------ مجلة علوم الرافدين، المجلد 17، العدد 2، ص105-123، 2006 ------

تطبيق اسلوب التشفير الانسيابي المبني على الشبكة العصبية الاصطناعية

لهيب محمد الزبيدي
قسم علوم الحاسبات
كلية علوم الحاسبات والرياضيات
جامعة الموصل

ريا جاسم العطيوي
قسم العلوم المالية والمصرفية
كلية الادارة والاقتصاد
جامعة الموصل

(تاريخ الاستلام 2002/4/29 ، تاريخ القبول 2003/7/27)

الملخص

يهدف البحث الى ايجاد السبل الكفيلة لمساعدة محلل الشفرة لكسر احد انظمة التشفير ذات المفتـاح السري وهو نظام التشفير الانسيابي، اذ يتم استخدام الشبكات العصبية كمهاجم مـن نـوع (Plain Text Attack) بدلاً من استخدام الطرق المعروفة سابقاً وهي طريقة المصفوفات وخوارزميـة ماسـي لكـسر التشفير الانسيابي .

وضع هذا العمل قيد التطبيق باستخدام لغة C++ باصداره (3.0) ونفذ على حاسبة شخصية من نوع (Pintume, 300 MHZ).

Application Stream Cipher on Artificial Neural Network

Laheeb M. Al zaubaidy
Department of Computer Science
College of Computers & Math.Science
Mosul University

Raya J. Al Etew
Department of Finance& Banking Science
College of Administration & Economics
Mosul University

ABSTRACT

This work aims to find the methods that help Cryptanalysis to break one of secret key system, that is stream cipher by used artificial neural network as plain text attack instead of using the old known methods, such as matrix and massy algorithm to break stream cipher.

C++ Language Version (3.0) was used in this study on computer type (Pentium 300 MHZ)

المقدمة

لقد تطورت تقنيات التشفير كي تستخدم للاغراض العسكرية والمدنية ولكن بقيت التقنيات المتقدمة في التشفير حكرا على الحكومات والمؤسسات الكبيرة فقد كانت تنفذ على الحاسبات الكبيرة في مراكز معالجة المعلومات التابعة لها. وفي نهاية القرن الماضي شهدت التعاملات المالية نقلة كبيرة فلم تعد هذه التعاملات تقتصر على اجهزة خاصة مرتبطة عبر شبكات الانترنيت من خلال التجارة الالكترونية والتي تتطلب في كثير من الاحيان تبادل معلومات شخصية مهمة مثل بطاقة الائتمان او الحساب الجاري المصرفي لاحظ الشكل (1)، وغير ذلك الامر الذي ادى الى زيادة الحاجة الى تشفير الملفات المختلفة على الحاسبات الشخصية، ولكن في بعض الاحيان وخصوصاً في المؤسسات الحكومية و العسكرية يتم الاحتياج الى فك شفرة الملفات لاغراض امنية أو عسكرية مهمة (Daniel, 2000 ; Charles, 1989).

ان قدرة الشبكات العصبية الاصطناعية على تنفيذ العمليات بالتوازي وقدرتها على تنفيذ العمليات الحسابية بقدرة عالية والتوصل الى الحل الصحيح بكفاءة عالية، وللاسباب اعلاه تم في هذا البحث بناء نظام يستخدم امكانيات الشبكات العصبية الاصطناعية (شبكة الانتشار الخلفي) في فك تشفير الملف المشفر بطريقة التشفير الانسيابي. ان الملف الناتج من تشفير رسالة بطريقة التشفير الانسيابي عبارة عن ملف مؤلف من (0 ، 1) أي ملف ثنائي، وان هذا النوع من الملفات يكون عرضة للضياع والتشويش اكثر من غيره، وذلك عند الارسال والاستلام، وان فقدان بعض النباتات من الملف سوف تؤثر على معنى الرسالة بشكل كبير، وسيكون من الصعب فك الرسالة المشفرة وارجاعها الى الرسالة الاصلية، لذا يتم استخدام الشبكات العصبية الاصطناعية في هذا النوع من الحالات لقدرتها على التمييز، وبشكل كفوء على الرغم من وجود نقص او تشويش في البيانات.(Chung, 1993; Ruppel, 1986).

1- علم التشفير

العلم الذي يبقي الرسالة في سرية تامة إلى حين فقدان أهميتها يسمى علم الكتابة المخفية (Cryptography)، وهذا ينجز من قبل الأخصائيين في علم التشفير (Encryption) والذي يتم عن طريق خوارزمية التشفير والمفتاح ، النص الناتج من عملية التشفير يسمى النص المشفر (Cipher text)، وعملية إرجاع النص المشفر إلى النص الأصلي (Plain text) هي عملية فك الشفرة (Decryption) .

أما عملية كسر أو حل الشفرات دون معرفة المفتاح هو ما يعرف بـ (Cryptanalysis) وهذا ينجز من قبل محللي الشفرات (Cryptoanalysers) (وزورت بروست، 1989 ; Charles , 1989).

2-تحليل الشفرات (Talie, 1998; Charles, 1989).

إن خوارزميات التشفير ممكن أن تكسر قبل وصول الرسالة إلى الطرف المعني، هذا يعني عند توفر الوقت والمعلومات الكافية يستطيع محلل الشفرة أن يحدد الخوارزمية المستخدمة، كذلك فإن محلل الشفرة سيحاول استخراج معنى الرسالة المشفرة عن طريق قيامه بكل أو بأحد النقاط التالية:

- محاولة كسر رسالة واحدة، وهذا ما يقوم به المهاجم عادة وهو ما يهمنا في هذا البحث.
- محاولة تمييز نماذج (Patterns) في الرسالة المشفرة لكي يكون قادر على كسر جزء من الرسالة بواسطة تطبيق خوارزمية فك الشفرة وعادة يقوم بها المصمم لمعرفة مدى قوة التشفير للنظام.
- محاولة إيجاد الضعف العام في خوارزمية التشفير دون الحاجة إلى التعرض لأي رسالة لغرض تحسين خوارزميات التشفير وهذا ما يقوم به المصمم.

يقسم مهاجمي الشفرات إلى مجاميع نذكر منها :

- إذا كان محلل الشفرة يمتلك النص المشفر فقط يسمى مهاجم النص المشفر (Cipher text attack). (Shneier, 1996).
- إذا كان محلل الشفرة يمتلك ما يقابل جزء من النص المشفر بالنص الصريح يسمى حينها بمهاجم النص الصريح (Known-Plaintext attack) (Shneier , 1996).

3-استخدام الشبكات العصبية في تحليل الشفرة

يتميز الإنسان بكفاءته العالية جدا في تنفيذ العديد من المهمات مثل اتخاذ القرارات وفهم اللغة إضافة إلى قابليته على التفكير، التخطيط، التمييز وحل المشاكل في الوقت الذي لا يستطيع الحاسب الرقمي حل العديد من المشاكل بنفس الكفاءة التي يتميز بها الإنسان.

هذا يعود إما لعدم وجود خوارزمية حل وحتى وإن وجدت تكون معقدة بحيث لا يمكن تنفيذها باستخدام الحاسب الرقمي، أو أن الوقت الذي يتطلبه حل المشكلة كبير جدا.

إن قابلية الإنسان وكفاءته ترجع إلى هيكل دماغه المتكون من عدد هائل من الخلايا العصبية المرتبطة مع بعضها البعض مكونة شبكة عصبية معقدة . لذلك كانت المحاولة في الوصول إلى كفاءة الإنسان في حل المشاكل من خلال تقليد ولو بشكل بسيط هيكل دماغ الإنسان، ولهذا كانت الشبكات العصبية الاصطناعية (Artificial Neural network [ANN]) التي تقوم بحل المشاكل دون الحاجة إلى وجود خوارزمية حل مما أدى إلى تقليل كمية البرامجيات الضرورية والتي يجب تصميمها من أجل تنفيذ العمليات باستخدام الحاسب الآلي (الحمداني، 1996).

