therefore, a mini algorithm of DES, which is called Simplified DES (S-DES), was used with a public key of 10 bits and a plaintext block of 8 bits and operates only two rounds. A visual interface supported by diagrams was designed to facilitate understanding the S-DES algorithm so the user can understand and follow the steps of the encryption and decryption processes. These two processes were implemented using the visual programing language: Visual Basic so that all the inputs and outputs of the steps of the algorithm S-DES are displayed on the graphical diagram clearly.

This system has been executed and tested through different samples of data. All the results were correct and distributed over the interface diagram properly for all the steps of the algorithm S-DES. Moreover, it has been experimented with by teaching the

ISSN: 2410-7727

information security course at Al-Andalus university to different groups of students. It has received great acceptance and satisfaction from students due to its ease of use and understanding.

Keywords: Graphical Interface, Implementation, DES Algorithm, S-DES Algorithm, Encryption, Decryption.

1. المقدمة **Introduction**

لقد اهتم الإنسان منذ القدم باستخدام أساليب مختلفة لحماية البيانات والحفاظ على سريتها، كاستخدام إخفاء البيانات بين حروف الرسائل أو في القصائد الشعرية، أو باستخدام الحبر السري.. الخ. ومع تطور الحاسوب ظهرت طرق التشفير الحديثة في القرن العشرين على يد العالم Shannon الذي جمع في مقترحه كلا من طريقتي النقل والتعويض Transposition & Substitution في تكوين شفرة قوية تقاوم الكسر إلى حد كبير. ومن أشهر هذه الخوارزميات الخوارزمية القياسية لتشفير البيانات Data Encryption Standard (DES). [1, 2]

إن الخوارزمية DES لها أفضلية على جميع الخوارزميات، وذلك لان معظم الخوارزميات الأخرى تستقي أفكارها الرئيسية من خوارزمية DES. لقد تم تطوير الخوارزمية DES في عام 1977 في الولايات المتحدة الأمريكية عن طريق المكتب الوطني الأمريكي للمقاييس NIST.[1]

تتكون الخوارزمية DES من جزئين رئيسيين هما:

1. توليد المفاتيح Key Generation.

2. توليد الشفرة Ciphertext Generation.

الجزء الأول يستخدم مفتاحاً عاماً بطول 64 bits ومنه يتم توليد 16 مفتاحاً فرعياً كل منها بطول 48 bits.

اما الجزء الثاني فيقوم بتوليد الشفرة، حيث تستخدم خوارزمية DES مقطع للنص الأصلي Plaintext بطول 64 bits حيث يتم تشفيره خلال 16 دورة Round، فكل دورة تُنتج شفرة مكونة من 64 bits ليمرر إلى الدورة التالية، وكل دورة تستخدم أحد المفاتيح الستة عشر.

ثم يتم إرسال الشفرة النهائية إلى المستقبل، الذي بدوره يستخدم نفس الخوارزمية ونفس المفتاح العام (مع تعديل طفيف هو عكس ترتيب المفاتيح المشتقة) للحصول على النص الأصلي Plaintext. [3, 4, 9]

ISSN: 2410-7727

أما النموذج المبسط للخوارزمية DES ويدعى Simplified DES (S-DES)، فإنه يتعامل مع مفتاح عام بطول 10 bits ومقطع من النص الأصلي بطول 8 bits ويعمل خلال دورتين فقط.

وكذلك تتكون الخوارزمية S-DES من جزئين رئيسيين هما:

1. توليد المفاتيح Key Generation.
2. توليد الشفرة Ciphertext Generation.

الجزء الأول يقوم بتوليد المفتاحين K_1, K_2 من المفتاح العام، طول كل منهما 8 bits يستخدم كل منهما في دورة من دورتي التشفير اللتان تمثلان الجزء الثاني من الخوارزمية. [5, 7, 8]

وفي هذا البحث نتطرق إلى تصميم وتنفيذ واجهة رسوماتية تساعد المستخدم على فهم واستخدام الخوارزمية S-DES.

2. تعريف المشكلة Problem Statement

على الرغم من أن الخوارزمية S-DES جاءت مبسطة من الخوارزمية DES إلا أن الدارس يجد صعوبة في تتبع تنفيذها بدقة نظراً لتعقيدها وكثرة عملياتها، ومن هنا برزت الحاجة إلى تزويد الخوارزمية S-DES بواجهة تطبيق مرئية كوسيط يساعد المستخدم على تتبع وفهم خطوات تنفيذها.

3. أهداف البحث Research Objectives

1. تقريب مفهوم عمل الخوارزمية DES للدارس.
2. التسهيل على الدارس فهم واستخدام الخوارزمية S-DES.
3. توفير أداة مبسطة للمدرس أثناء شرح الخوارزمية S-DES.
4. الحصول على نتائج حقيقية لعمل خوارزمية S-DES بحيث تستخدم في دراسات وإحصاءات خاصة بالتشفير وفك الشفرة.
5. إعداد نموذج محاكاة للتشفير يمكن استخدامه لغرض تطوير أفكار جديدة في علم التشفير.

