بحوث مستقبلية (27، 28)
ص ص [183-207]
2009

تصميم نظام حاسوبي للحماية متعددة المستويات

ابراهيم أحمد صالح[1]

الملخص

يتضمن البحث دراسة عن الحماية متعددة المستويات (MLS multilevel) والتي تستخدم في التطبيقاتِ التي تمتلك مستويات أمنية و سرية. تتضمن الطريقة المُقتَرَحة تقسيم النظام إلى مجموعة من المستويات الحسّاسةِ المتعدّدةِ ويتم اختبارُ المستخدمين بإحدى طرقِ التحقُّقِ المختلفةِ، وذلك عن طريق تقسيمه إلى مستويات ثانوية تكون آمنة إلى أبعد مستوى. بحيث يكون لكُلّ مستوى من هذه المستويات الثانوية امتيازاته وبياناته الخاصة به والتي تكون مُدَارة مِن قِبل مديرِ يسمى (Identity Manager IM) الذي يتحمل المسؤولية الكاملة ويمتلك الصلاحية لنقل المستخدم إلى مستوى أعلى أو بقائه بالمستوى نفسه. إنّ قرارَ الانتقال من مستوى إلى آخر يتم بواسطة تخصيص أوزانِ (تقديرات) مختلفةِ لكُلّ طريقة بعد إجراء سلسلة من الاختبارات، تسمح لـ(IM) بإصدار تقرير يَصِفُ النَتائِجَ و نشاط كُلّ المستخدمين (users). وتمنح هذه التقنيةِ امتيازات لمجموعةَ المستخدمين الذين يسمح لهم بالدخول إلى النظام. إن طريقة الحماية للمستويات المتعددة تتضمن الطرق الآتية: (كلمة السر/ أسئلة متعددة/ طريقه ديفي وهلمان/ DES/ RSA)، وتم اختبارها على مجموعة منتخبة من المستخدمين وحققت نسبه أمنية عالية المستوى.

Abstract

This research produces multilevel authentication used in sensitive applications that contain sensitive levels of security and the maintain confidential data. Proposed method divides the system to variety of levels and tests users against different authentication methods for each level these levels are further subdivided into more secure sublevels. Each of these levels has its privileges and data that are managed by the administrator called Identity Manager (IM) who has the full responsibility and authority to decided transfer the user from one level to a higher level, or stay at the same level. The decision of transition is done by allocate different weights for each method achieved after a series of tests, the Director of identity must issue a report describing the findings and resolution to the activity of all users. This technique gives only the required privileges to selected users who set their permissions to enter the system. The multi-level protection methods include (password, multiple questions, cutting (Hash), RSA, and DES) system was tested on a set of users, and has high security level.

(1) مدرس مساعد، قسم هندسة البرمجيات، كلية علوم الحاسبات والرياضيات، جامعة الموصل.

تاريخ الاستـــــلام:
2009/06/18

Keywords: Security, MLS, Multi level security, Authentication, Security Management.

المقدمة:

في السنوات الأخيرة أصبح التطور الحاصل في مجال الشبكات والذي يسمح بتبادل المعلومات بين عدد كبير من الحواسيب فضلاً عن اللتطور الحاصل في مجال المعلوماتية وقواعد البيانات الموسعة والتجارة الالكترونية سببا إلى ضرورة توفير طرق أمنيه ذات وثوقية عاليه لحماية هذه البيانات من المتطفلين وقراصنة الانترنيت.

تحتاج العديد مِنْ الأعمال التجارية والمنظماتِ تكون في أمس الحاجة إلى حماية وثائقها السريةِ الخاصة من قراصنة الانترنيت. لذلك تم اللجوء إلى اَستعمال أساليب أمنية متعددة المستويات (Multi Level Security MLS) والتي لا تسمح بمهاجمتها من أجل الحفاظ على سرية تلك المعلومات عن طريق استخدام وسائل اتصال محصنه لدعم المشاريع والتي لا يمكن استرداد بياناتها بسهوله عند تسرب المعلومات. لذا أصبحت الحاجة إلى استخدام النظام الأمني متعدد المستويات الذي يدعم أمنية الأعمال والذي يسمح بتصنيف البيانات وقاعدة المستخدمين في المنظومات الأمنية المتسلسلة وذلك من خلال توحيدها مع نظـام أمني غير متسلسل يسمح بعـزل بيانات المستخدمين عن بعضهم البعض (Foley Simon, 1992)(Stewart,1990)

2. النظام الأمني المتعدد المستويات :