إن المشكلة المناسب حلها باستخدام الشبكات العصبية يجب أن تتميز بما يلي :

- القواعد التي تستخدم لحل المشكلة ربما تكون غير معروفة، أو من الصعب توضيحها وصياغتها نظاميا.

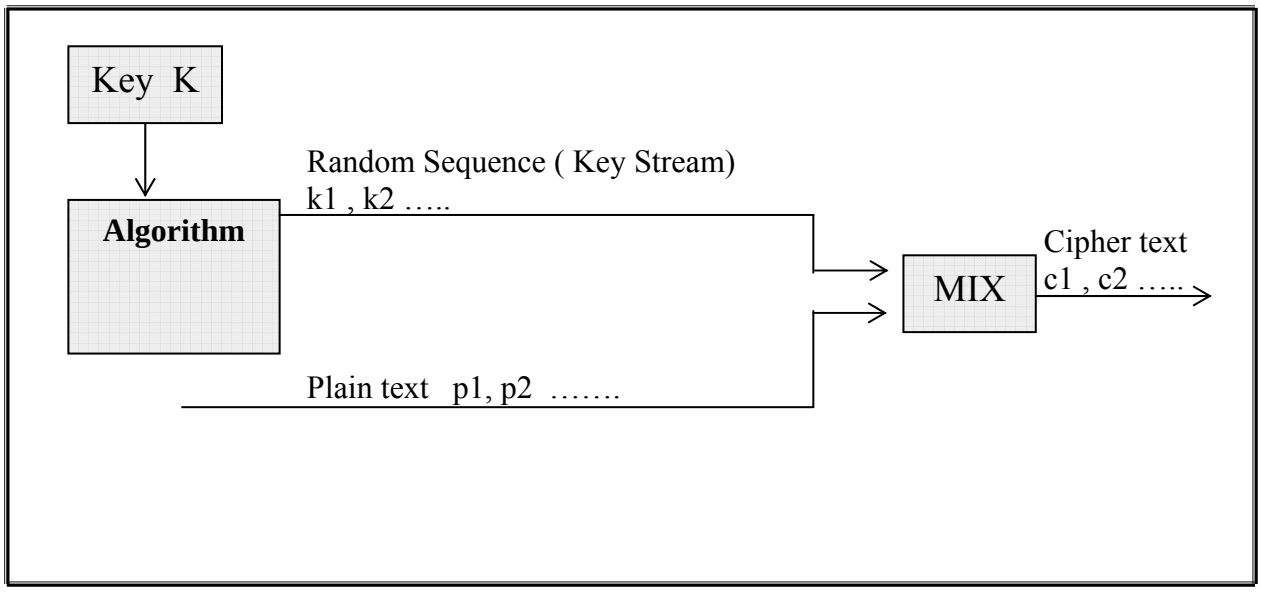
- تستخدم المشكلة بيانات مشوشة أو ناقصة.
- قد لا تتوفر حلول نقية للمشكلة.
- يحتاج حل المشكلة إلى سرعة معالجة عالية جدا.

من خلال الصفات التي تتميز بها الشبكات العصبية الاصطناعية وجد ان مشكلة تحليل الشفرة لانظمة التشفير الانسيابي مناسبة جدا لحلها باستخدام الشبكات العصبية حيث أنه تم استخدامها كمهاجم من نوع مهاجم النص الصريح (Known - Plaintext attack) ضد مسجلات الإزاحة ذات التغذية المرتدة الخطية (Linear Feedback Shift Registers LFSR) للحصول على المكافيء الخطي ومواصفات الحد المميز (الحمداني، 1996 ; ياسين، 2000).

4- التشفير الانسيابي

يتكون نظام التشفير الانسيابي من جزأين أساسيين هما :

- خوارزمية توليد المتتابعة شبه العشوائية (Pseudo Random Sequence Algorithm)
- المازج (Mixer) : تقوم خوارزمية هذا النظام بتوليد متتابعة شبه عشوائية اعتمادا على مفتاح يغذيها ثم تدمج هذه المتتابعة المتولدة مع متتابعة النص الصريح بوساطة المازج لتوليد متتابعة النص المشفر. وفي حالة النظام الثاني يكون المازج هو عملية الـ (XOR) إذ يستخدم في التشفير وفي فك الشفرة (الحمداني، 1996) ، وكما موضح بالشكل (1) :



الشكل 1: مخطط التشفير الانسيابي

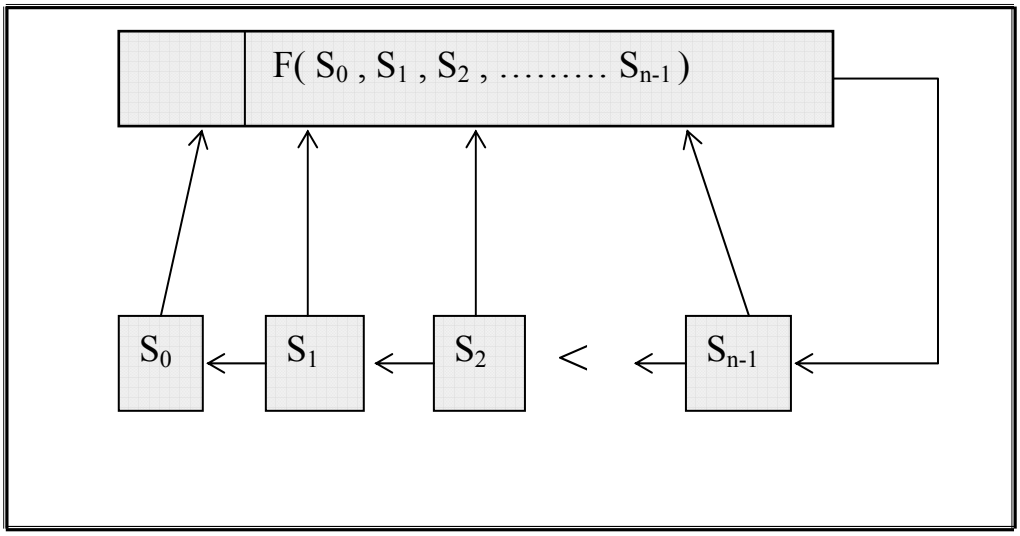
- **خواص إحصائية جيدة (Good Statistical Properties) :** إن سرية النظام تعتمد على متتابعة المفتاح الانسيابي، بصورة عامة وهنالك متطلبات ضرورية يجب توفرها في متتابعة المفتاح وهي :-
- **طول الفترة (Long Period) :** وهي عدد البتات الموجودة في المتتابعة غير المتكررة إذ أن الفترة الطويلة أفضل من الفترة القصيرة ، خصوصا عند عدم استخدام أي جزء من السلسلة مرة أخرى في عملية تشفير النص ، فإذا كانت الفترة طويلة جدا سوف نستطيع الحصول على سلسلة عشوائية كفوءة، إذ أنه أي معلومات عن عدد (جزء) من عناصر المتتابعة سوف لن يساعد على اكتشاف بقية عناصر سلسلة المفتاح(الحمداني، 1996 ؛ Charles, 1989) احتياج متتابعة المفتاح الانسيابي إلى الخواص الإحصائية الجيدة هو لغرض تحطيم المعلومات الإحصائية التي تحويها الرسالة (النص الصريح)(أي لكي يصعب على الإحصائيين الاستفادة من هذه المعلومات) وبالتالي يصعب كسر الرسالة المشفرة ، وسيبدو النص المشفر وكأنه عشوائيا (الحمداني، 1992; Charles, 1989; Ronald, 1997).
- **تعقيد خطي كبير (Long Linear Complexity) :** يجب أن يكون لمتتابعة المفتاح الانسيابي تعقيد خطي كبير (وهو طول أقصر مسجل إزاحة ذو مرتدة خطية يقوم بتوليد المتتابعة) مما يجعل عدد اختيارات المفاتيح كبيرة ولا يستطيع محال الشفرة تجريبها جميعا (الحمداني، 1992; Charle,1989; Ronald, 1997).