ISSN: 2410-7727

4. منهجية البحث Research Methodology

لقد تم إنجاز هذا البحث باتباع الخطوات الآتية:

1. دراسة الخوارزمية DES بالتفصيل.
2. دراسة وتحليل الخوارزمية S-DES وتطبيق الأمثلة المختلفة عليها.
3. تصميم واجهة تخطيطية Graphical Interface مدعمة بمخطط يوضح مسارات عمل الخوارزمية S-DES.
4. توزيع جميع النتائج الجزئية والنهائية على المخطط ليسهل على المستخدم تتبع خطوات عملية التشفير وفك الشفرة.
5. استخدام أكواد برمجية وهياكل بيانات لتنفيذ عمليتي التشفير وفك الشفرة.
6. اختبار النظام على عينات مختلفة من البيانات للتحقق من صحة عمله.
7. اختبار النظام على مجموعات من الطلبة خلال تدريس مقرر أمن المعلومات في جامعة الأندلس للتحقق من فعاليته.

5. الدراسات السابقة

لم يعثر الباحث على دراسات سابقة في مجال هذا البحث، غير أنه وجد دراستين سابقتين مقاربتين لهذا البحث وهما:

1. دراسة **(Elizabeth E. Huntoon, 2018)** بعنوان: "Graphical User Interface To Facilitate Understanding Of Encryption Algorithms"، وتقدم هذه الدراسة واجهات تطبيقية تستخدم مربعات الحوار بدلاً عن استخدام الأوامر النصية لاستخدام بعض خوارزميات التشفير، دون استعراض مراحل عمل هذه الخوارزميات.

2. دراسة **(Mohammed A. Hameed 1, Ahmed I. Jaber, Dr. Jamhoor M.Alobaidy, Alaa A. Hajer, 2018)** بعنوان:
" Design and Simulation DES Algorithm of Encryption for Information Security" وتقدم هذه الدراسة نظام محاكاة لتنفيذ خوارزمية التشفير DES حيث يتم إدخال

ISSN: 2410-7727

النص الأصلي ثم الحصول على النص المشفر، وكذلك دون استعراض مراحل عمل هذه الخوارزمية.

6. نظرة عامة Review

أولاً: خوارزمية التشفير DES [4, 9, 10]

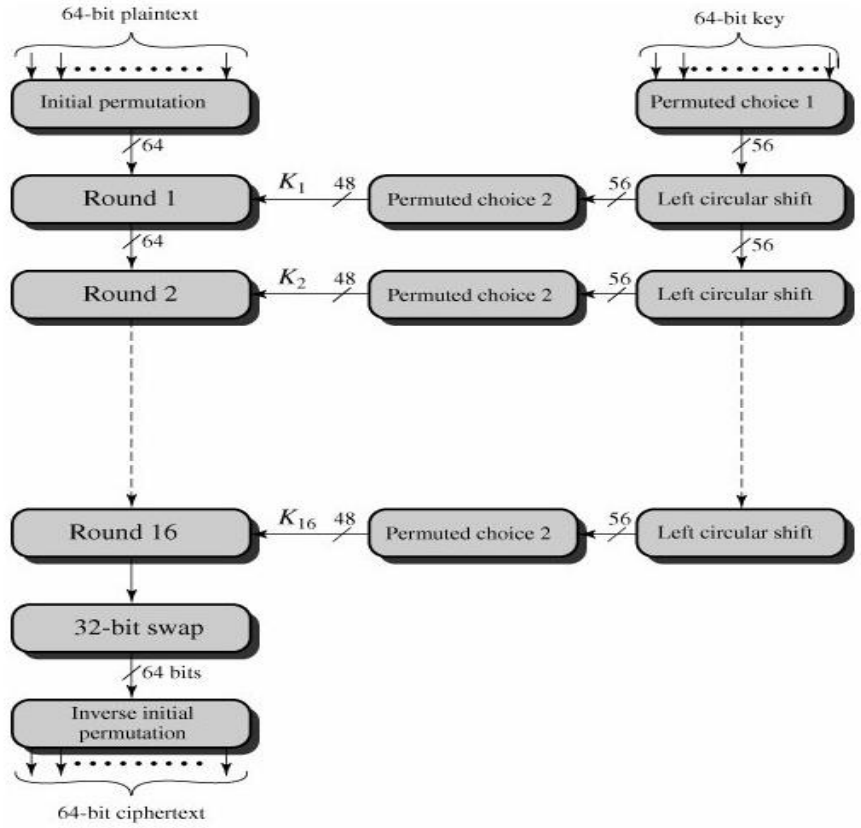
تستخدم الخوارزمية DES في تشفير البيانات بكفاءة عالية في إنجاز عمليتي التشفير وفك الشفرة معاً، وتستخدم مفتاحاً واحدا للعمليتين معا يدعى بالمفتاح العام بطول 64 bits، أي أنها خوارزمية تناظرية Symmetric Algorithm. تقسم الرسالة المراد تشفيرها إلى مقاطع blocks طول كل منها 64 bits، أما المقطع الأخير فيضاف إليه أصفارا إلى نهايته حتى يكتمل طوله إلى 64 bits في حال كان طوله أقل من 64 bits. ويتم تشفير كل مقطع عبر ستة عشر دورة 16 Rounds، الشكل (1) يوضح الهيكل العام للخوارزمية DES.

