تطوير طريقة نكلست للتشفير المتماثل للمقاطع النصية بشكل القطري المتدرج داخل السلسلة المشفرة

Suhad Abbas yassir
Technical Institute, Shattra
suhadabbass@yahoo.com
م.م سهاد عباس ياسر
المعهد التقني/ الشطرة
هيئة التعليم التقني

Nahla Flih Hassani
Assistant Programmer
Nahla_hassani@yahoo.com
م.مبرمج نهلة فليح حساني
كلية التربية الأساس
جامعة سومر

أُستلم 30 تشرين الاول 2013 قُبل 17 آذار 2014

الملخص

تعد هذه الطريقة من الطرق التقليدية ونتيجة للتقدم العلمي في مجال الحاسبات حيث تعتمد على طول المقطع المشفر وطول مفتاح التشفير(Key) المستخدم بين المرسل والمستلم لفك عملية التشفير الحاصل في النص، بحيث تتم عملية قراءة النص المشفر بشكل أفقي داخل المصفوفة بالاعتماد على مفتاح التشفير الذي يعتمد نفسه لفك الشفرة من قبل المستلم , أما في بحثنا الحالي تم تطوير هذه الطريقة وجعلها أكثر تعقيدا من اجل المحافظة على النص المشفر الذي يجب أن يكون محميا بأكثر من طريقة او وسيلة يستخدمها الباحث لكي تتم عملية التشفير بشكل أكثر فاعلية حيث تم إضافة بعض الصيغ رياضية لإخراج النص المشفر الذي يعتمد على العلاقة بين أعمدة وصفوف في مصفوفة كذلك تتم قراءة الحروف الموجودة داخل المصفوفة بشكل أخر اعتمادا على النهاية المضافة على الخوارزمية لكي تتم قراءتها بشكل قطري متدرج للقطر الرئيسي أولا ثم الحروف الموجودة فوق القطر الرئيسي وأخيرا الحروف الموجودة أسفل القطر الرئيسي.

Develop a way Nklst Symmetric encryption for text clips in diameter gradient inside the encrypted string

Abstract

The aim of this Paper is Find anew scheme for text encryption. This process depending an reading the cipher horizontally within the matrix which depends on the relationship between the

columns & rows in the matrix & the end which added to the algorithm to be read diagonally graded diameter.

1-المقدمة:

التشفير هو احد عمليات اخفاء المعلومات المهمة او نقلها بحيث لا يمكن قراءتها الا من قبل المرسل والمستلم وتعتبر احد أنواع الحفظ لسرية المعلومات المستخدمة.

ويعتبر التشفير من العلوم التي تأخذ طابع التطوير بشكل مستمر بحيث يستخدم طرق متنوعة تسعى الى سرية للمعلومات المرسلة عبر قنوات الاتصال المختلفة. ونتيجة للتطور الحاصل في علم الحاسوب التي يهدف الى إيجاد وسائل مختلفة لضمان جودة العمل المنجز احدها طرق حماية المعلومات عن طريق تطوير التقنيات في علم التشفير لتكون فعالة في الحفاظ على المعلومات من خلال أنظمة معلومات دفاعية. ففي العقود الثلاثة الأخيرة قُدمت عدة طرق تشفير لكي تحمي العديد من وسائل الاتصال مثل الفيديو والصور الرقمية. أنها مفيدة جدا في تقديم أغراض سرية خاصة في تطبيقات حقيقة كخدمات الإرسال متعددة الوسائل والمؤتمرات الفيديوية السلكية واللاسلكية وكذلك الصور العسكرية...الخ. (Rabinovich,Vlad 2004)

ومن الأهداف التي يسعى اليها معظم الباحثون هو حصولهم على طرق تشفير تتناسب مع حجم المعلومات المرسلة من جانب ومن الجانب الأخر استخدام او تطوير الطرق التي باتت معروفة او سهلة الاستخدام بحيث تكون أكثر فاعلية في حفظ المعلومات المهمة .

ويعد هدف اغلب برامج التشفير هو التحقيق وصول المعلومات السريعة وبمستوى عالي من السرية والأمان , واحدة من هذه البرامج هو تشفير الكلي او الجزئي من النص وبمختلف الطرق من اجل ضمان الحفاظ على مستوى المعلومات المرسلة .(Alan, G, 2007.)

2- تشفير النصوص:

تقنية التشفير cryptography هي فن حماية المعلومات عن طريق تحويلها إلى رموز معينة غير مقروءة تدعى النصوص المشفرة cyphertext لا يمكن حلها إلا من خلال مفتاح سري يقوم بفك ذلك التشفير وتحويله إلى نص عادي مقروء، ونظراً للانتشار الكبير الذي حققته الاتصالات الإلكترونية وخصوصاً الإنترنت، فقد غدا الأمن الإلكتروني من أسخن القضايا التي يركز عليها العالم بأجمعه، وتستخدم تقنية التشفير في هذا المجال لحماية الرسائل الإلكترونية والمعلومات المهمة المنقولة إلكترونياً كالبيانات المتعلقة ببطاقات الائتمان والبيانات الخاصة. (Iyengar,Venugopal.2003)

والهدف من التشفير هو ضمان حفظ الخصوصيات وعدم السماح لأحد بالعبث بها أو الاطلاع عليها وذلك كونها إما سرية أو خاصة جداً، ولا يمكن لأحد أن يفهم مضمون تلك المعلومات أو الرسائل إلا من لديه

المفتاح السري الخاص بها والذي تتم عن طريقه عملية فك التشفير Decryption أي إعادة البيانات إلى صيغتها الأصلية كنص عادي .

وتتطلب كل من عمليتي التشفير وفك التشفير استخدام بعض التعليمات السرية التي يشار إليها عادة بمفاتيح خاصة. وتستخدم بعض تقنيات التشفير المفتاح نفسه في العمليتين في حين تختلف تلك المفاتيح من عملية لأخرى في تقنيات أخرى. (Peeter Laud,Varmo Vene 2005)

ولكن تقنيات التشفير اليوم أعقد بكثير وأكثر تطوراً من مجرد التشفير وفك التشفير، وفي الواقع أن موضوع أصالة وصحة البيانات والمعلومات لا يقل أهمية بالنسبة إلى الجميع عن موضوع الخصوصية، فكما نقوم في حياتنا اليومية بالتوقيع مثلاً على مستند ما أو البصم عليه للدلالة على أنه صحيح فإننا بحاجة في المقابل إلى نظام يضمن الشيء ذاته ولكن بطريقة إلكترونية، كما يشمل موضوع التشفير أموراً أخرى كثيرة فمن خلال أدوات معينة يمكن بناء برامج وأنظمة معقدة تتيح إمكانية الدفع باستخدام المال الإلكتروني . (Qi, Hairong,2002)

2-1 التشفير المتماثل:

يعد الاهتمام بعلم التشفير في الوقت الحالي من المواضيع التي يعنى بها الكثير من الباحثين من اجل تامين النصوص او المعلومات بالشكل الذي يكون آمناً ومضموناً تماماً وأن يكون يشكل متكامل من جميع جوانبه وبكافة أغراضه، وفي الوقت ذاته فإن للتشفير أنواع كثيرة وتقنيات مختلفة، "ومن تلك التقنيات هنالك تقنية المفتاح السري Secret Key وهي من التقنيات العلمية التي يعتمد فيها كل من المرسل والمرسل إليه المفتاح السري ذاته، حيث يقوم الأول باستخدام ذلك المفتاح لتشفير الرسالة فيما يستخدمه الثاني لفك ذلك التشفير وقراءته، وتعرف هذه الطريقة باسم التشفير المتماثل symmetric cryptography" . (Papamarkos,2000) وان مثل هذه الطريق التي تسهل عملية وصول المعلومات إلى الشخص المراد إرسال مثل هذه النصوص بسرية وأمان الى الشخص المعني وهي تحقق متطلبات العمل الناجح بين كلا الطرفين من خلال معرفة الشفرة الخاصة بالخوارزمية المستخدمة في تطبيق التشفير. ومن اجل تامين النص الصريح الذي يتكون $X = [X_1, X_2, ... X_m]$ ولانجاز تكوين المفتاح $K = [K_1, K_2, ..., K_j]$. كما في شكل (1)

2-2- طريقة نكلست:

تعتمد هذه الطريقة على طول المقطع المشفر وكذلك على طول مفتاح التشفير(Key) المستخدم بين المرسل والمستلم لفك عملية التشفير الحاصل في النص، وفي نفس الوقت ان المقطع المشفر يجب ان يكون النص المستخدم فيه عدد من الأحرف التي يكون لها عددا زوجيا من الأحرف مضاف لها عدد الفراغات التي تكون محسوبة مع عدد الأحرف المراد تشفيرها ، أما في حالة أذا كان عدد الأحرف المراد تشفيرها في المقطع بشكل فردي يضاف إلى هذه الأعداد فراغ واحد لكي يصبح العدد الكلي للمقطع المشفر عددا زوجي

حيث تعتمد الخوارزمية على طول النص الصريح X وطول المفتاح K من أجل توليد النص المشفر K والمفتاح X تقوم الخوارزمية باستخدام النص الصريح $Y = [Y_1, Y_2 ...., Y_N]$ التي يمكن كتابتها على النحو التالي $Y = E_K(X)$

وبمعنى اخر يمكن استنتاج Y من خلال الخوارزمية E بالاعتماد على كل من [K,X] .