النظام الأمني متعدد المستويات هو تطبيق حاسوبي يتعامل المعلومات بالاعتماد على مستوى حساسيتها. أي تصنف المعلومات بمستويات أمنية مختلفة وتسمح للمستخدم الحصول على البيانات في آن واحد ومن دون أن يدخل على بيانات أخرى أكثر حساسية. إذ إنه يطلَع على كل ما يحتاجه من معلومات اقل حساسية من المعلومات الأخرى. ويسمح هذا النظام بان يتشارك الأفراد جميعهم بتكوين وثائق محصنة. (Lampson, 1990) (Patel, 2005) (Schaefer, 2000)

إن للنظام الأمني المتعدد المستويات هدفين رئيسيين (Wayne, 2003) (Bell,1997) وهما:

- الهدف الأول: لايسمح لأي مستخدم بالاشتراك بالمعلومات إلا بعد تفويض بالوصول إلى مدخل المعلومات عالية التصنيف.
- الهدف الثاني: يمنع المستخدمين غير المخولين من نشر تلك المعلومات.

لقد ابتكرت الأمنية المتعددة المستويات(MLS) في عام 1970 من قبل الجيش الأميركي وذلك بالسماح لبعض المستخدمين بالاشتراك بالمعلومات ذات التصنيفات المحدودة بينما يعمل على منع استخدام المعلومات ذات التصنيفات الحساسة. وقد تم استخدام هذا النظام في ميادين أخرى مثل نظام الإدارة الموثوقة في تطبيقات الشبكة (Grid) والذي يُمكن الموظفين الإداريين والذين يعملون كمستخدمين للنظام بأن يضعوا سياسات متعددة المستويات في تطبيقاتهم، وذلك للسيطرة التامة على اتصال المستخدمين. ومن أمثلتها النموذج الأمني الذي وضعه (BLP Bell-LaPadul) والذي يعدّ

تشكيلاً لنظام حماية تعددي للسيطرة على المعلومات المتدفقة في الأنظمة (Keefe, 1998) (Welch, 1967) (Laddad, 2003)

إن مهمة (MLS) هي السيطرة على سريان تدفق البيانات داخل أنظمة الرؤية التقليدية للنظام الأمني المتعدد وتأمين المعلومات بمستوى عالٍ وبدرجة حماية عالية جدا، إذ تم وضع آلية معينة تضع محددات عن كيفية تدفق البيانات إلى داخل مركز النظام باستخدام آليات وسياسات متعددة لها تأثيرات مباشره لغرض الوصول (Sandhu, 1993)((Rivest, 1998 ومن ناحية أخرى فإنها تقيد الكيفية التي يتم بها مرور البيانات داخل مركز النظام بعدة آليات للحماية وسياسات حماية مباشرة ومصطلحات من نظام السيطرة الأمني متعدد المستويات(Millen, 1992)..

3. الدراسات السابقة

إن نموذجَ أمنِ بيل(BLP LaPadula-1976) لتشكيل MLS يقوم بتعريف قاعدتين ذات خصائص مبرهنة رياضياً لمَنْع المعلوماتِ من التَدَفُق من مستوى أمنِي عالٍ إلى أدنى، وهذا ما يسمى بـ(No Read Down) (NO Read UP"NRU"-"NRD")، إذ إن مفهوم قاعدة (NRU) هو عدم السماح لكيان ما بقراءة البيانات الموجودة في مستوى حماية أعلى، أما مفهوم قاعدة الـ(NRD) هو أن الكيانات التي لها مستويات عليا لاتسمح بقراءة البيانات الموجودة في المستوى الواطئ (Farag, 2001) (Bell, 1997).

أما الباحث ستيوارت (Stewart-1990) فقد استخدم الحماية المتعددة المستويات على أنظمة البرمجة الشيئية (OOP)، إذ قام بتقسيم الكيانات إلى أربع مجاميع وكل مجموعة وضع عليها نموذج تحقق وهذه المجاميع هي: (الكيانات التي تقوم بعملية التنصيب، مجموعة إمرار الرسالة، طرق إضافة كيان جديد، مجموعة الحذف والتحديث) (Stewart-1990).