1-الهيكل المستخدم للتوليد العشوائي

هنالك عدة طرق لتوليد الارقام العشوائية:

1-مسجلات الإزاحة ذات التغذية المرتدة

ان أغلب مولدات المفتاح الانسيابي (Key stream) تستخدم مسجلات الإزاحة (Shift Register) ولذلك لتوفرها ورخص أسعارها (Beker, 1998). يتكون كل مسجل إزاحة من النطاطات – (Flip Flops) وهي عبارة عن ذاكرة ذات عناصر ثنائية كل منها تسمى مرحلة (Stage) وبعدد هذه المراحل يتحدد طول مسجل الإزاحة ودرجة التعقيد، ويمكن إشراك معظم هذه المراحل بواسطة دالة تدعى دالة التغذية المرتدة (Feedback Function) (الحمداني، 1992; Charles, 1989; Ruppel, 1986). في كل نبضة (Pulse) تزحف محتويات أي مرحلة إلى المرحلة التي تسبقها . المرحلة الأخيرة يظهر فيها ناتج دالة التغذية المرتدة . أما المتتابعة الناتجة (مخرجات مسجل الإزاحة) فهي محتوى المرحلة الأولى ، وكما موضح في الشكل (2) :



الشكل 2 : مسجل الإزاحة

وهنالك نوعين من هذه المولدات :

أ ـ مولدات تحقق الصفة الخطية

مسجلات الإزاحة ذات دالة التغذية المرتدة الخطية

في عام (1970) ظهرت أول صناعة لمسجلات الإزاحة ذات دالة التغذية المرتدة الخطية ، ففي هذه المسجلات تكون الدالة الخلفية (F) دالة خطية، فلو عرفنا طور مسجل الإزاحة بـ $(S_0 , S_1 ....., S_{n-1})$ ، عليه يمكن كتابة الدالة كما يلي :-

$$F(S_0 , S_1 ..... , S_{n-1}) = C_0S_0 + C_1S_1 + ... + C_{n-1}S_{n-1} \quad ... (1)$$

إذ أن كل C_i هي إما (0 أو 1) وأن الثوابت $C_0C_1 .....C_{n-1}$ تسمى معاملات التغذية الخلفية الخطية (Coefficint Feedback) وأن$(i = 0 , 1 , ... n-1)$، وان الجمع المستخدم هو (XOR) (الحمداني، 1996; Ronald A, 1997) . والشكل (3) يوضح n من الـ Stage للـ LFSR . كل مسجل إزاحة ذو تغذية خلفية خطية يمكن وصفه بصورة وحيدة بما يسمى متعددة الحدود المميزة له (Characteristic Polynomial) ويمكن تعريف متعدد الحدود بما يلي :-

$$F(x) = C_0 + C_1x + C_2 x_2 ..... C_{n-1} X_n + X_n . \quad ...(2)$$

لأي متعدد حدود هنالك 2^n من القيم الابتدائية المختلفة الممكنة ، وعليه يمكن استخدام متعدد حدود لتوليد 2^n متتابعة مختلفة . المتتابعة الناتجة من مسجل الإزاحة ذو دالة تغذية مرتدة $C_0 =1$ تكون دورية فإذا كانت f(x) أولية فان المتتالية الناتجة m-sequence لها دورة طولها $(2^n -1)$ وهي الحد الأعلى لطول السلسلة الممكن توليدها بواسطة LFSR بـ (n) من المراحل (الحمداني، 1992; Talie, 1998).

ب ـ مولدات تحقق الصفة اللاخطية

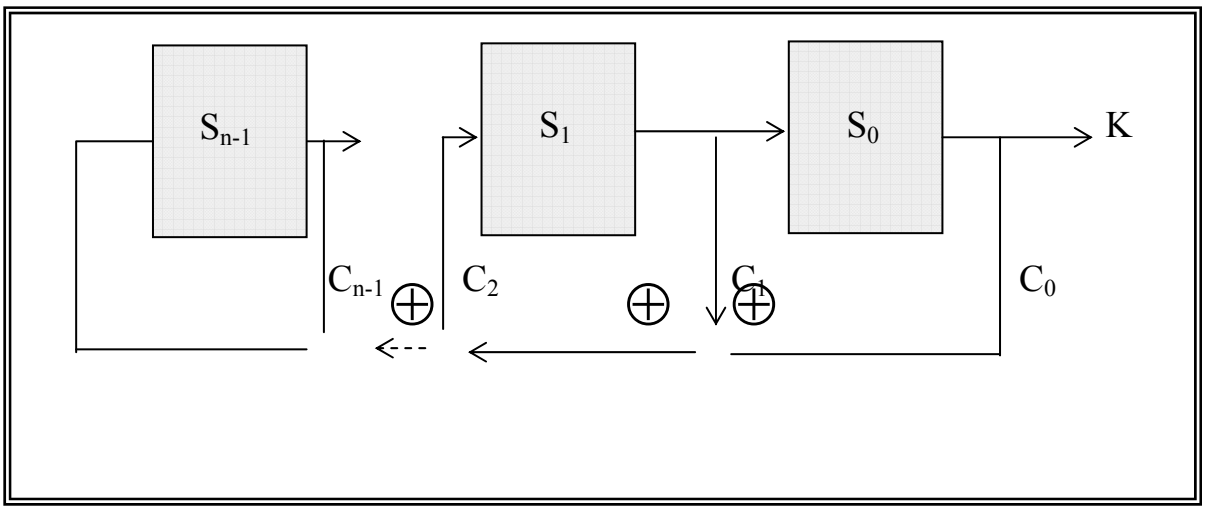
من الممكن تحقيق الصفة اللاخطية بطريقتين :

- **استخدام مسجلات الإزاحة ذات دالة التغذية المرتدة اللاخطية**(Zeng, 1991)