3- خوارزمية التشفير :

ان الغاية الأساسية لعمل كل باحث من خلال الانسجام والاتفاق مع طبيعة الهدف الذي يسعى لتحقيقه وفي اغلب عمليات التي يستند عليها كل الباحثون هي المبادئ او القواعد الأساسية لهذا العمل لذ اتجه عمل الباحثتان في هذا البحث لتطوير احد الطرق التشفير.

1.حساب طول النص المطلوب تشفيره وجعله بالمتغير n .

2.حساب طول مفتاح التشفير وجعله بالمتغير j .

3. ايجاد قيمة المتغير i بحيث أن i=n/j .

4. تقطيع النص المطلوب تشفيره وخزن كل حرف منه بموقع من مواقع المصفوفة a(i,j) بحيث يكون الحرف الأول بـ(الصف الأول والعمود الأول) والحرف الثاني بـ(الصف الأول والعمود الثاني) ....وهكذا .

5.تعاد الخطوة رقم 4 الى أن يتم ادخال كل حروف النص بالمصفوفة a(I,j) .

6. تقطيع مفتاح التشفير واخذ أول رقم منه وجعله بالمتغير k ليمثل رقم العمود بالمصفوفة a ليتم بعد ذلك أخذ الحروف الموجودة بالعمود رقم k من المصفوفة a(I,k) وجعلها بالعمود الأول من مصفوفة التشفير b(I,j) بحيث أن d=a(I,k) , b(I,j)=d .

7. تكرار الخطوة رقم 6 حتى يتم قراءة أخر رقم من أرقام مفتاح التشفير ليتم من خلاله ادخال آخر عمود من أعمدة مصفوفة التشفير b .

8. اخراج النص المشفر وخزنه بالمتغير s من خلال قراءة الحروف الموجودة بالمصفوفة b(I,j) حيث يتم أخذ الحرف الأول من (الصف الأول ,العمود الأول) وجعله بالمتغير s ثم أخذ الحرف الثاني من (الصف الأول , العمود الثاني) واضافته الى محتويات المتغير s ... وهكذا.

9. تعاد الخطوة رقم 8 حتى يتم الانتهاء من أخذ حروف الصف الأخير من مصفوفة التشفير b(I,j) واضافتها الى المتغير s.

10.طباعة المتغير s ليمثل النص المشفر . كما موضح في (Flow Chart 1).

3-1 خوارزمية فك الشفرة :

1.حساب طول النص المشفر وجعله بالمتغير n .

2.حساب طول مفتاح التشفير وجعله بالمتغير j .

3. ايجاد قيمة المتغير i بحيث أن i=n/j .

4. تقطيع مفتاح التشفير واخذ أول رقم منه وجعله بالمتغير k ليمثل رقم العمود بمصفوفة فك التشفير C ليتم بعد ذلك أخذ الحروف الموجودة بالعمود الأول من المصفوفةB(I,J) وجعلها بالعمود رقم K من مصفوفة فك التشفير C بحيث أن d=b(x1,y1) ومنه c(x1,k)=d .

5. تكرار الخطوة رقم 4 حتى يتم قراءة أخر رقم من أرقام مفتاح التشفير ليتم من خلاله أخذ آخر عمود من أعمدة المصفوفة B وادخاله بالعمود رقم K من المصفوفة C .

6. اخراج النص الصريح وخزنه بالمتغير S1 من خلال قراءة الحروف الموجودة بالمصفوفة C(I,j) حيث يتم أخذ الحرف الأول من (الصف الأول ,العمود الأول) وجعله بالمتغير S1 ثم أخذ الحرف الثاني من (الصف الأول , العمود الثاني) واضافته الى محتويات المتغير S1 ... وهكذا.

7. تعاد الخطوة رقم 6 حتى يتم الانتهاء من أخذ حروف الصف الأخير من مصفوفة فك التشفير C(I,j) واضافتها الى المتغير S1 .

8.طباعة المتغير S1 ليمثل النص الصريح . كما مبين في شكل(3)

4- الطريقة الجديدة (القطرية):

تم تطبيق الطريقة على النصوص من اجل تشفيرها بشكل أكثر تعقيدا من خلال استخدام برمجه في لغة (فجول بيسك) لتشفير وإرسال النص بسلامة وأمان أكثر من خلال الإضافات التي جعلت من المصفوفة أكثر تعقيدا عما كانت علية

ويقوم البرنامج بحساب طول النص المشفر الذي يشترط ان يكون الناتج النهائي مع الفراغات عددا زوجيا ومن ثم يقوم البرنامج بقراءة طول المفتاح الذي يجب ان يكون ضمن عوامل العدد الزوجي لطول النص فمثلا يكون طول النص المشفر متكون من (16) حرفا فيجب ان يكون المفتاح المستخدم يتكون من أربعة أرقام من عوامل العدد لنص المشفر فالأرقام (4) تكون من عوامل العدد(16) حرفا بحيث يتم إدراج الأربعة أرقام بشكل مبعثر لا على التعيين أي بطريقة عشوائية مثلا (4123) والغرض من ذلك وضع النص الصريح بمصفوفة عدد أعمدتها مساوي لطول المفتاح وعدد صفوفها = طول النص مقسوما على طول المفتاح .

وبعد ذلك يقوم البرنامج بوضع النص المشفر بمصفوفةٍ a= [i,j] كل حرف بمكان وكما مبين

$$A=[I,j]\begin{pmatrix} S & u & m & m \\ E & r & - & u \\ N & I & v & e \\ R & s & t & y \end{pmatrix}$$

تعتمد طريقة التشفير من خلال إبدال أعمدة المصفوفة بالاعتماد على عدد الأرقام المدخلة للمفتاح والتي كانت بالمثال أعلاه (4123) لكي يتم وضع المصفوفة بشكلها الطبيعي [i,j] =B وعلى النحو التالي التي من خلالها يتم قراءة النص المشفر من المصفوفة (b) بدلا من المصفوفة (A)

$$b\,[I,j] = \begin{pmatrix} M & s & u & m \\ U & e & r & - \\ E & n & I & v \\ Y & r & s & t \end{pmatrix}$$

يتم التشفير من خلال تبديل أماكن الحروف بالمصفوفة بالاعتماد على الأرقام الموجودة بالمفتاح Key وهذه هي طريقة نيكلست , وفي ما يخص الإضافة التي تم اعتمادها من اجل تطوير هذه الطريقة وذلك من خلال إضافة صيغ رياضية أخرى لإخراج النص المشفر يعتمد هذه الصيغ هذه الصيغ الرياضية المستندة على العلاقة بين أعمدة وصفوف داخل مصفوفة التشفير .

حيث يتم قراءة المتدرجة للحروف الموجودة داخل المصفوفة للقطر الرئيسي أولا ثم الحروف الموجودة فوق القطر الرئيسي وأخيرا الحروف الموجودة أسفل القطر الرئيسي وكما موضح في الخوارزمية.

4-1 الخوارزمية الجديدة :

1.حساب طول النص المطلوب تشفيره وجعله بالمتغير n .