الجانب الأيمن من الشكل (1) يمثل الجزء الخاص بمعالجة المفتاح العام بطول 64 bits، بحيث يتم تقليصه إلى 56 bits والتبديل بين مواقعها، ومنه يتم توليد المفاتيح الفرعية وعددها 16مفتاحاً وذلك بإجراء عملية إزاحة دورانية لجهة اليسار وعملية تبديل للمواقع لتوليد كل مفتاح فرعي، بحيث كل دورة من الدورات المذكورة تستخدم أحد هذه المفاتيح الفرعية.

أما الجانب الأيسر فيمثل الجزء الخاص بمعالجة النص الأصلي Plaintext لتوليد الشفرة Ciphertext، بدءاً من عملية التبديل الابتدائي لمواقع النص Initial Permutation (IP)، ثم يليها 16 دورة تشفير تعتمد كلٌ منها على عمليتي التبديل والتعويض Permutation and Substitution. والناتج النهائي للدورة الأخيرة 16 Round يتكون من 64 bits، ثم يتم التبديل بين نصفيه الأيسر بطول 32 bits والنصف الأيمن بطول 32 bits، ثم تتم عملية عكسية لعملية تبديل المواقع IP وتدعى IP^{-1} للحصول على الشفرة النهائية.

ويتم فك الشفرة باستخدام نفس الخوارزمية DES، غير أن استخدام المفاتيح الفرعية يتم بصورة عكسية، أي أن يُستخدم المفتاح K_{16} من قبل $Round_1$، والمفتاح K_{15} من قبل $Round_2$، وهكذا وصولاً إلى استخدام المفتاح K_1 من قبل $Round_{16}$.

ISSN: 2410-7727



شكل1: الهيكل العام لخوارزمية التشفير DES

ثانياً: خوارزمية التشفير S-DES [7,8]

كما في الخوارزمية DES، فإن الخوارزمية S-DES تتكون من جزئين رئيسيين هما:

1. توليد المفاتيح Key Generation.
2. توليد الشفرة Ciphertext Generation.

الجزء الاول يقوم بتوليد المفتاحين K_1, K_2 من المفتاح العام، طول كل منها 8 bits، أما الجزء الثاني فيقوم بتوليد الشفرة ويتكون من دورتي تشفير Rounds كل منهما تستخدم أحد المفتاحين الفرعيين K_1, K_2 على الترتيب، الشكل 2 يوضح الهيكل العام للخوارزمية S-DES.

ISSN: 2410-7727

ويعمل الجزء الأول عبر الدوال التالية:

1. 10Permutation (P10): وظيفتها التبديل بين محتويات مواقع المفتاح العام (بطول 10 bits) ، ثم تجزئة الناتج إلى جزئين كل منهما بطول 5 bits.
2. Circular Shift Left (LS1): تستقبل كل جزء من مخرجات الدالة 10P على حدة، وتقوم بعملية إزاحة دورانية لمحتويات كل جزء إلى جهة اليسار بمقدار 1bit.
3. Permutation (P8): وظيفتها دمج الجزئين الناتجين من الدالة 1LS إلى جزء واحد وتقليصه إلى 8 bits ، مع التبديل بين محتويات مواقعها، لينتج المفتاح الفرعي الأول K_1.
4. Circular Shift Left (LS2): تستقبل ناتج كل جزء من مخرجات الدالة 1LS كلاً على حدة، وتقوم بعملية إزاحة دورانية لمحتويات كل جزء إلى جهة اليسار بمقدار 2 bits. ثم تقوم الدالة 8P بنفس ما حصل في الخطوة السابقة لينتج عنها المفتاح الفرعي الثاني K_2.

أما الجزء الثاني فيعمل عبر الدوال التالية:

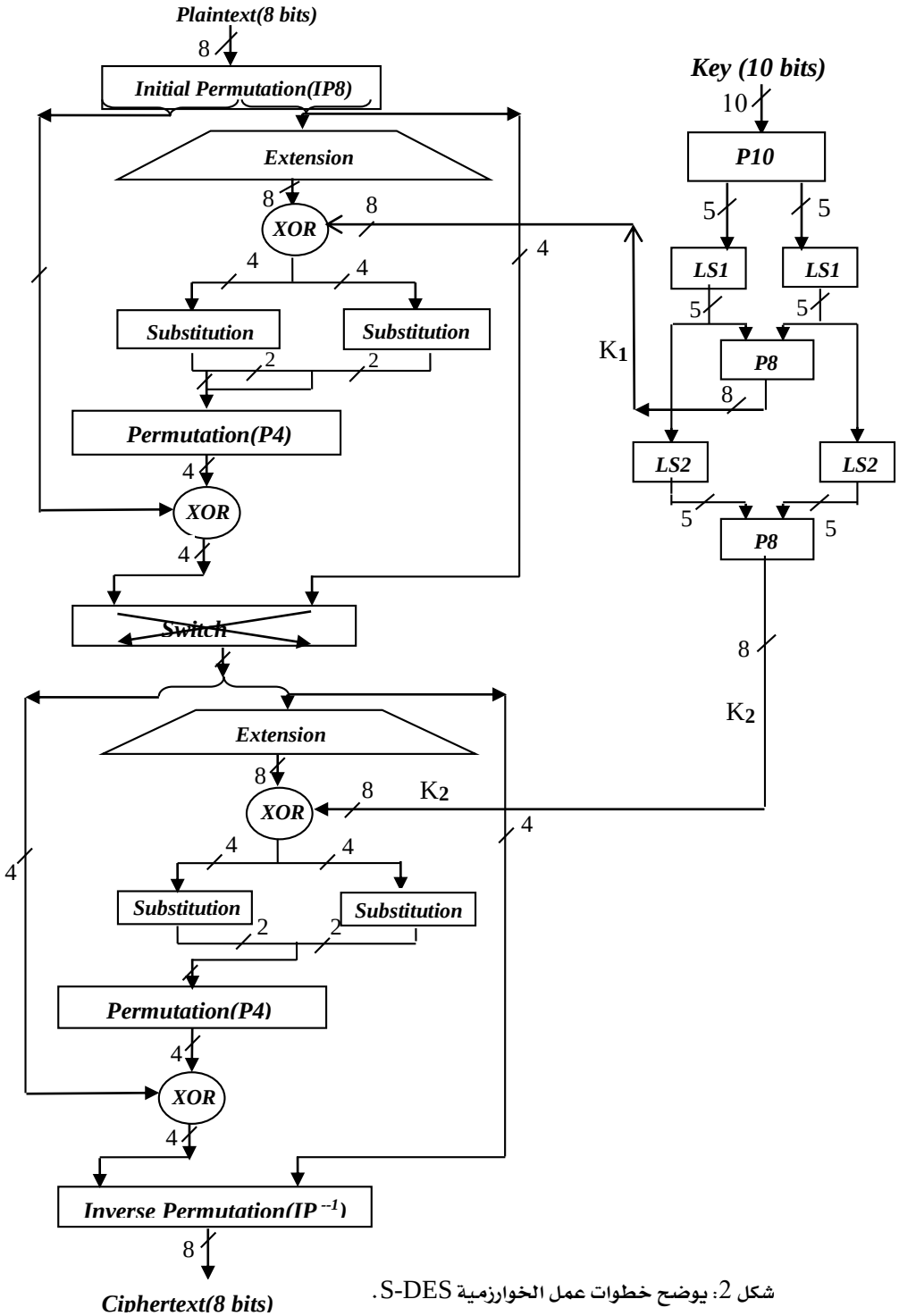
1. Initial Permutation (IP): مدخلاتها النص الأصلي Plaintext بطول 8 bits، وتقوم بالتبديل الابتدائي بين محتويات مواقع النص الأصلي، ثم تجزئ مخرجاتها إلى جزئين، الأيمن بطول 4 bits يستخدم كمدخلات للدالة(Extension Permutation EP)، والأيسر بطول 4 bits ليستخدم لاحقاً.
2. Extension Permutation (EP): تقوم بتبديل محتويات مواقع الجزء الأيمن المذكور في النقطة السابقة (بطول 4 bits)، وتوسعتها بمضاعفة عددها وذلك بتكرارها أو بتكرار بعضها، لتصبح بطول 8 bits. ثم يحدث لناتج التوسعة عملية XOR مع محتويات المفتاح الفرعي الأول K_1، ثم يجزأ ناتج العملية XOR إلى جزئين كل منهما بطول 4 bits ويمرر كل جزء على حدة إلى دالة تعويض Substitution.
3. Substitution : وتستقبل كلاً من الجزئين المذكورين في النقطة السابقة كمدخلات لمصفوفتي التعويض S_0وS_1 حجم كل منهما 4*4، و محتويات كل منهما قيم تتراوح من 0 إلى3، فتقوم الدالة Substitution باستبدال القيم الداخلة إلى كل مصفوفة بإحدى قيم محتويات المصفوفة بعد تحويلها إلى النظام الثنائي لتعطي ناتجاً بطول 2 bits لا علاقة له بالمدخلات.

ISSN: 2410-7727

4. Permutation(P4): وظيفتها دمج الجزئين الناتجين من كل من مصفوفتي التعويض إلى جزء واحد ليصبح بطول 4 bits والذي يستخدم كمدخلات للدالة 4P التي تقوم بالتبديل بين محتويات هذه المدخلات، ثم يحدث لناتج الدالة 4P عملية XOR مع الجزء الأيسر من مخرجات الدالة 8IP.
5. Swap: تستقبل نسخة من الجزء الأيمن من مخرجات الدالة 8IP، و تستقبل مخرجات العملية XOR المذكورة في النقطة السابقة، ثم تبدل بين مواقع كل من الجزئين، بحيث الجزء الأيمن من مخرجات الدالة 8IP يصبح في الجهة اليسرى، ومخرجات العملية XOR تصبح في الجهة اليمنى.