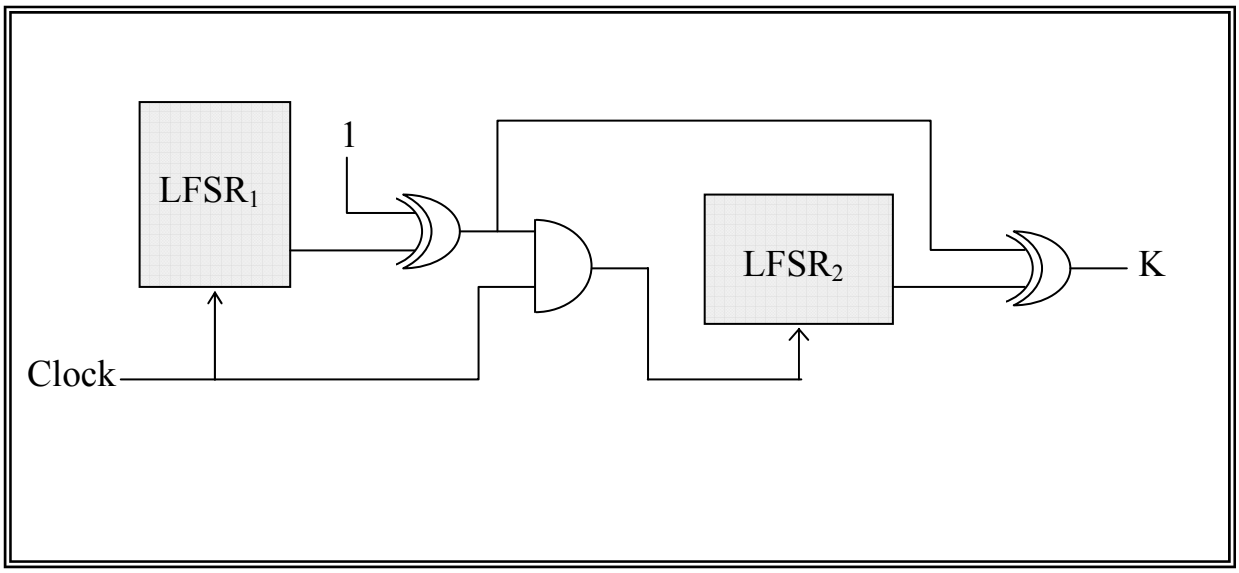
وهو نوع خاص من المسجلات في هذا النوع يكون عـدد السلاسـل التي من المحتـمل توليـدها هو $(2^{2(n-1)} - n)$، إذ أن n تمثل عدد المراحل (Stage) .

- **استخدام أكثر من LFSR .**

العديد من المولدات للأرقام العشوائية تعتمد على ربط اثنين أو أكثر من LFSR للحـصول علـى سلسلة بأطول فترة ممكنة، الشكل (4) يوضح أحد هذه الأنواع ويطلـق عليـه (Gollman Generator) (الحمداني، 1992 ; John, 1996 ; Talie,1998).



الشكل 3 :مولد ازاحة من نوع (LFSR) بـ(n) من المراحل



الشكل 4 :مولد قف وتحرك من نوع (NLFSR)

2- متعدد الحدود المميز الابتدائي

أن الطول الأعظم لدورة متتابعة المفتاح المتولدة من مسجل الإزاحة الخطي بطول n هو 2^n-1 والذي يتحدد بمتعدد الحدود المميز لمسجل الإزاحة . إن متعدد الحدود المميز الذي يعطي أكبر دورة ممكنة له مواصفات خاصة ، وفي ما يلي توضيح لذلك :

لأي متعدد حدود g(x) بدرجة n يوجد عدد صحيح e يسمى الأس (Exponent) حيث $g(x) \mid x^e+1$ ، $g(x) \mid x^r+1$ لكل $r < e$. إن الخصائص المهمة التي يتميز بها العدد e هي :

- $e \le 2^n - 1$.
- طول الدورة p للسلسلة الخارجة من مسجل الإزاحة ذو دالة التغذية المرتدة g(x) بأس e يجب أن يقسم العدد e، أي $p \mid e$. فإذا كانت g(x) غير قابلة للاختزال (Irreducible) وبأس e، سيكون طول الدورة مساوي الى e . إن أكبر قيمة للعدد e لمتعدد حدود بدرجة n هي 2^n -1 فإذا كانت g(x) بدرجة n و $e = 2^n - 1$ يسمى g(x) متعدد حدود ابتدائي (Primitive Polynomial) والسلسلة المتولدة من مسجل الازاحة ذو متعدد حدود مميز ابتدائي تكون سلسلة شبه عشوائية لذلك عندما يكون المطلوب توليد سلسلة بطول دورة $p = 2^n - 1$ من مسجل إزاحة بطول n ، يجب أن يكون متعدد الحدود المميز ابتدائيا بدرجة n ، حيث أنه لكل n هناك

$$\lambda(n) = \frac{\theta(2^n - 1)}{n} \qquad \dots (3)$$

متعدد حدود ابتدائي بدرجة n (الحمداني، 1992)، $\theta(m)$ تمثل دالة أويلر. بصورة عامة لا توجد طريقة سهلة للحصول على متعدد الحدود الابتدائي لدرجة معينة، ولكن يمكن القول أن أسهل طريقة هي اختبار متعددات حدود عشوائية شرط أن تكون غير قابلة للاختزال ومن الدرجة (n) واختبارها فيما إذا كانت أولية أم لا . بالرغم من أن هذه الطريقة معقدة بعض الشيء ولكن هنالك العديد من البرامجيات الرياضية الجاهزة التي تؤديها، الجدول (1) يوضح بعض متعددات الحدود الابتدائية بدرجات مختلفة ، ونلاحظ من خلاله أن جميع متعددات الحدود الابتدائية تمتلك عدد فردي من المعاملات (Odd Number of Coefficients) كما نلاحظ بان كل متعدد حدود في الجدول ممكن أن يعطي متعدد حدود ابتدائي آخر ، (John,1996) وحسب القاعدتين التاليتين :

- إذا كان $X^a + X^b + 1$ متعدد حدود ابتدائي فإن $X^a + X^{a-b} + 1$ متعدد حدود ابتدائي أيضا.
- إذا كان $X^a + X^b + X^c + X^d + 1$ متعدد حدود ابتدائي

فإن $X^a + X^{a-d} + X^{a-c} + X^{a-b} + 1$ متعدد حدود ابتدائي أيضا.

وفي ما يلي توضيح لذلك:

مثال 1 : إذا كان لدينا متعدد الحدود الابتدائي التالي :

$$X^3 + X^1 + 1$$

فإن $X^3 + X^2 + 1$ هو متعدد حدود ابتدائي ايضا.

مثال 2 : إذا كان لدينا متعدد الحدود الابتدائي التالي :

$$X^8 + X^4 + X^3 + X^2 + 1$$

فإن $X^8 + X^6 + X^5 + X^4 + 1$ هو متعدد حدود ابتدائي ايضا.

وسنعطي في الجدول ادناه بعض متعددات الحدود لدرجات مختلفة

الجدول1 :بعض متعددات الحدود لدرجات مختلفة

الدرجة	متعدد الحدود	الدرجة	متعدد الحدود
17	$X^{17} + X^3 + 1$	1	$X^1 + 1$
17	$X^{17} + X^5 + 1$	2	$X^2 + X^1 + 1$
17	$X^{17} + X^6 + 1$	3	$X^3 + X^1 + 1$
18	$X^{18} + X^7 + 1$	4	$X^4 + X^1 + 1$
18	$X^{18} + X^5 + X^2 + X^1 + 1$	5	$X^5 + X^2 + 1$
19	$X^{19} + X^5 + X^2 + X^1 + 1$	6	$X^6 + X^1 + 1$
20	$X^{20} + X^3 + 1$	7	$X^7 + X^1 + 1$
21	$X^{21} + X^2 + 1$	7	$X^7 + X^3 + 1$
22	$X^{22} + X^1 + 1$	8	$X^8 + X^4 + X^3 + X^2 + 1$
23	$X^{23} + X^5 + 1$	9	$X^9 + X^4 + 1$
24	$X^{24} + X^4 + X^3 + X^1 + 1$	10	$X^{10} + X^3 + 1$
25	$X^{25} + X^3 + 1$	11	$X^{11} + X^2 + 1$
26	$X^{26} + X^6 + X^2 + X^1 + 1$	12	$X^{12} + X^6 + X^4 + X^1 + 1$
27	$X^{27} + X^5 + X^2 + X^1 + 1$	13	$X^{13} + X^4 + X^3 + X^1 + 1$
28	$X^{28} + X^3 + 1$	14	$X^{14} + X^5 + X^3 + X^1 + 1$
29	$X^{29} + X^2 + 1$	15	$X^{15} + X^1 + 1$
30	$X^{30} + X^6 + X^4 + X^1 + 1$	16	$X^{16} + X^5 + X^3 + X^2 + 1$