2.حساب طول مفتاح التشفير وجعله بالمتغير j .

3. إيجاد قيمة المتغير i بحيث أن i=n/j .

4. تقطيع النص المطلوب تشفيره وخزن كل حرف منه بموقع من مواقع المصفوفة a(i,j) بحيث يكون الحرف الأول بـ(الصف الأول والعمود الأول) والحرف الثاني بـ(الصف الأول والعمود الثاني) ....وهكذا .

5.تعاد الخطوة رقم 4 إلى أن يتم إدخال كل حروف النص بالمصفوفة a(I,j) .

6. تقطيع مفتاح التشفير واخذ أول رقم منه وجعله بالمتغير k ليمثل رقم العمود بالمصفوفة a ليتم بعد ذلك أخذ الحروف الموجودة بالعمود رقم k من المصفوفة a(I,k) وجعلها بالعمود الأول من مصفوفة التشفير b(I,j) بحيث أن b(I,j)=d , d=a(I,k) .

7. تكرار الخطوة رقم 6 حتى يتم قراءة أخر رقم من أرقام مفتاح التشفير ليتم من خلاله إدخال آخر عمود من أعمدة مصفوفة التشفير b .

8. إخراج النص المشفر وخزنه بالمتغير s من خلال قراءة الحروف الموجودة بالقطر الرئيسي للمصفوفة b(I,j) ثم الحروف الموجودة فوق القطر الرئيسي ثم الحروف الموجودة تحت القطر الرئيسي أي أنه :

S= (حروف القطر الرئيسي)+(الحروف فوق القطر الرئيسي)+(الحروف أسفل القطر الرئيسي)

2-4 خوارزمية فك الشفرة :

1.حساب طول النص المشفر وجعله بالمتغير n .

2.حساب طول مفتاح التشفير وجعله بالمتغير j .

3. إيجاد قيمة المتغير i بحيث أن i=n/j .

4. إدخال النص المشفر بالمصفوفة b(I,j) بثلاث مراحل حيث يتم أولا إدخال عناصر القطر الرئيسي ثم عناصر فوق الرئيسي وأخيرا عناصر تحت القطر الرئيسي .

5. تقطيع مفتاح التشفير واخذ أول رقم منه وجعله بالمتغير k ليمثل رقم العمود بمصفوفة فك التشفير C ليتم بعد ذلك أخذ الحروف الموجودة بالعمود الأول من المصفوفةB(I,J) وجعلها بالعمود رقم K من مصفوفة فك التشفير C بحيث أن d=b(x1,y1) ومنه c(x1,k)=d .

6. تكرار الخطوة رقم 4 حتى يتم قراءة أخر رقم من أرقام مفتاح التشفير ليتم من خلاله أخذ آخر عمود من أعمدة المصفوفة B وإدخاله بالعمود رقم K من المصفوفة C .

7. إخراج النص الصريح وخزنه بالمتغير S1 من خلال قراءة الحروف الموجودة بالمصفوفة C(I,j) حيث يتم أخذ الحرف الأول من (الصف الأول ,العمود الأول) وجعله بالمتغير S1 ثم أخذ الحرف الثاني من (الصف الأول , العمود الثاني) وإضافته إلى محتويات المتغير S1 ... وهكذا.

8. تعاد الخطوة رقم 6 حتى يتم الانتهاء من أخذ حروف الصف الأخير من مصفوفة فك التشفير C(I,j) وإضافتها إلى المتغير S1 .

9.طباعة المتغير S1 ليمثل النص الصريح . كما مبين في شكل(5)

5- الاستنتاجات :

ارتأت الباحثتان القيام بطريقة مقترحة للتطوير طريقة نكلست لتشفير وجعها أكثر فاعلية بحيث يصعب على الآخرين اختراقها ولتامين وصول المعلومات بشكل أكثر دقة.

في طريقة التشفير الجديدة التي تم من خلالها إضافة بعض العلاقات رياضية الخاصة للأعمدة وصفوف داخل المصفوفة يتم التعامل بشكل قطري متدرج ، استنتجت الباحثتان ان هذه الطريقة أصبحت أكثر فاعلية من خلال التعامل بشكل قطري متدرج وهذ يصعب على الآخرين الغير معنيين فك هذه الشفرة فضلا عن الفترة الزمنية التي تستخدم بين المرسل والمستلم تكون بشكل مباشر ولا تتطلب وقت طويل لكي يتسنى لهم التحاور فيما بينهم بشكل سريع مع الشفرة وكأنه عملية إرسال رسائل يمكنهم الإجابة عليها بسرعة على الرغم من وجود تشفير داخل هذه النصوص. كذلك تعمل الإضافة الجديدة

بتكوين نص مشفر يتكون من ثلاث أجزاء في الجزء الأول للحروف الموجودة بالقطر الرئيسي من المصفوفة, الجزء الثاني الحروف الموجودة فوق القطر الرئيسي والجزء الثالث العناصر الموجودة تحت القطر الرئيسي التي تجعلها أكثر حماية مما كانت عليه .

REFERANCES

[1] Rabinovich, Vlad: "Steganography–a Cryptography Layer" . Accessed, Jan,2004,p80.

[2]. Alan G. , Computer security & cryptography , Prentice Hall : United States of merica, 2007, P 101.

[3] Iyengar, Venugopal,;"Hiding Messages in Images and Text:Risk Associated with the Technology of Steganography", ISACA InfoBytes Journal, 2003, p98.

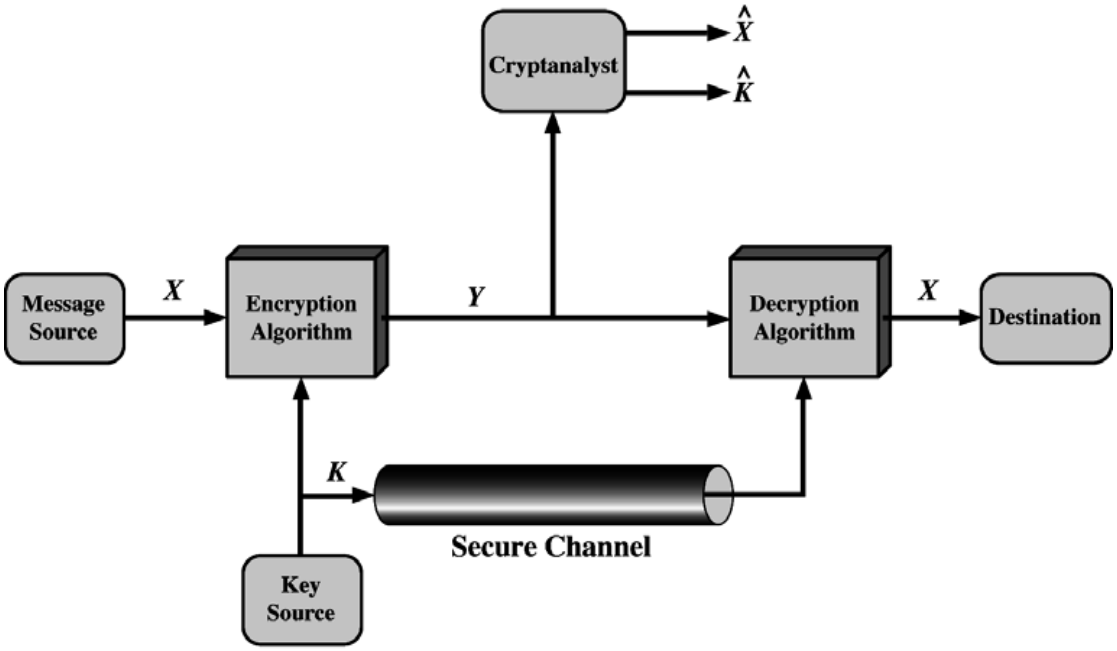
[4] Peeter Laud and Varmo Vene: A type system forc omputationally secure information flow. In Maciej Liskiewicz and R¨udiger Reischuk, editors, FCT, volume 3623 of LNCS2005, p 365–377. Springer,.

[5] J. Daemen and V.Rijmen, "The Design of Rijndael, Advanced Encryption Standard", ISBN 3-540-42580-2, Springer-Verlag,Berlin, 2002.