ناتج الدالة Swap يستخدم كمدخلات للدورة الثانية مثلما تم استخدام ناتج الدالة 8IP كمدخلات للدورة الأولى، بحيث تقسم مخرجات الدالة Swap إلى جزئين، الأيمن يستخدم كمدخلات للدالة (Extension Permutation EP)، والأيسر تحدث له عملية XOR مع ناتج الدالة 4P، و ناتج الدالة (Extension Permutation EP) في هذه الدورة تحدث له عملية XOR مع المفتاح الثاني K_2، وناتج هذه العملية XOR يستخدم كمدخلات للدالة Substitution، وناتج الدالة Substitution يستخدم كمدخلات للدالة 4P، وناتج الدالة 4P يحدث له عملية XOR مع الجزء الأيسر من ناتج الدالة Swap. وناتج العملية XOR هذه تدمج مع الجزء الأيمن من ناتج الدالة Swap ليستخدمان كمدخلات للدالة (Inverse Permutation(IP-1 التي تقوم بتبديل مواقع هذه المدخلات بعكس قاعدة التبديل الابتدائي للدالة IP. فنحصل على الناتج النهائي الذي يمثل الشفرة النهائية Ciphertext. ويتم فك الشفرة باستخدام نفس الخوارزمية S-DES، غير أن استخدام المفاتيح الفرعية يتم بصورة عكسية أي أن يستخدم المفتاح K_2 من قبل 1Round والمفتاح K_1 من قبل 2Round، الشكل 2 يوضح عمل الخوارزمية S-DES.

ISSN: 2410-7727



شكل 2: يوضح خطوات عمل الخوارزمية S-DES.

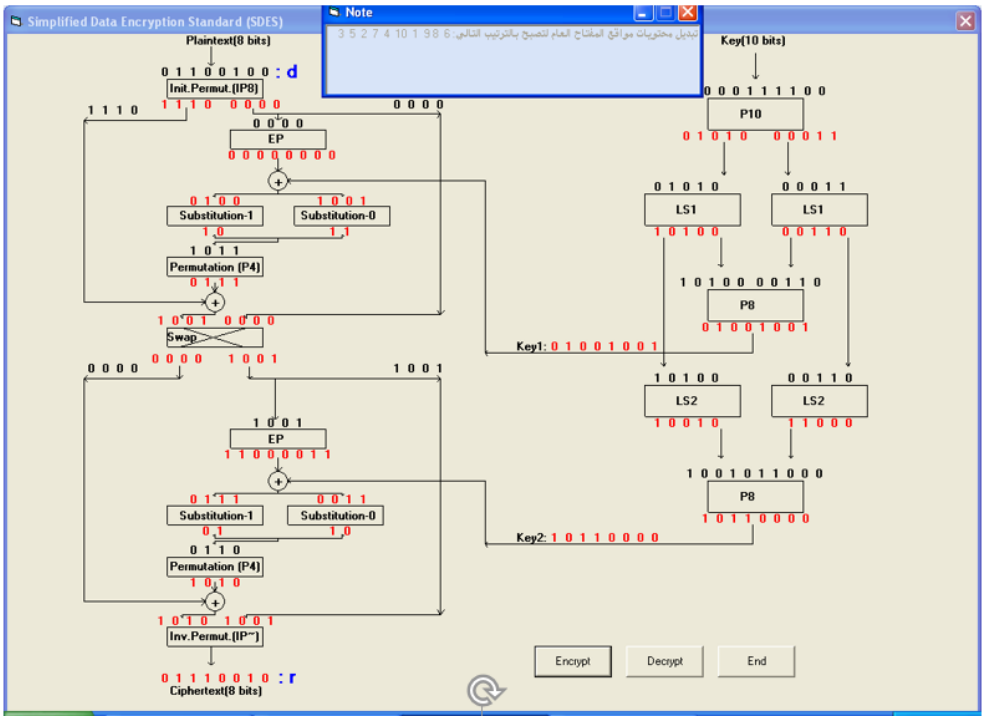
ISSN: 2410-7727

7. التمثيل البرمجي لخوارزمية S-DES S-DES Implementation

لقد تم التمثيل البرمجي لخوارزمية S-DES على شكل نظام برمجي باستخدام لغة فيجوال بيسك، بحيث أُستخدمت فيه هياكل البيانات المناسبة لتمثيل البيانات التي تتعامل معها الخوارزمية S-DES.

وكذلك صُممت أكواد برمجية لمعالجة تلك البيانات، سواء في الجزء الخاص بتوليد المفاتيح الفرعية أو الجزء الخاص بتوليد الشفرة، كما صُممت واجهة رسوماتية مشابهة لمخطط عمل الخوارزمية S-DES في الشكل 2، بحيث تساعد هذه الواجهة المستخدم على فهم وتتبع خطوات عملية التشفير.

ومن أجل الدقة في الرسم وتوزيع المعطيات والنتائج الجزئية والنهائية على المخطط تم استخدام أوامر الرسم بالحاسوب التي تساعد على اختيار الإحداثيات بدقة، الشكل 3 يوضح الواجهة الرسوماتية التي يتعامل معها المستخدم.