3- المكافئ الخطي

إذا استطعنا توليد متتابعة من مسجل إزاحة خطي ذي قياس معين فانه بالإمكان الحصول على نفس المتتابعة من مسجل إزاحة آخر ذي حجم أكبر، لذلك يمكن القول إن المكافئ الخطي هو أقل طول لمسجل الإزاحة المستخدم في توليد المتتابعة ومتعدد الحدود المميز لمسجل الإزاحة الخطي هذا ذو درجة مساوية للمكافيء الخطي، وإن المكافيء الخطي للسلسلة يحدد درجة التعقيد الخطي لتلك السلسلة، فإذا كان المكافيء الخطي لسلسلة ثنائية هو n فإن معرفة $n \times 2$ مرتبة ثنائية متلاحقة من متتابعة المفتاح تكون

كافية لكسر النظام، حيث أنه عن طريقها يمكن استنتاج بقية متتابعة المفتاح، لذلك فإنه كلما كان المكافيء الخطي كبير كلما حصلنا على درجة سرية أكبر وذلك لأنه عندها يجب معرفة جزء كبير مـن متتابعـة المفتاح (الحمداني، 1995).

5-الشبكات العصبية الاصطناعية

تعرف الشبـكة العصبية الاصـطناعية (Artificial Neural Network (ANN))على أنها نظام حسابي مكون من عدد من وحدات المعالجة تسمى خلايا عصبية أو عقد أو وحدات . وهي مرتبطة مـع بعضها وتتصف بطبيعتها الديناميكية وسميت بالشبكات العصبية الاصطناعية لكونها بنيت مـن محاكـاة الشبكة العصبية في الكائنات الحية بقدر المعرفة المتوفرة عنها. تتشابه الشبكة العصبية الاصطناعية مـع الشبكة العصبية الطبيعية في كونها تتألف من عدد كبير من الخلايا، وكل خلية عصبية ترتبط بعـدد مـن الخلايا المجاورة لها، كما أن لها القابلية على التعلم باسلوب التكييف . كل خلية يكون لها عدد مـدخلات، من المحيط الخارجي أو خلايا عصبية أخرى ولها خرج واحد فقط يتوزع إلى خلايا عـصبية أخـرى أو يكون خرج إلى المحيط الخارجي (ابراهيم, 2000; Daniel, 2000 ;Kinnebrock, 1998).

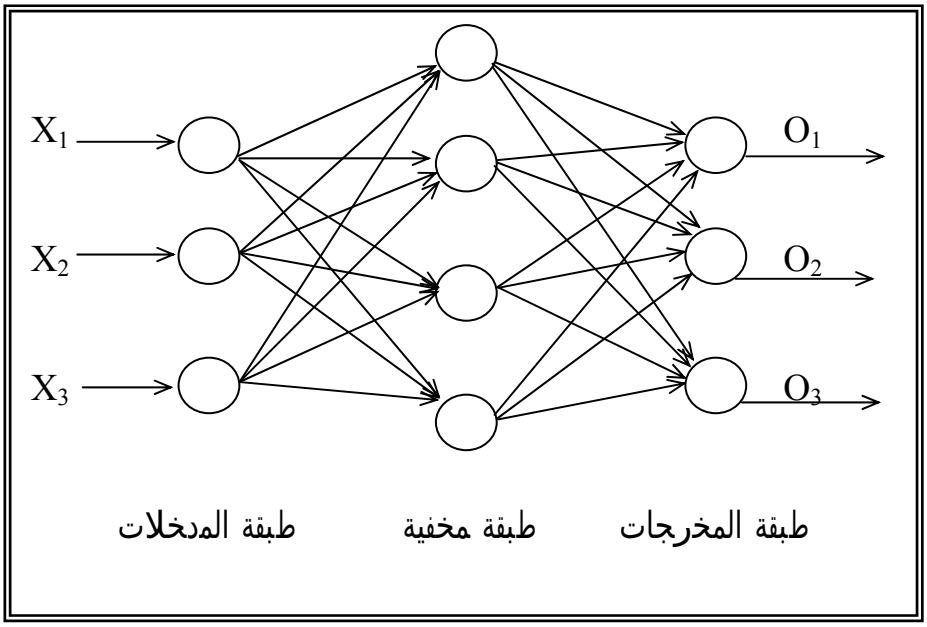
1- هيكل الشبكات العصبية الاصطناعية

تتكون الشبكة العصبية من عدد من الطبقات (أول طبقة تكون طبقة المدخلات وآخر طبقة تكـون طبقة المخرجات والطبقات الوسطى إن وجدت تسمى الطبقات المخفية، الشكل (5) يوضح شبكة عـصبية متعددة الطبقات لكونها محتوية على طبقات مخفية.

2- طريقة التدريب ذي الانتشار العكسي

إن طريقة التدريب ذات الانتشار العكسي يمكن تطبيقها على أية شبكة متعددة الطبقات تستعمل دالة انتقال قابلة للاشتقاق في تمثيل إخراج خلاياها . إن عملية التدريب ذات الانتشار العكسي تُعد مـن أهـم طرائق التدريب بإشراف ، إذ يمكن استخدامها لتدريب الشبكات العصبية بغض النظر عن عدد الطبقـات المكونة لها . إن عمليات التدريب بإشراف ومنها طريقة التدريب ذي الانتشار العكسي تحتاج إلى تطبيق زوج التدريب الذي يضم الإدخال المطبق على الشبكة والهدف أو الإخراج المطلوب إيجـاده مـن قبـل الشبكة في كل عملية تكرار ، إذ أن بتطبيق الإدخال على الطبقة الأولى فإنه ينتشر أماميا عبـر الـشبكة المتعددة الطبقات وصولا إلى طبقة الإخراج، إذ يـتم عنـد ذاك موازنـة الإخـراج (Actual Output) بالإخراج المطلوب إيجاده من قبل الشبكة لحساب الخطأ الذي ينتشر بدروه عكـسيا ابتـداءً مـن طبقـة الإخراج وصولا إلى طبقة الإدخال لتتم عملية تحديث أوزان كل طبقة أثناء عملية الانتشار العكسي تلك . الخلايا العصبية في شبكة الانتشار العكسي لا ترتبط مع خلايا عصبية أخرى في نفس الطبقة ، أي أن كل

خلية عصبية في طبقة الإدخال ترسل إخراجها إلى خلايا الطبقة المخفية ، وكل خلية في الطبقة المخفيـة ترسل إخراجها إلى خلايا طبقة الإخراج (Ignor, 1990) .



الشكل 5 : شبكة عصبية متعددة الخلايا

إن عملية التدريب ذي الانتشار العكسي يمكن اختزالها بتتبع الأسلوب الآتي :

1. ضع قيما ابتدائية صغيرة لأوزان كل الخلايا المكونة للشبكة .
2. اختر زوج التدريب القادم (x^P, t^P) المتكون من الإدخال x^P والهدف t^P واحسب إخراج كـل خليـة (j) في كل طبقة (q) ابتداءً من طبقة الإدخال :

$$O_j^q = f(\sum_i O_i^{q-1} W_{ji}^q) \quad \ldots\ldots (4)$$

إذ أن

O_j^q : إخراج الخلية (j) في الطبقة (q) . لاحظ إن إيجاد اخراجات الطبقة الأولى أن (q=0) أي :

$$O_j^q = O_j^0 = X_j$$

3. احسب الخطأ بين الإخراج الفعلي للشبكة (O) وبين الهدف (t) ثم احسب قيمة (δ) :

$$\delta_j^Q = (O_j^Q - t_j^p) f'(NET_j^Q) \quad \ldots\ldots (5)$$

لكل قيم j عند استعمال زوج التدريب المفهرس بـ p

إذ أن :

O_j : إخراج الخلية (j) .