[6] N. Papamarkos and A. Atsalakis: "Gray-Level Reduction Using Local Spatial Features", Computer Vision and Image Understanding,2000,p 78 .

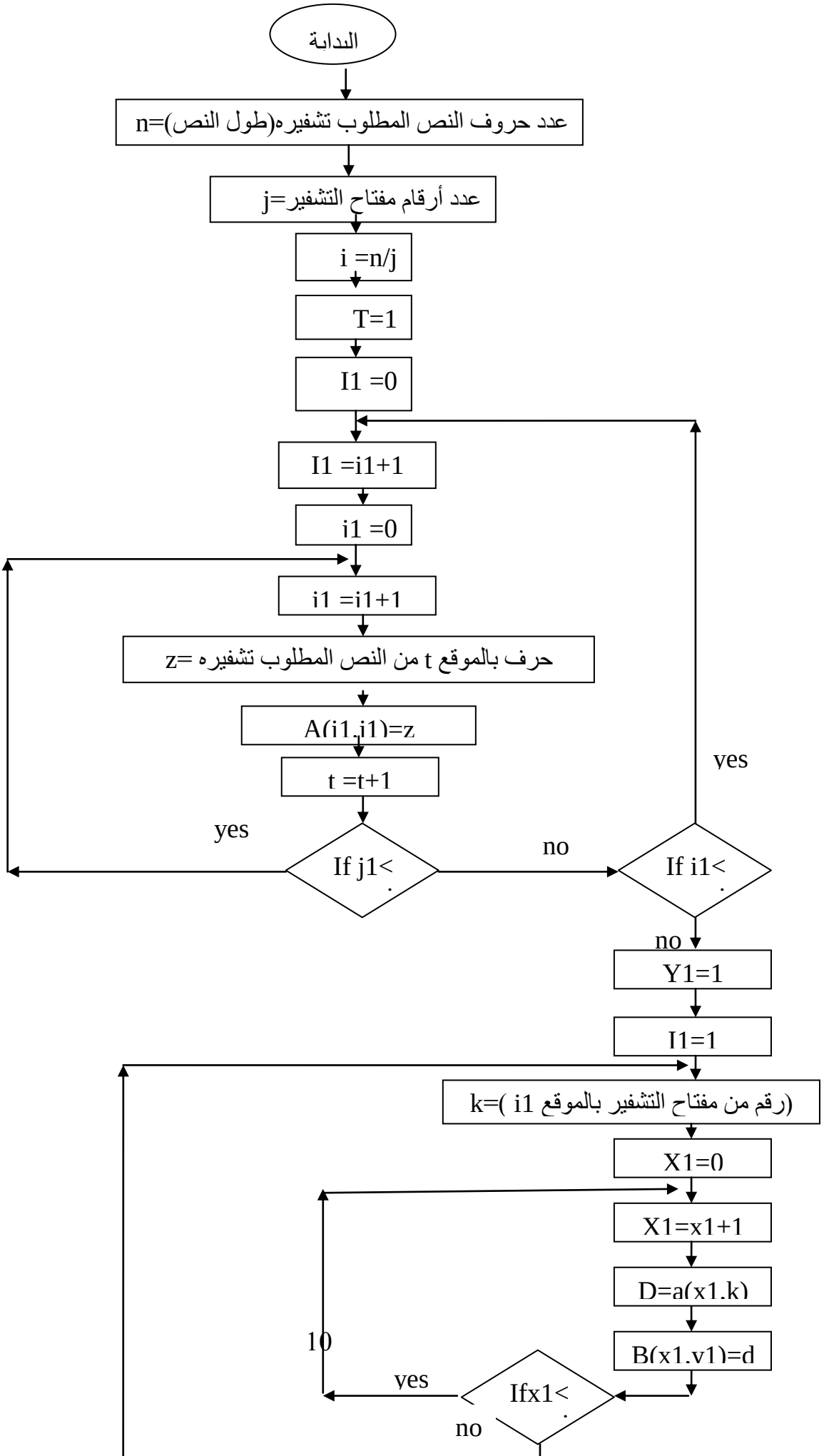
[7]Geoffrey Smith and Rafael Alpzar: Secure information flow with random assignment and encryption. In FMSE, 2006, p 33–44.

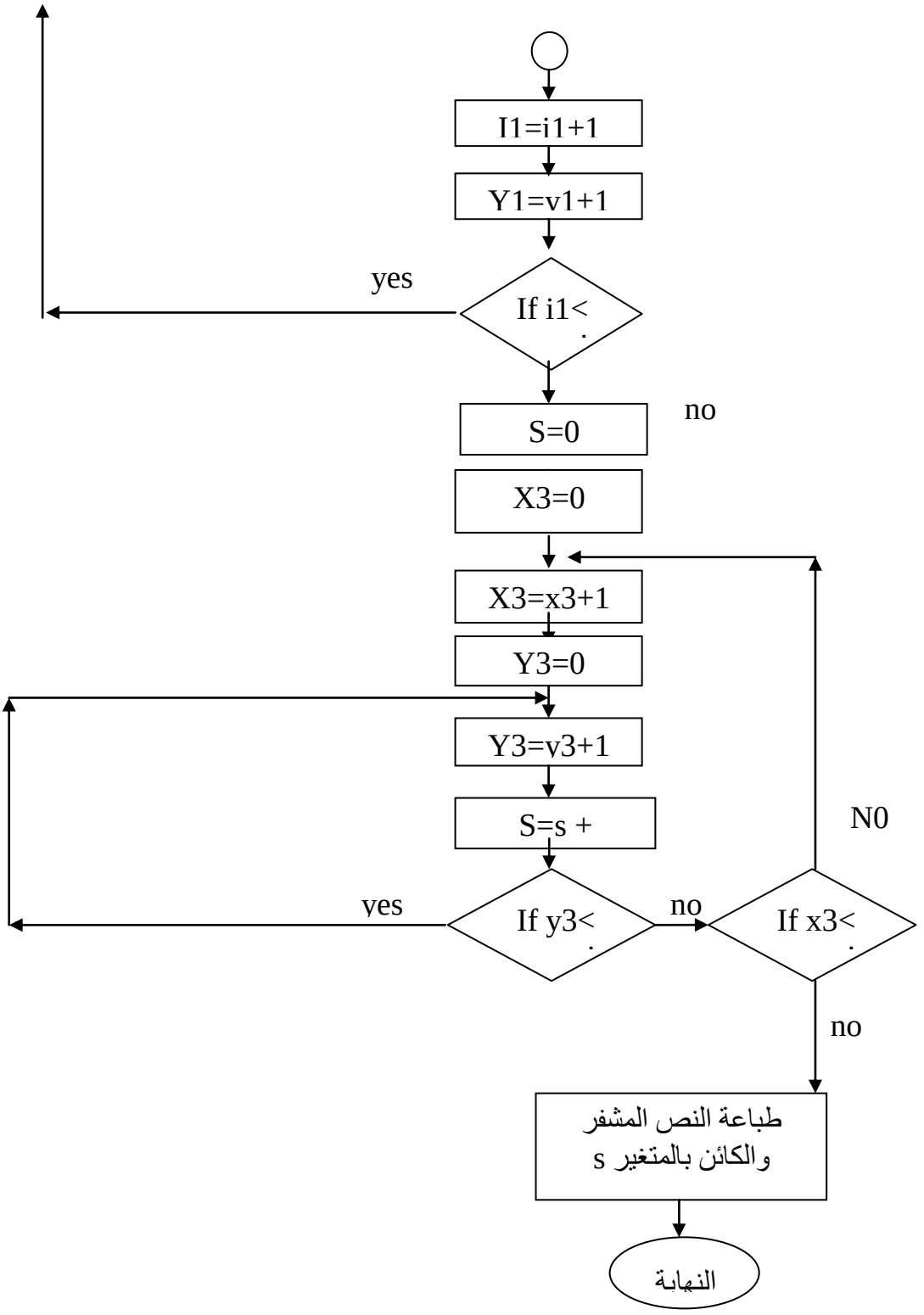
[8] Qi, Hairong, Snyder, Wesley E. & Sander, William A.: " Blind Consistency-Based Steganography for Information Hiding in Digital Media". Multimedia and Expo, 2002. ICME '02. Proceedings. 2002 IEEE International Conference on Vol. 2002, p, 585- 588.