شكل **3**: الواجهة الرسوماتية لخوارزمية S-DES

ISSN: 2410-7727

8. النتائج Results

لقد تم فحص النظام واختباره على عدد من مجموعات طلبة الأندلس في تخصص تقنية المعلومات وتخصص نظم المعلومات لمقرر أمن المعلومات وكان له أثر إيجابي لدى الطلبة لتسهيله عليهم فهم واستيعاب طريقة عمل الخوارزمية S-DES في التشفير وفك التشفير.

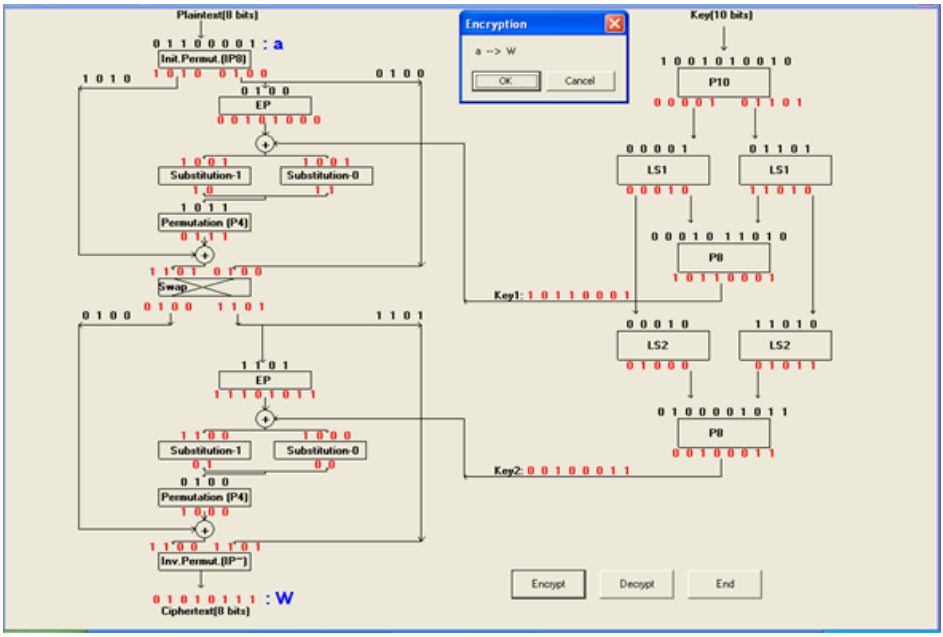
وقد تم تطبيق النظام على عينات مختلفة من البيانات (أنظر الجدول 1) سواء من أجل التشفير أو فك الشفرة، وتم تتبع النتائج الجزئية خطوة خطوة من خلال مسار توليد المفاتيح الفرعية أو من خلال مسار توليد الشفرة، وصولاً إلى النتائج النهائية. حيث تم التحقق من صحة عمل الخوارزمية S-DES. كذلك فإن المثال 1.4 يوضح بالتفصيل خطوات عمل النظام.

جدول 1: عينات ونتائج باستخدام النظام

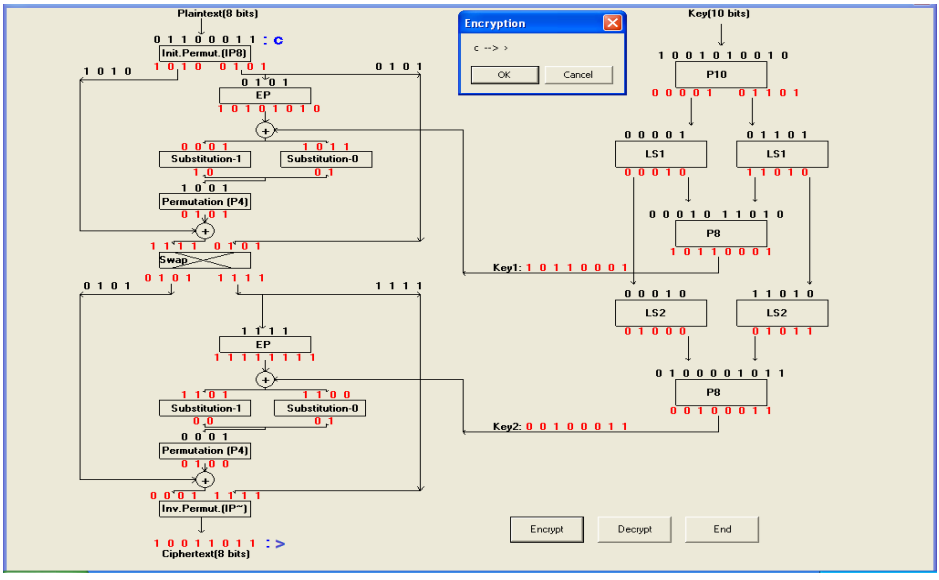
م	النص الأصلي (قبل التشفير)	المفتاح العام	الشفرة	النص الأصلي (بعد فك الشفرة)
1	computer	1000101110	×ªÕ±ât É	computer
2	computer	1111011000	èNTV(·{	computer
3	جامعة	0001110001	Fخ#ه	جامعة
4	Attack	1010100111	c]]Ë4º	Attack
5	attack	1010100111	Ë]]Ë4º	attack

مثال 1: لتشفير النص "abc"، باستخدام مفتاح عام هو 1001010010 فإن النظام يقوم بتوضيح مراحل تشفير النص حرفاً حرفاً بالتفصيل، الشكل 4 يوضح خطوات تشفير الحرف الأول 'a' إلى الحرف 'W'، حيث يُمثِّل الحرف 'a' بالآسكي كود ممثلاً بالنظام الثنائي 01100001، وكذلك الشفرة الناتجة 01010111 والتي تمثل الآسكي كود للحرف 'W'. وبنفس الطريقة يُشَفير الحرف الثاني 'b' إلى الحرف 't' كما في الشكل 5، وتشفير الحرف الثالث 'c' إلى الحرف '<' كما في الشكل 6.