Q : فهرس الطبقة الأخيرة .

$f'(NET_j)$: مشتقة دالة تمثيل إخراج الخلية (NET_j) f التي يجب أن تكون قابلة للاشتقاق (عـادة تستعمل دالة Sigmoid) .

NET_j : المجموع الوزني للإدخال :

$$NET_j^q = \sum_i O_i^{q-1} W_{ji}^q \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (6)$$

4. احسب قيم (δ) لكل طبقة سابقة باستخدام قيم الخطأ المنتشر عكسيا :

$$\delta_j^{q-1} = f'(NET_j^{q-1}) \left[\sum_{i=1}^{M} \delta_j^q W_{ji}^q \right] \quad \ldots\ldots\ldots\ldots\ldots\ldots (7)$$

إذ أن :

لكل (j) في كل طبقة ستكون :

$$q = Q , Q - 1 , \ldots 2$$

M : عدد الخلايا في الطبقة q

5. جد الوزن الجديد W_{ji} :

$$W_{ji}^{new} = W_{ji}^{old} + \Delta W_{ji}^q \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (8)$$

لكل طبقة q إذ :

$$\Delta W_{ji}^q = \eta \delta_i^q O_j^{q-1}$$

η : معامل نسبة التعليم

6. أعد الخطوات من 2 إلى 5 لكل ادخالات الشبكة إلى أن يصبح الخطأ الكلي أقل ما يمكن .

إذ :

$$E_{total} = \sum_c E_c$$

$$E_c = \frac{1}{2} \sum_j (O_j - t_j^p)^2 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (9)$$

إذ (j) هو فهرس كل خلية ضمن خلايا طبقة الإخراج .

تجنبا للنهاية الصغرى (Local minimum) فإنه عادة ما يتم وضع η ذات قيمة قليلة بالرغم مـن أن ذلك سيكون على حساب زمن التقارب الذي يتناسب عكسـ ـ ـيا مع η (شفاء عبـد الـرحمن ياسـين، 2000; Wasserman, Philip, 1989 ; Valluru, 1993).

6- مهاجمة التشفير الانسيابي

هنالك عدة طرق معروفة لمهاجمة التشفير الانسيابي وهي مهاجمة التـشفير الانـسيابي باسـتخدام المصفوفات، أو باستخدام خوارزمية ماسي. ومن الطرق الحديثة هي مهاجمة التشفير الانسيابي باسـتخدام الشبكات العصبية الاصطناعية (الحمداني، 1996) (والذي يهمنا في هذا البحث).

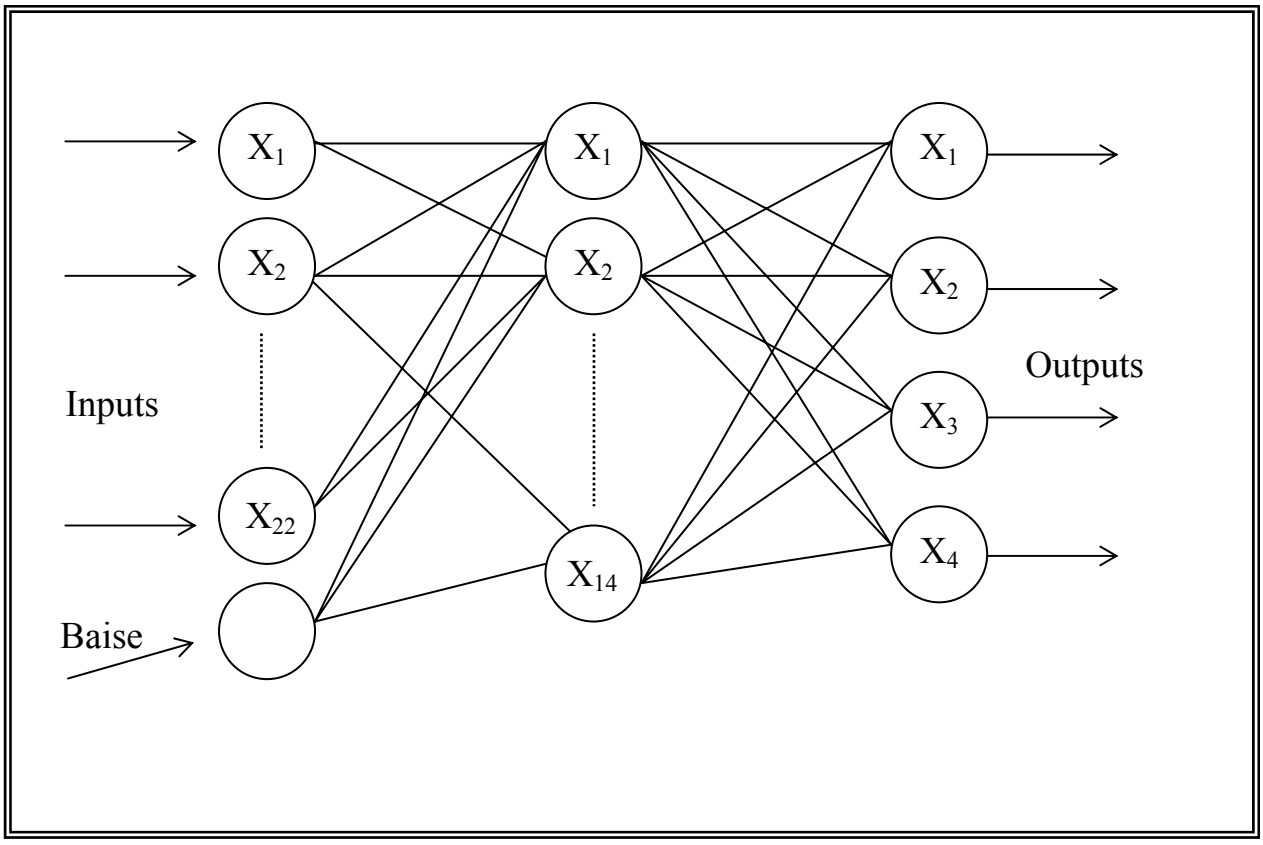
يمكن استخدام الشبكات العصبية في مهاجمة التشفير الانسيابي من خلال القيام بالخطوات التاليـة (الحمداني، 1996):