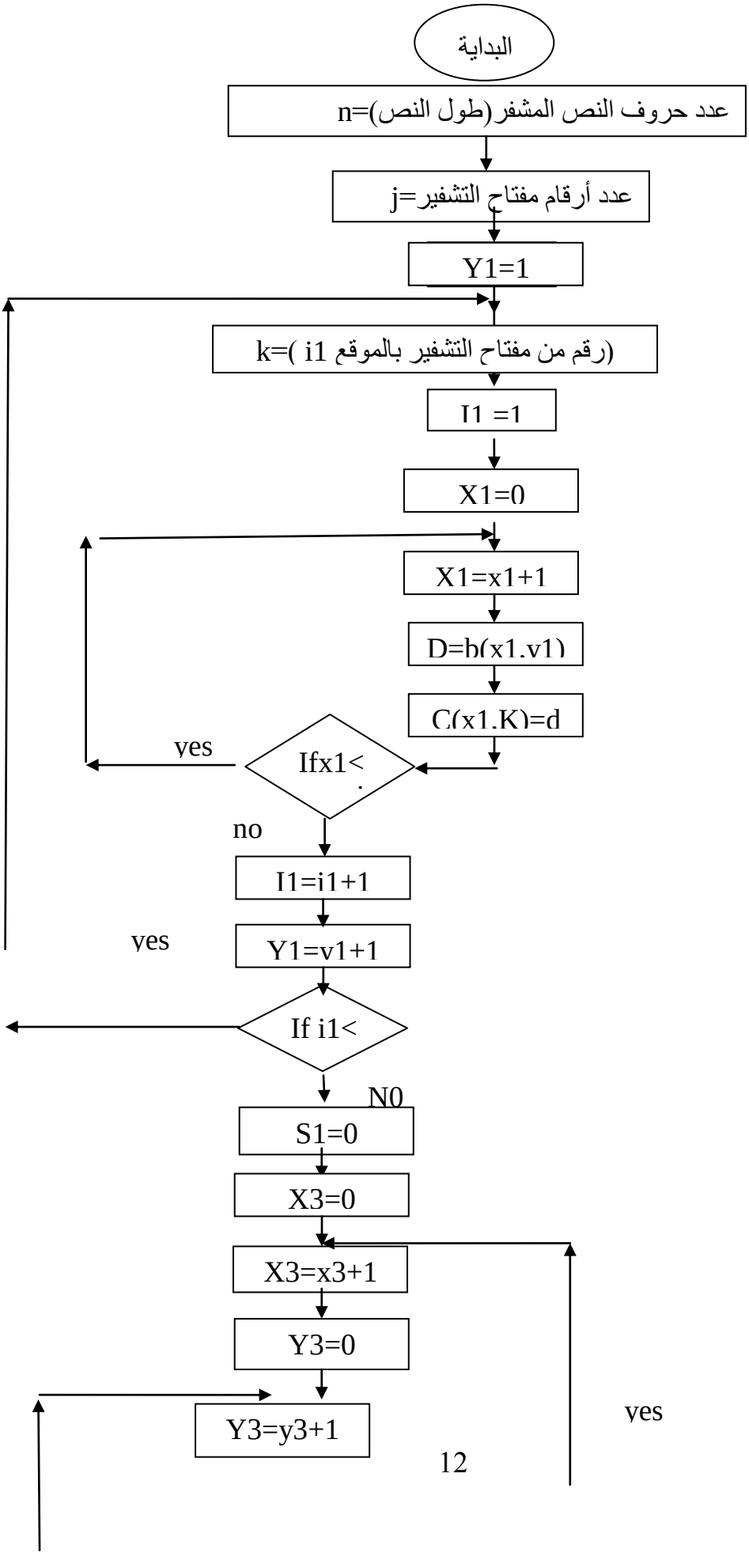
(Daemen ,2002)….

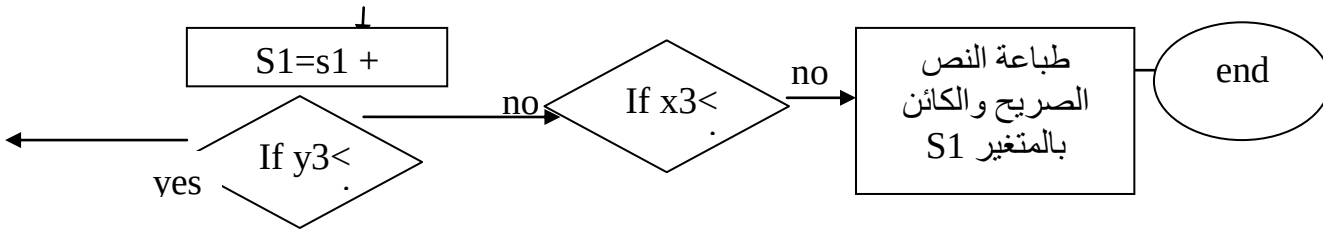
شكل (1) نموذج للتشفير المتماثل


البداية
عدد حروف النص المطلوب تشفيره(طول النص)=n
عدد أرقام مفتاح التشفير=j
i =n/j
T=1
I1 =0
I1 =i1+1
i1 =0
i1 =i1+1
حرف بالموقع t من النص المطلوب تشفيره =z
A(i1,j1)=z
t =t+1
yes
If j1<
.
no
If i1<
.
yes
no
Y1=1
I1=1
(رقم من مفتاح التشفير بالموقع i1)=k
X1=0
X1=x1+1
D=a(x1,k)
B(x1,y1)=d
10
yes
Ifx1<
.
no