ISSN: 2410-7727



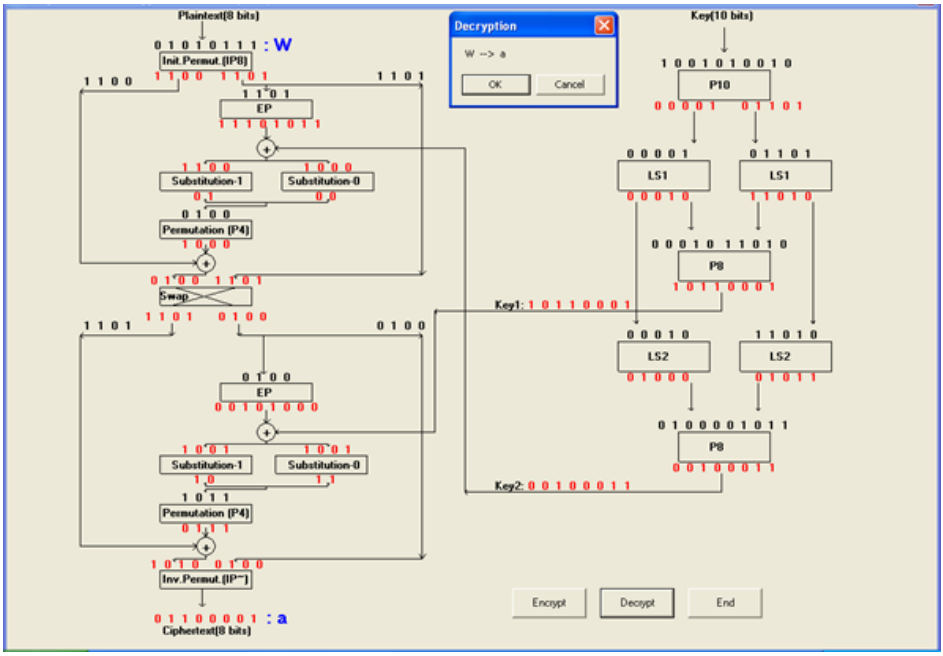
شكل 4: تشفير الحرف 'a' إلى الحرف 'W'



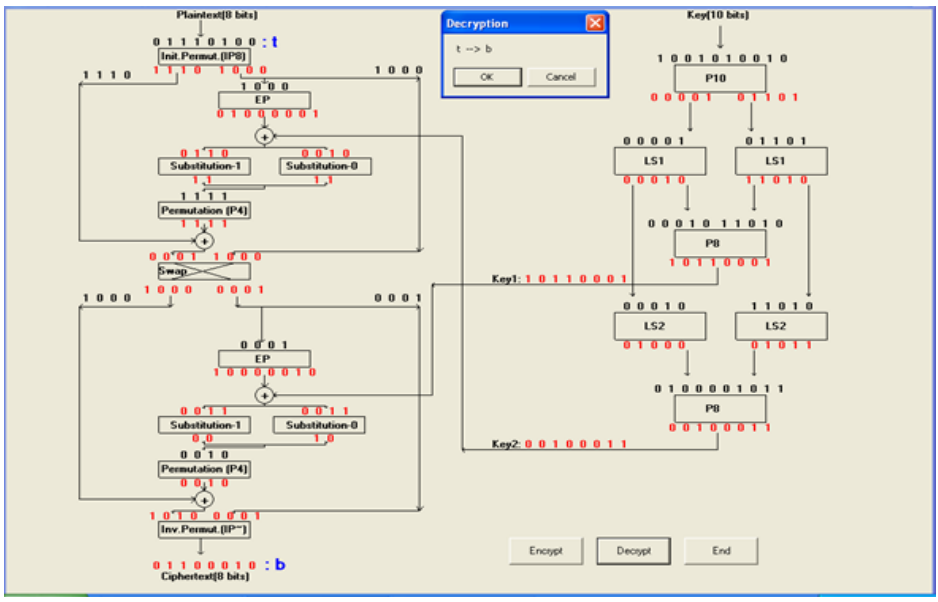
شكل 6: تشفير الحرف 'c' إلى الحرف '>'

ISSN: 2410-7727

وكذلك الأشكال 7, 8, 9 توضح فك الشفرة "Wt>"، للحصول على النص الأصلي "abc". حيث يستخدم نفس المفتاح العام السابق وهو 1001010010، ولكن مع بترتيب عكسي للمفاتيح الفرعية، المفتاح K_2 من قبل الدورة الأولى، بينما يستخدم K_1 من قبل الدورة الثانية، وكما يلي:

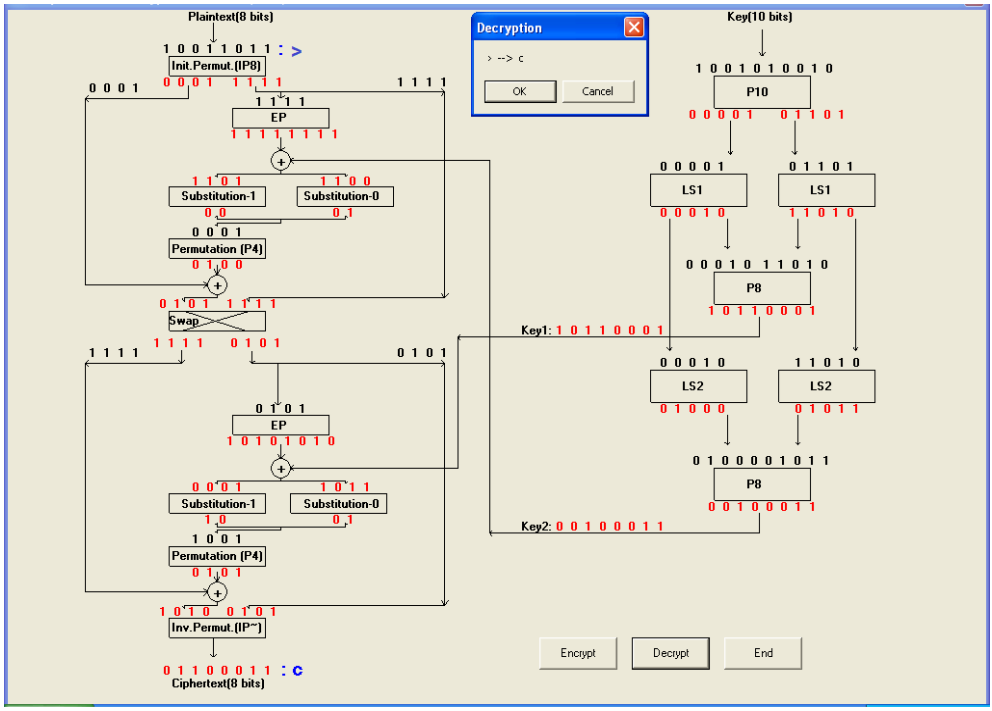


شكل 7: فك الشفرة "W" إلى الحرف "a"



شكل 8: فك الشفرة 't' إلى الحرف 'b'

ISSN: 2410-7727



شكل **9**: فك الشفرة '>' إلى الحرف '**c**'

9. الاستنتاجات **Conclusions**

لقد تم تصميم وتنفيذ النظام المقترح الذي يمثل واجهة تخطيطية للخوارزمية S-DES (النموذج المبسط للخوارزمية DES)، وتميز بسهولة استخدام الواجهة الرسوماتية للنظام ووضوحها. وتم التحقق من صحة النتائج من خلال استخدام عينات مختلفة من البيانات، وكذلك تم اختباره على عدد من مجموعات الطلبة في جامعة الأندلس خلال تدريس مقرر أمن المعلومات، مما يجعل النظام قابلاً للاستخدام كأداة تسهل على المستخدم فهم واستيعاب عمل الخوارزمية S-DES.

10. الأعمال المستقبلية **Future Works**

1. تدعيم النظام بالوسائط المتعددة لعرض الشروحات النصية والصوتية المرافقة لكل خطوة من خطوات تنفيذ الخوارزمية S-DES.
2. تطوير النظام ليتعامل مع تشفير ملفات من البيانات.
3. تطوير نسخ جديدة من النظام لمحاكاة بقية خوارزميات التشفير مثل DES وAES.. الخ.

ISSN: 2410-7727

References المراجع

[1] Joan Daemen, Vincent Rijmen , "The Design of Rijndael: The Advanced Encryption Standard (AES) (Information Security and Cryptography)", 2nd Edition, 2020.

[2] William Stalling, "Cryptography and Network security", 7th Edition, Prenticed Hall, 2016.

[3] Christof Paar, Jan Pelzl, and Bart Preneel, "Understanding Cryptography", 1st Edition, 2010.

[4] Jonathan Katz and Yehuda Lindell, "Introduction to Modern Cryptography", 2007.

[5] Dan Boneh Victor Shoup. "A Graduate Course in Applied Cryptography", 2015.

[6] R. F. Churchhouse, "Codes and ciphers, Julius Caesar, the Enigma and the internet", 2004.

[7] Rajashekarappa, Dr K M Sunjiv Soyjaudah, "Cryptanalysis of Simplified-Data Encryption Standard Using Tabu Search Method" ,2012.

[8] Poonam, G, 2009, “Crypatanalysis of SDES via Evolutionary Computation Techniques”, International Journal of Computer Science and Information Security.

[9] http://homepage.smc.edu/morgan_david/vpn/website-perry-sdes/all-sdes.html#SDES - Simplified DES.

[10] http://www.tropsoft.com/strongenc/des.htm.