- **إيجاد المكافئ الخطي(Linear Equivalence) :** لايجاد المكافئ الخطي لسلسلة ثنائية يمكننا استخدام شبكة عصبية اصطناعية بدون تغذية خلفية ومتكونة من ثلاث طبقات . في الطبقـة الأولـى (طبقـة المدخلات) توجد 2*n خلية عصبية اصطناعية إذ أن n تمثل المكافئ الخطي، و m خليـة عـصبية اصطناعية توجد في طبقة المخرجات، حيث m تمثل عدد المراتب الثنائية الضرورية لتمثيـل قيمـة المكافئ الخطي باستخدام النظام الثنائي . أما الطبقة المخفية فلا يوجد قانون عام ومحدد لعدد الخلايـا فيها.
- **إيجاد متعدد الحدود المميز(Primitive Polynomial):** بنفس الأسلوب أعلاه، فلإيجاد متعدد الحـدود المميز يمكن استخدام شبكة عصبية اصطناعية مكونه من ثلاث طبقات، تحتوي الطبقة الأولـى علـى (2* n) خلية عصبية اصطناعية وتحتوي الطبقة الثالثة على L خلية عـصبية اصـطناعية إذ أن L تمثل عدد المراتب الثنائية التي تحتاجها لتمثيل أرقام متعددات الحدود المميزة ثنائيا، لكل مكافيء خطي يتم بناء شبكة عصبية تمتلك هذه الصفات، فمثلا لو كان عدد قيم المكافئ الخطي هو 11 عندها يجـب بناء 11 شبكة عصبية اصطناعية ، لذا فإن قيمة المكافئ الخطي لسلسلة ثنائية تحدد رقم الشبكة التـي سوف تستخدم لإيجاد متعدد الحدود المميز.
- **كسر التشفير الانسيابي بواسطة الشبكات العصبية الاصطناعية :** كسر التشفير الانسيابي يتم من خلال مرحلتين، في المرحلة الأولى وعن طريق مولد الازاحة تتولد سلاسـل لأي مـسجل ازاحـة خطـي (LFSR)، هذه السلاسل ستمثل مجموعة التدريب (Training Set) والتي تعطى الى المرحلة الثانية . في المرحلة الثانية ستقوم الشبكة العصبية الاصطناعية بايجاد المكافيء الخطي لأي سلسلة متولدة وذلك بان يكون الادخال الى الشبكة هو السلسلة التي نريد ايجاد المكافيء الخطي لها والإخراج من الـشبكة هو الرقم الثنائي الذي يمثل المكافيء الخطي.

7- التطبيق العملي

سوف يتم في هذا البحث استخدام الشبكات العصبية الاصطناعية متعددة الطبقات مـع خوارزميـة (الانتشار العكسي) في كسر نظام التشفير الانسيابي، إذ يمكن إيجاد المكافئ الخطي ومتعدد الحدود المميز الابتدائي الذي يولد السلسلة الثنائية المعطاة، اذ استخدم في هذا البحث الـشبكات العـصبية الاصـطناعية كمهاجم من نوع (Plain Text Atack) ضد متتابعة المفتاح لغرض كسر التشفير الانسيابي وذلـك مـن خلال تقديم سلسلة مشوشة أو غير كاملة بطول 2*n الى الشبكة العصبية الاصـطناعية وهـي بـدورها ستتعرف على المكافئ الخطي والحد المميز للمكافي الخطي لتلك السلسلة . استخدمنا في هذا البحث شبكة الانتشار العكسي المتألفة من (22) خلية ادخال و (4) خلية اخراج وتم استخدام طبقة مخفية واحدة تحتوي على (14) خلية، ولغرض تحسين عمل الشبكة استخدمنا (Baise Node) مضافة الـى طبقـة الادخـال،

الشكل (6) يوضح ذلك. وسنستخدم شبكة الانتشار العكسي لايجاد متعدد الحدود المميز البـدائي لمكـافئ خطي لدرجة معلومة.



الشكل 6 : الشبكة العصبية الاصطناعية المستخدمة لايجاد المكافيء الخطي

1- خطوات العمل

- **توليد متتابعة المفتاح (Key Stream Generator)**

يتم استخدام مسجلات الإزاحة الخطية (LFSR) لتوليد متتابعة المفتاح، إذ أن الإدخالات لهذا المولد هي القيمة الابتدائية لمسجل الإزاحة، طول مسجل الإزاحة، دالة التغذية المرتدة .

والاخراج لهذه المولدات ستكون سلسلة ثنائية شبه عشوائية .

مثال :- لتكن قيم الإدخال لمسجل الإزاحة الموضح في الشكل (7) هي :

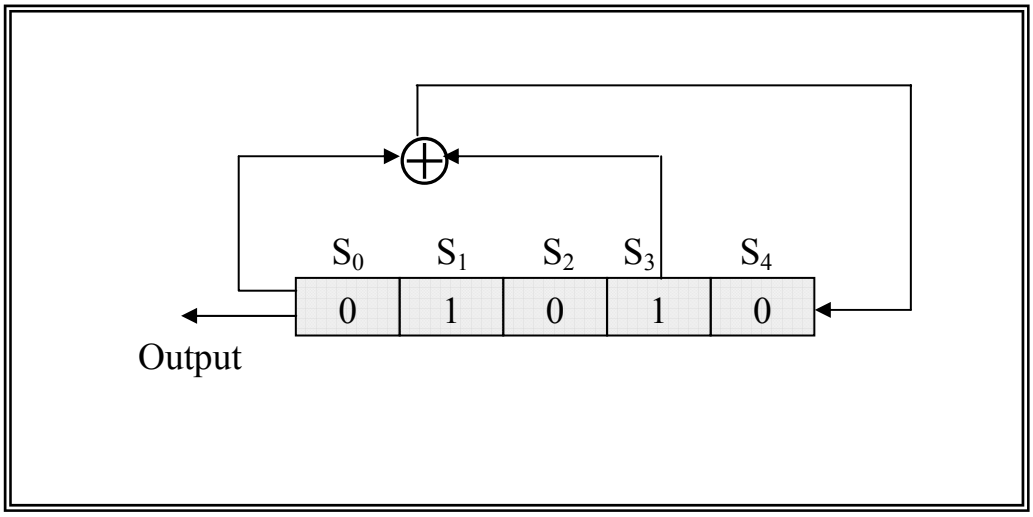
القيمة الابتدائية : 01010

طول مسجل الإزاحة : 5 ، لاحظ الشكل (7)

دالة التغذية المرتدة : $C_0S_0 \oplus C_3S_3$

ستكون السلسلة الثنائية الناتجة هي : 01010111011000111110011010010000

أطول سلسلة ممكن أن نحصل عليها من مسجلات الإزاحة الخطية هي :$2^n - 1 = 2^5 - 1 = 31$



الشكل 7 :مسجل الإزاحة ذو دالة التغذية المرتدة الخطية بدرجة (5).

- **الحصول على المكافئ الخطي (Linear Equivalence)**

المدخلات لشبكة الانتشار العكسي هي السلاسل الثنائية المراد إيجاد مكافئها الخطي، أما المخرجات فهي المكافئ الخطي المتمثل باستخدام النظام الثنائي . لذلك فإن مجموعة التعلم أو الأمثلة الخاصـة لهـذه الشبكة تتضمن السلاسل الثنائية مع قيم المكافئ الخطي انظر الجدول (2)، طول السلاسل الثنائية هـي $2 \times n$ ، ومعرفتها كافية لمعرفة بقية متتابعة المفتاح المتولدة من مسجل ازاحة بدرجة n . يتم تعليم الشبكة العصبية باستخدام خوارزمية الانتشار الخلفي، ومجموعة التعلم المحتوية على الـسلاسل الثنائيـة وقـيم المكافئ الخطي بعد إعطاء قيم عشوائية صغيرة لأوزان الشبكة . بعد مرحلة تعلـم الـشبكة يمكـن لأي محشفرة معرفة قيمة المكافئ الخطي لأي سلسلة ثنائية بتقديم السلسلة الثنائية للشبكة وحساب مخرجاتها في وقت كفوء جدا.