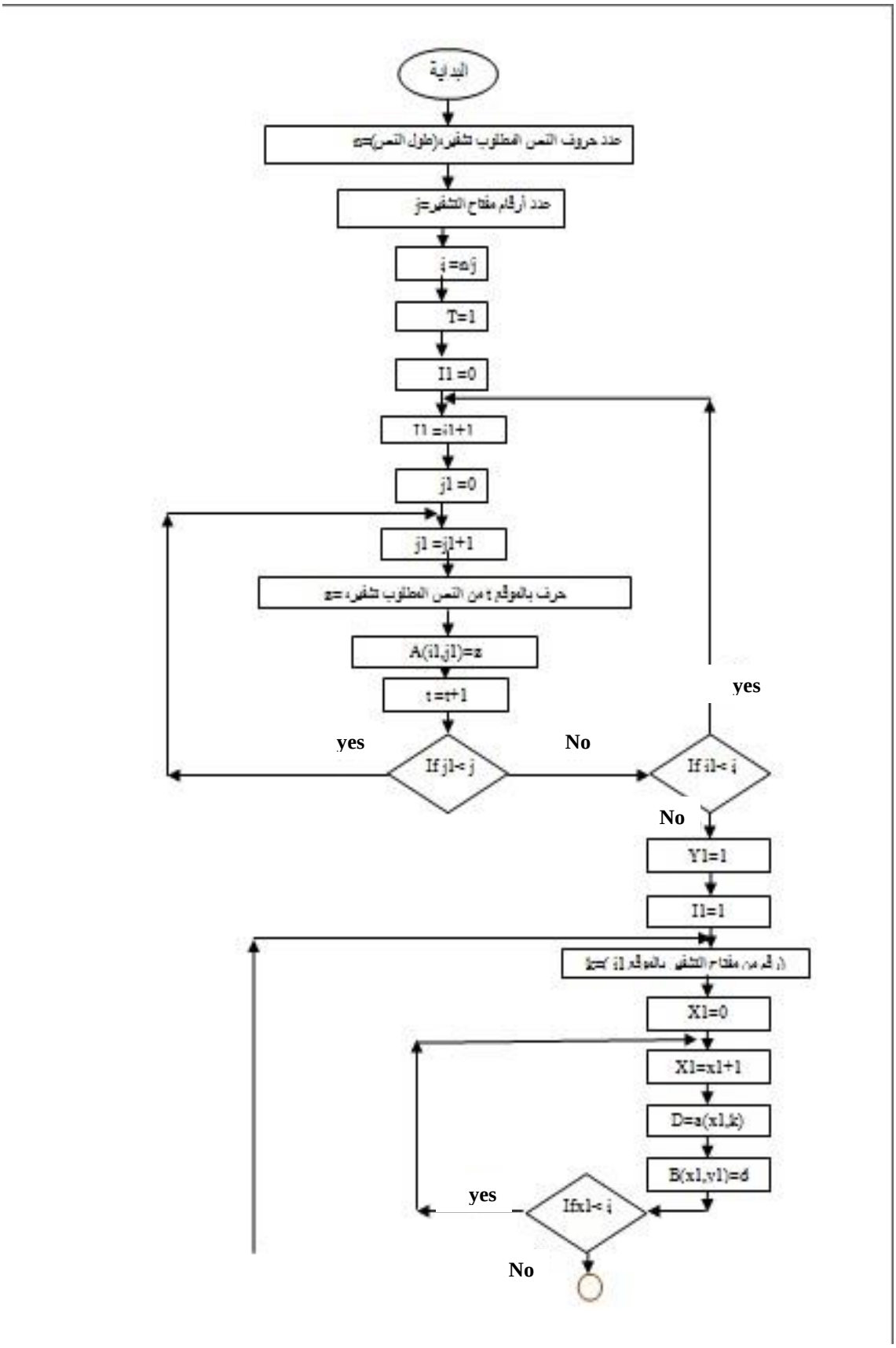


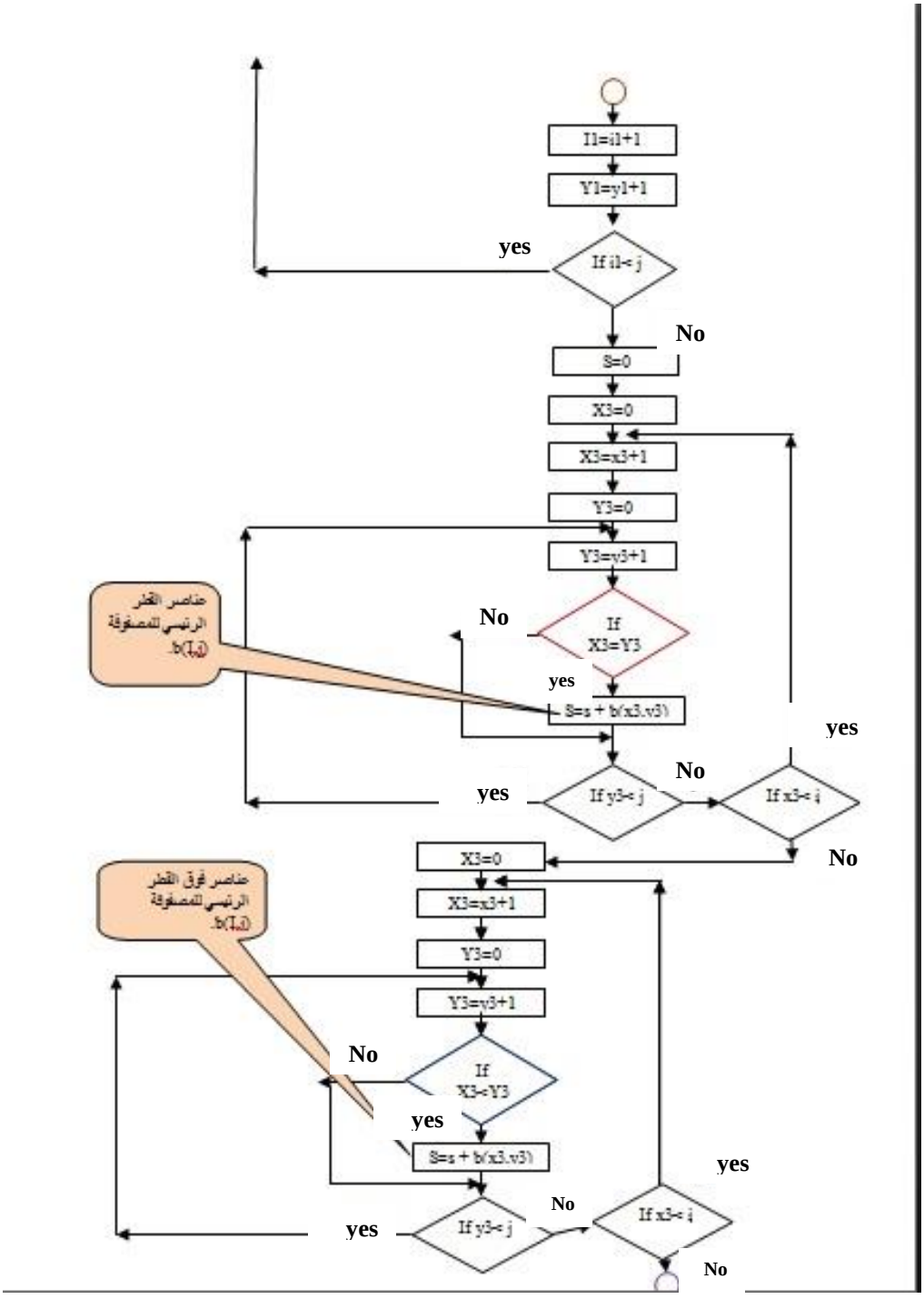
شكل(2) يوضح المخطط الانسيابي لخوارزمية نكلست للتشفير

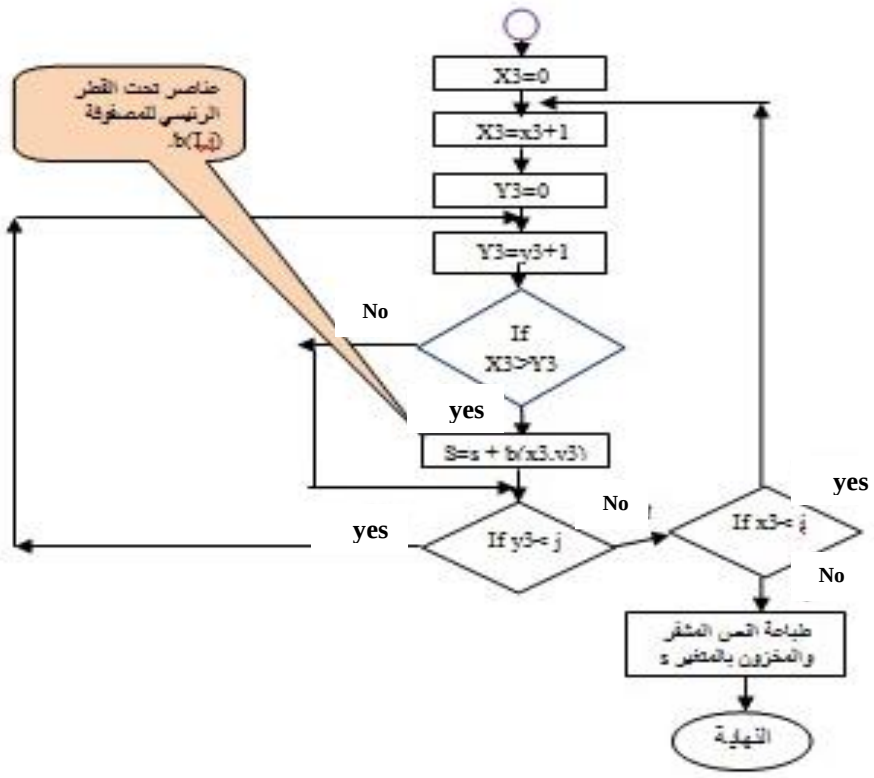

البداية
عدد حروف النص المشفر(طول النص)=n
عدد أرقام مفتاح التشفير=j
Y1=1
(رقم من مفتاح التشفير بالموقع i1)=k
I1 =1
X1=0
X1=x1+1
D=b(x1,v1)
C(x1,K)=d
yes
Ifx1<
no
I1=i1+1
yes
Y1=v1+1
If i1<
N0
S1=0
X3=0
X3=x3+1
Y3=0
Y3=y3+1
yes