- **الحصول على الحد المميز**

بعد معرفة قيمة المكافيء الخطي للسلسلة الثنائية يمكن الحصول على الحد المميز الذي استخدم في توليد هذه السلسلة، عن طريق استخدام شبكة الانتشار العكسي، المدخلات لهذه الـشبكة هـي $n \times 2$ مـن السلسلة المراد ايجاد الحد المميز لها أما الاخراج فهو رقم متعدد الحدود الذي ولد هذه السلسلة، استخدمنا شبكتين عصبيتين للحصول على الحدود المميزة لسلاسل ثنائية متولدة من مسجل ازاحة ذو مكافيء خطي بدرجة (4) و(8) . الجدول (3) والجدول (4) يمثل مجموعة التعلم الخاصة بتلك الشبكات على التعاقب . فإذا أردنا ايجاد متعدد الحدود المميز لسلسلة ثنائية المكافيء الخطي لها هو (4) فإن عدد متعددات الحدود المطلوبة لتوليد السلسلة يحدد كالآتي :

$$\lambda(4) = \frac{\theta(2^4 - 1)}{4} = 2$$

لذا فإن الشبكة ستحتوي على (8) خلايا في طبقة الادخال وخلية واحدة في طبقة الاخراج .

2- تدريب الشبكة

الـشبكة تتـدرب باشـراف (Supervised) تـم اسـتخدام خوارزميـة الانتـشار العكـسي مع عدد محدد من النماذج المتكونة من زوج من الأرقام ، الأول يمثل الإدخال، والثاني يمثل الإخـراج المطلوب (والذي يمثل هنا المكافئ الخطي) .

في البداية سوف تزود الشبكة بالقيم التالية :

1. قيم عشوائية صغيرة للأوزان .
2. قيمة لنسبة التعلم، وقيمة لنسبة الخطأ وتكون قيمة صغيرة جدا (Error Tolerance).
3. قيم تمثل حد العتبة لخلايا الطبقة المخفية وطبقة الإخراج .

الجدول 2 :مجموعة التدريب الخاصة بالمكافيء الخطي

Binary Sequence	Desired Output
001011????????????????	0011
010011????????????????	0011
010111????????????????	0011
00011110????????????????	0100
00110101????????????????	0100
001111000????????????	0101
001110011??????????	0101
001110000??????????	0101
001111101??????????	0101
111010111111??????????	0110
000111010111??????????	0110
111010000011??????????	0110
000111000010??????????	0110
000111111011??????????	0110
111010001111??????????	0110
000001000100111????????	0111
000011111011011??????	1000
010101011000011011????	1001
000001000010001100????	1001
000000100001000110????	1001
11101111010111111001??	1010
11011111111101111010??	1010
11111111101111010111??	1010
011111111110101111100	1011
011111111110100111110	1011

3- اختبار الشبكة

في هذه المرحلة يتم تشغيل الشبكة لخطوة واحدة فقط، إذ أنه لا يوجد أي تعديل للأوزان في هذه المرحلة، بل يتم اعتماد الأوزان التي استقرت عليها الشبكة في المرحلة السابقة وهي مرحلة التدريب. سيقوم المستخدم بتقديم السلسلة الثنائية المشوشة (أو غير كاملة) التي يريد إيجاد المكافئ الخطي لها ومن خلال تشغيل الشبكة لخطوة واحدة سيحصل على الإخراج المطلوب وهو المكافئ الخطي للسلسلة المدخلة والذي يحدد رقم الشبكة المستخدمة لايجاد متعدد الحدود المميز لتلك السلسلة .

الجدول 3 :مجموعة التدريب الخاصة بالحدود المميزة لمكافيء خطي بدرجة (4)

Input Vector	Desired Output
00010011	0
00100110	0
10011010	0
01001101	0
00011110	1
11110101	1
11101011	1
11010110	1

الجدول 4 :مجموعة التدريب الخاصة بالحدود المميزة لمكافيء خطي بدرجة (8)

Input Vector	Desired Output
0011110011100110	0000
0111111110000101	0000
1010101011100000	0001
1100110010111111	0001
1111000010100011	0011
1111111100011000	0011
1111111101101001	0101
1111111100011010	0110
0000000101110001	1010
0000000101001010	1100
1111111101101100	1110

8- الاستنتاجات

من خلال البحث المنجز استخلصنا النقاط التالية:

1. تم التعامل مع أكفأ الشبكات العصبية الاصطناعية وهي شبكة الانتشار العكسي، والتي تعتمد نشر الخطأ الحاصل بين الاخراج المحسوب والاخراج المطلوب عبر الطبقات المخفية وصولا الى طبقة

الادخال ومن ثم تحسين الاوزان اعتمادا على ذلك الخطأ . ولكونها تستخدم دالة الـسحق (Sigmoid) فهي تضمن نشر جيد للخطأ.

2. بالرغم من أن الوقت المستغرق في عملية تعليم شبكة الانتشار العكسي كبيـر فـإن الوقـت الـلازم للحصول على الاخراج المطلوب بعد عملية انتهاء التعلم هو وقت قليل جدا.
3. الكفاءة العالية في التعامل مع البيانات الناقصة أو مشوشة، مقارنة مع الطرق الـسابقة ففـي طريقـة المصفوفات ، وخوارزمية ماسي إذا كان عدد المراتب الناقصة هو k يجب اختيار 2^k من الحالات.
4. تتطلب هذه الطريقة كسر شفرة جزء من النص المشفر لمعرفة الجزء المقابل مـن الـنص الـصريح وبالتالي معرفة جزء من متتابعة المفتاح . وهذا موضح في الجدول (2) الذي يمثل مجموعة التـدريب التي تم اعتمادها في ايجاد المكافئ الخطي وبالتالي في كسر التشفير ضمن هذا البحث.

المصادر العربية

بروست، زورت، ترجمة الدكتور المهندس ميثم محمود، 1989 . الرموز والشفرات والحاسبات، مقدمـة الى أمن المعلومات، الجامعة التكنولوجية، بغداد، الطبعة الأولى .

ياسين، شفاء عبد الرحمن، 2000 . تمييز الوجوه باستخدام الشبكة العـصبية النيوكوكنترونيـة، رسـالة ماجستير، هندسة حاسبات، جامعة الموصل.

ابراهيم، محمود خليل، 2000. الشبكات العصبية الاصطناعية، مجلة ابحاث الحاسوب، العدد الأول.

الحمداني، وسيم عبد الأمير، 1992. انظمة التشفير الإنسيابي، الجامعة التكنولوجية، بغداد .

الحمداني، وسيم عبد الأمير و وسن شاكر، 1996 . أنظمة التشفير الانسيابي، الجامعة التكنولوجية، بغداد.

المصادر الاجنبية

Beker, H. and Piper, F., 1982. Cipher System The Protection of Communication, North Wood Books, London .

Charles, P., 1989. Security in Computing, Prentice-Hall, Inc.

Daniel and Gottesman, Nov., 2000. From Quantum Cheating To Quantum Security, Physics Today, Vol. 53, Issu 11, 22 p.

Igor, A. and Helen, M., 1990. An Introduction to Neural Computing, Chapman and Hall, London .

Kinnebrock, W., Neural Networks: Fundamentals, Applications, Examples, Galgotia publications Pvt .

Ronald, A. and Gove, 1997. An Overview of Modern Cryptography, Information System Security, Vol. 6, Issue 3, 55 p.

Ruppel, R., 1986 . Analysis and Design of Stream Ciphers , Berlin-Heidelberg.

Shneier bruce, 1996. Applied Cryptography Protocol, Algorithms and Source Codes in C, Second Edition, prentice- Hill.

Talie, S., 1998. Cryptanalysis By Artificial Intelligence Techniques , M.Sc. Thesis, Iraq, Mosul .

Valluru, B. Rao and Hayagriva, V. Rao, 1993. C++ Neural Network and Fuzzy logic, BPB publications, New York .

Wasserman, Philip, D., 1989. Neural Computing Theory and Practice, Van Nostrand Reinhold .

Zeng, K. and Rao, T., Feb. 1991. Pseudo-random Bit generators in Stream Cipher Cryptography , Computer, pp.8-17 .