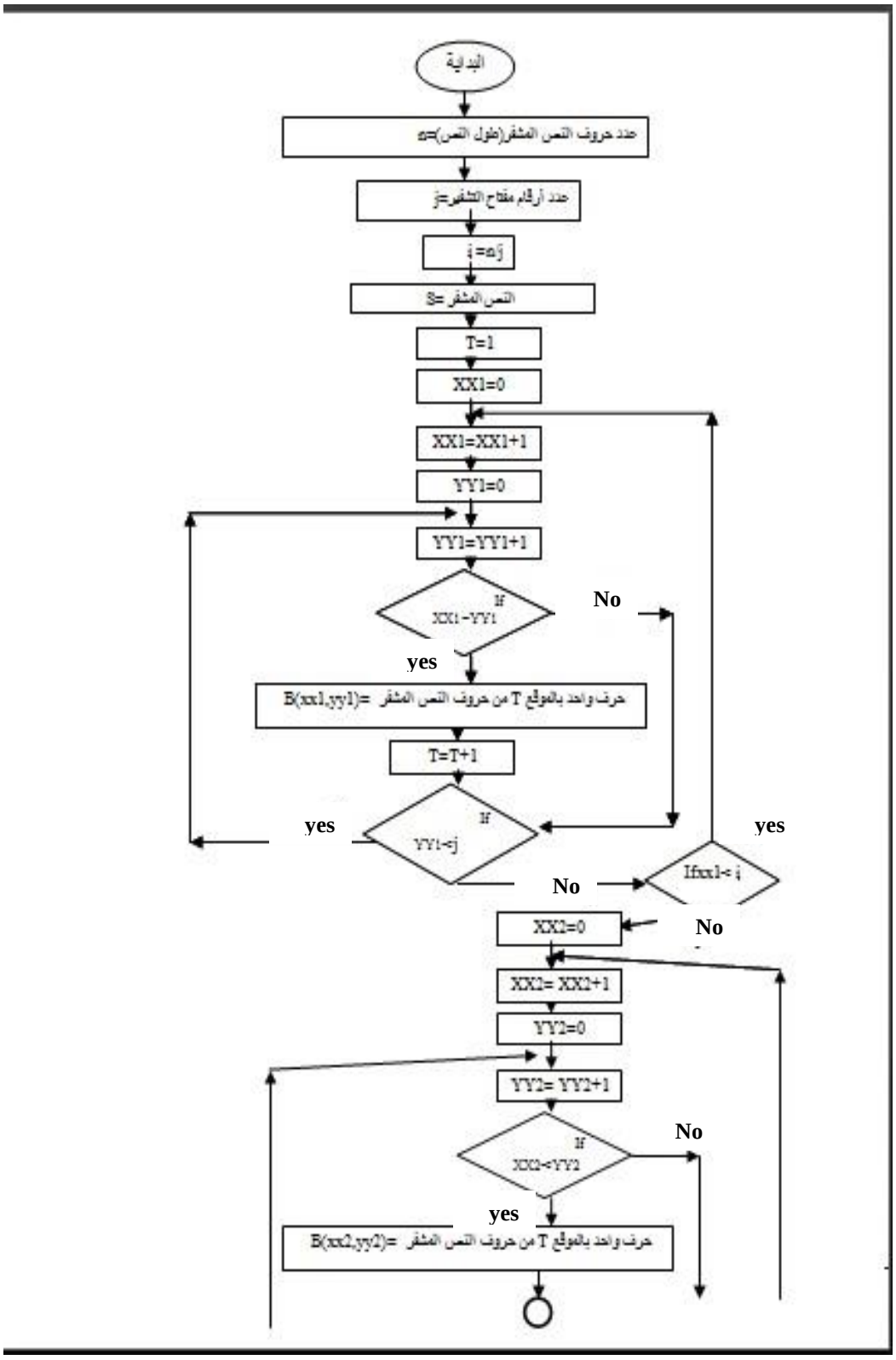
شكل(3) يبن عملية فك الشفرة

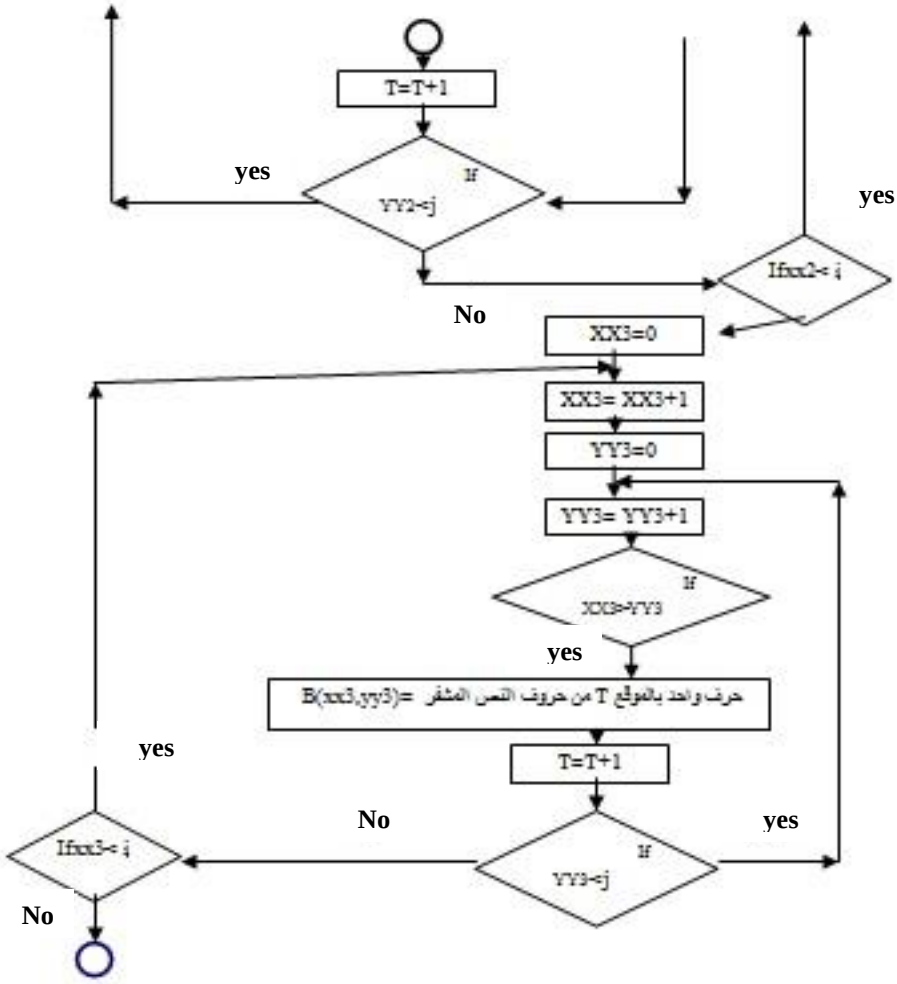

البداية
حدد حروف النص المطلوب تشفيره(طول النص)=n
حدد أرقام مفتاح التشفير=j
i =nj
T=1
I1 =0
I1 =i1+1
j1 =0
j1 =j1+1
حرف بالموقع t من النص المطلوب تشفيره=z
A(i1,j1)=z
t=t+1
yes
If j1< j
No
If i1< i
yes
No
Y1=1
I1=1
X1=0
X1=x1+1
D=a(x1,k)
B(x1,y1)=d
yes
Ifx1< i
No

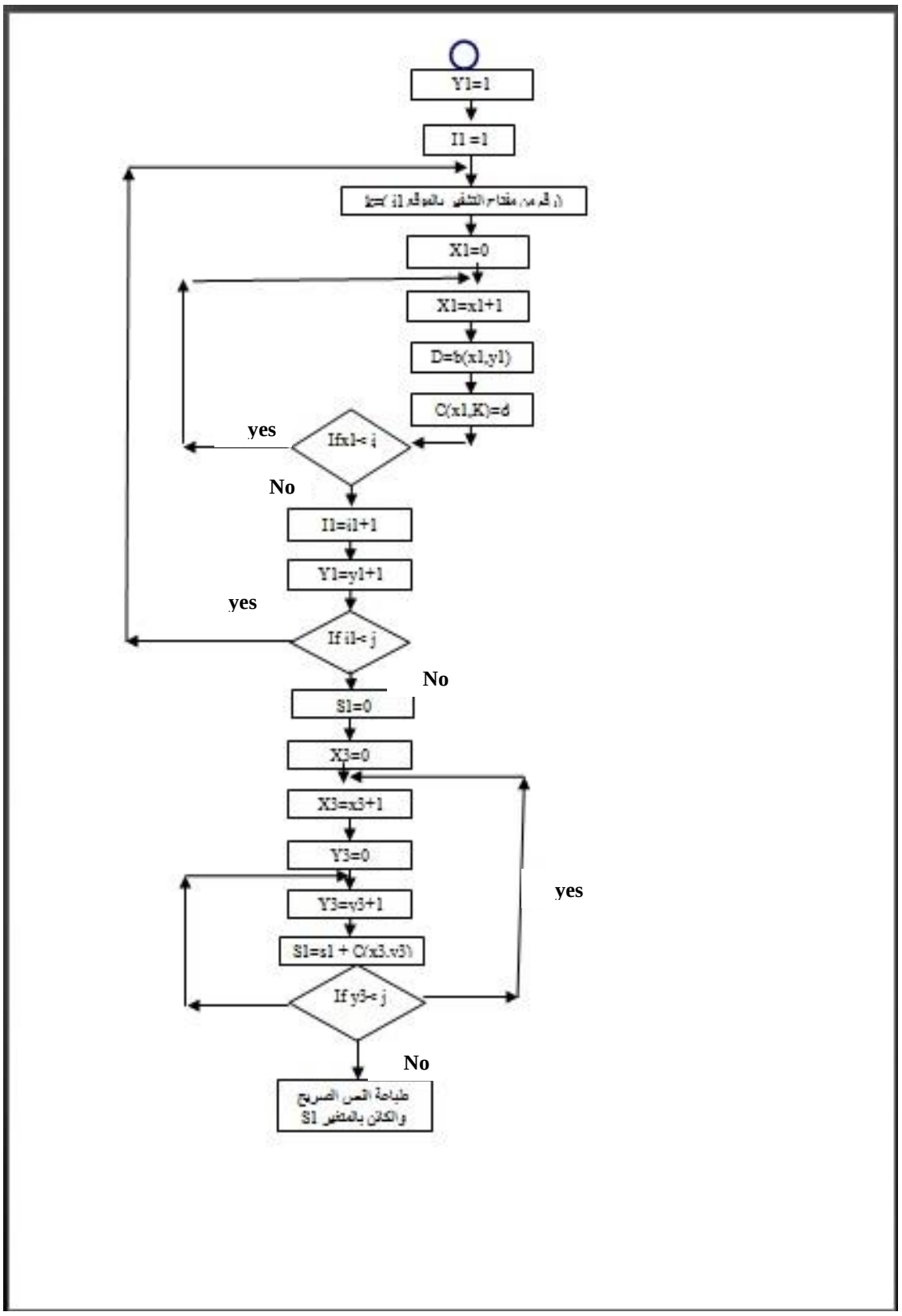

I1=i1+1
Y1=y1+1
yes
If i1< j
No
S=0
X3=0
X3=x3+1
Y3=0
Y3=y3+1
عناصر القطر الرئيسي للمصفوفة b(I,J).
No
If X3=Y3
yes
S=s + b(x3,y3)
yes
No
yes
If y3< j
No
If x3< i
X3=0
عناصر فوق القطر الرئيسي للمصفوفة b(I,J).
X3=x3+1
Y3=0
Y3=y3+1
No
If X3<Y3
yes
S=s + b(x3,y3)
yes
No
yes
If y3< j
No
If x3< i
No



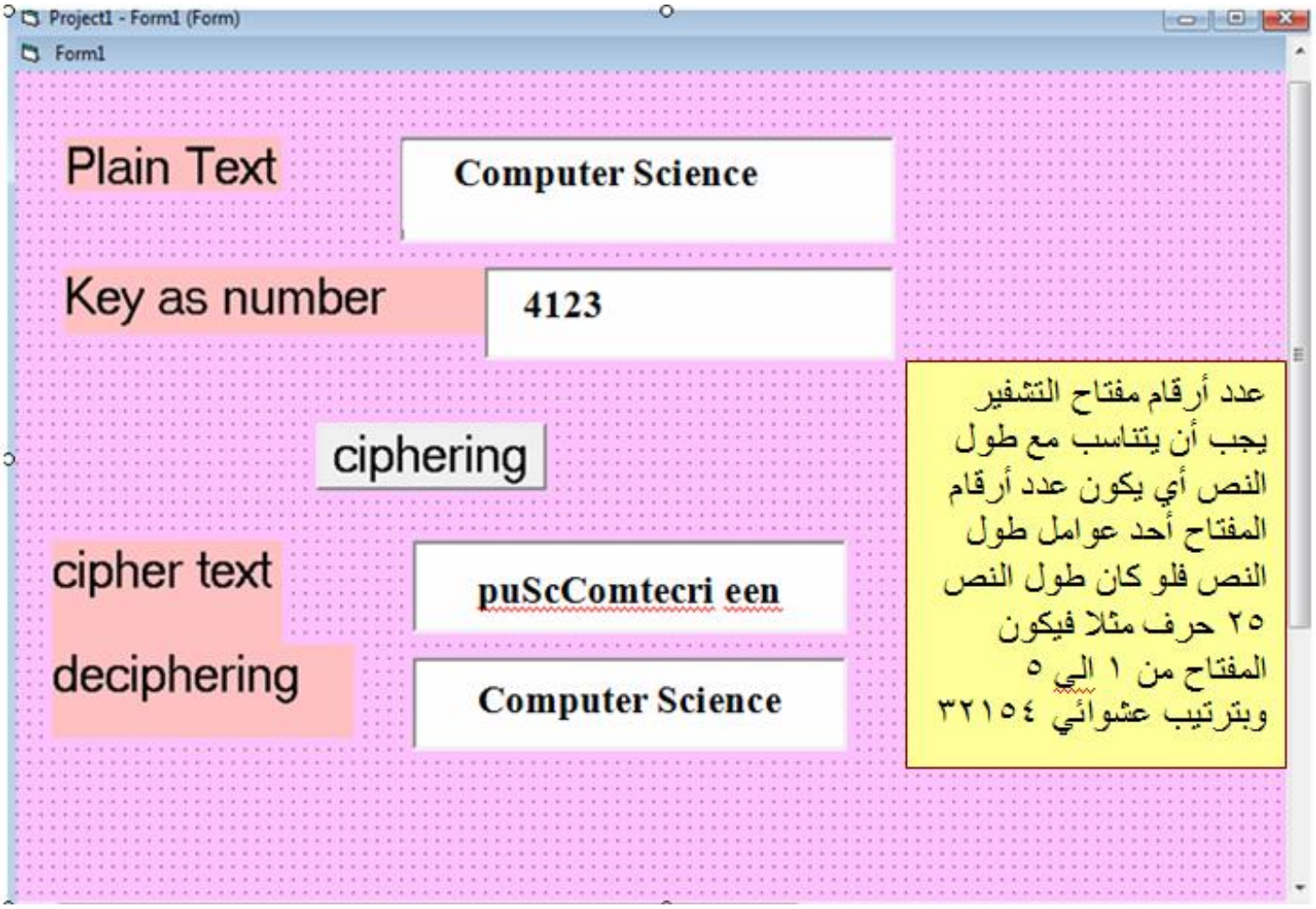
شكل(4): يبين الخوارزمية الجديدة


البداية
عدد حروف النص المشفر(طول النص)=n
عدد أرقام مفتاح التشفير=j
i =n\j
النص المشفر =S
T=1
XX1=0
XX1=XX1+1
YY1=0
YY1=YY1+1
If
XX1 -YY1
No
yes
حرف واحد بالموقع T من حروف النص المشفر =B(xx1,yy1)
T=T+1
If
YY1-<j
yes
No
Ifxx1-< i
yes
No
XX2=0
XX2= XX2+1
YY2=0
YY2= YY2+1
If
XX2-<YY2
No
yes
حرف واحد بالموقع T من حروف النص المشفر =B(xx2,yy2)


T=T+1
If
YY2<j
yes
yes
Ifxx2< j
No
XX3=0
XX3= XX3+1
YY3=0
YY3= YY3+1
If
XX3>YY3
yes
B(xx3,yy3)= حرف واحد بالموقع T من حروف النص المشفر
T=T+1
yes
No
yes
Ifxx3< j
If
YY3<j
No



شكل(5): عملية فك الشفرة



شكل(6): يبين واجهة البرنامج