قام الباحثان ويان وكورليف (Wayne,korolev-2003) بوصف الإطار العام لنموذج التوثيق(MAF) لتَطبيق سياساتِ الأمنِ التنظيميةِ والذي يسمح بتنوع تقنيات التوثيق واندماجها بسهولة ليعطي واجهه بسيطة لدعم سياسات متنوعة في التنفيذ الآلي (7). كما قام الباحث رايست (Rayest) وأعقبه الباحث فاراك (Farag) باستعمال طريقة التحقُّقِ متعدّدِ العواملَ، ثم بناء نظام مستويات التوثيق المستخدم في نقل النصوص والصور باستخدام شبكة محلية (LAN) وشبكة الاتصال الموسعة (WAN) المجهزة بعدة مستويات حماية, فضلاً عن التوقيع الرقمي وكبس البيانات وتقنيات البطاقات الذكية (Bell,)(Rivest, 1998) 1995

أما وكالة ناس (NAS-2004) فقد قدمت تطويرِ أمنِ حاسوبي يدعى الأنظمة الأمنية المبدئية للمعلومات المتعددة المستويات (Multilevel Information Systems MISSI-Security Initiative). إذ يقوم بإحاطة مجالات كلا من أمن الإيصالات التقليدي (Com Sec) وأمن الحاسوب (Compu Sec)، وذلك بتزويد الوكالةَ بأجهزةَ أمن ذات وثُوقية ضروريةَ لحِماية المعلوماتِ مِنْ الكشفِ أَو التعديلِ من قبل غير مخولين، ويُمكن المشاركين من استخدام آليات تحقق (verification) ولتَزود المستعملين من تبادل المعلوماتِ (Popescu, 2004) (Foley, 1990).

4. الهدف من البحث

يهدف هذا البحث إلى انجاز نظام حماية متعدد المستويات لحماية الأنظمة الحاسوبية من اللصوص وقراصنة الانترنيت، يقسم هذا النظام إلى مستويات عديدة وبدورها يتم تقسيم هذه المستويات إلى مستويات ثانوية ذات درجة حساسية عالية، ويعطى صلاحية معينة لكل مستخدم وعلى وفق مستواه ودرجة أهمية البيانات. وفي حالة زيادة مستوى سرية مستخدم مايتم نقله إلى مستوى أعلى بعد إجراء سلسلة من الاختبارات اعتمادا على الطريقة الأمنية ولضمان حماية أكبر بعد أن يمر هذا المستخدم باختبارات عديدة باعتماد طرق أمنية عالية المستوى.

5. **طرق التحقق المستخدمة في البحث**

تم في هذا البحث استخدام طرق تحقق أمنية عالية المستوى وهي كالآتي:

أ. كلمة السر (Password)

ب. طريقة الاسئلة المتعددة (Multi question)

ج. دالة ديفي-هلمان . الملحق –أ-

د. طريقة تشفير البيانات (Data Encryption Standard DES) الملحق – ب-

هـ . طريقه التشفير (Rivest, Shamir, and Adleman RSA) الملحق –ج-

تم في هذا البحث تقديم نموذج لنظام حماية متعدد المستوى يطبق على الانظمة التي تحتاج إلى درجة سرية عالية حيث تم تطبيقه على نظام قاعدة بيانات (لجنة امتحانية) ووضع له العديد من مستويات الحماية والإجراءات اللازمة لأجل تحقيق هذا الغرض.

تم تطبيق النظام المقترح على مجموعه من المستخدمين $U=\{u_1,u_2,....u_{10}\}$، وهؤلاء المستخدمون يعملون ضمن مستوى ترخيص معين ومختلف الحساسية، ليكن هذه المستويات $L=\{l_0,l_1,....,l_4\}$ وهذه المستويات (إدخال أسماء طلبة، إدخال درجات، حساب درجة السعي، حساب المعدل، النتائج) ان العملية المعتمدة في التصنيف الأمني لكل مستوى كما يأتي:

1. l_{01} : Low Security
   مستوى حماية منخفض الذي يمثل أوطأ درجة في السرية (محدود)
2. l_{02} : Medium Security
   مستوى حماية متوسط الانخفاض أو ما يسمى بدرجة سرية (مكتوم)
3. l_{11} : High Medium Security
   مستوى حماية بدرجة سرية متوسط عالٍ (سري)
4. l_{12} : High Security
   مستوى حماية بدرجة سرية عالي (سري للغاية)
5. l_2 : Very High Security
   مستوى الحماية بدرجة سرية العالي جدا(سري وشخصي للغاية)

ولضمان تطبيق نظام أمني صحيح وآمن يجب أن يؤدي النظام المقترح اختبار حادّ إلى كُلّ مستخدم داخل النظام باستعمال طرقِ التحقُّقِ المختلفةِ المدرجة أعلاه التي في المجموعةِ الآتية:

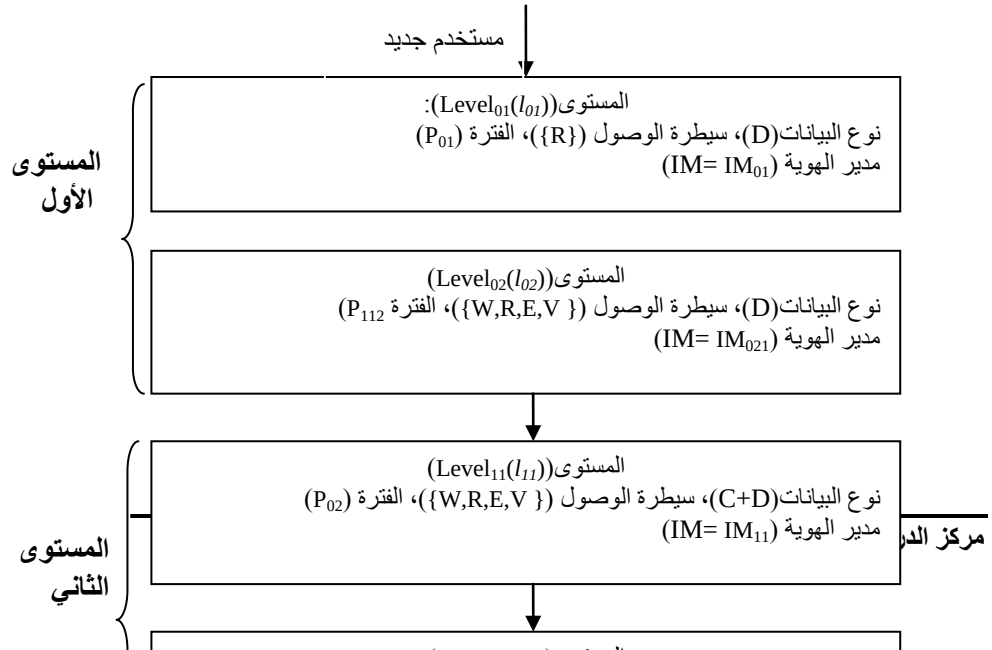
$$AU = \{au_1, au2 \ldots\ldots au_k\}$$

إذ يمثل كُلّ عناصر هذه المجموعةِ طريقة تحقُّقِ معيّنةِ

وبالاطلاع على عدة دراسات (Schellhorn,2000)(Popescu,2004) وجد أن النظام ينقسم إلى عدة مستويات تحقُّقِ مختلفةِ والبعض مِنْ هذه المستويات منقسمة إلى مستويات ثانويةِ على سبيل المثال، المستوى l0 قَدْ ينقسم إلى مستويين ثانويين l01 و l02وكُل منهما لِه مستخدم خاص به الذي يعمل على مجموعة من أنواع البياناتَ والإمتيازاتَ. لتكن مجموعةَ الإمتيازاتِ P={p1,p2,….pl} مُمَثَّلة بمصفوفة سيطرة على دخولِ والتي تَحتوي بَعْض الإمتيازاتِ مثل قراءة (R)، كتابة (W)، يُنفّذُ (E)، ملحق (A)، وجهة نظر(V-View)، مراقب(M-Monitor)، تقييم (AS-Assessment)، إدارة (Ma-manger) وهكذا. (لاجل السيطرة على الدخولَ تكون هناك (n) من الإمتيازات والتي تؤدي الى 2n من المجموعات. على سبيل المثال، في حالة وجود سيطره ذات اربعة إمتيازاتَ مثل R, W, E, A، تؤدي للحصول على 16 مجموعةِ مثل R/W, R/E....الخ فضلاً عن ذلك يحتوي النظام المُقتَرَح على مجموعة تحتوي على أنواع البيانات.{T={D,C,B,A حيث تم تخصيص كل من هذه البيانات الى مستتخدم على وفق الرقم التسلسلي لذلكِ المستوى وكما يأتي:

1. البيانات غير المصنفة التي يمكن تمثيلها بالحرف(D)
2. البيانات ذات سرية خاصة محدودة تمثل بالحرف (C)
3. البيانات ذات درجة السرية العالية تمثل بالحرف (B)
4. البيانات ذات السرية العالية جدا تمثل بالحرف(A)

الشكل ذو الرقم (1) يوضح نظامَ التحقُّقِ ذا المستوي المتعدّدِ العامّ:



شكل رقم (1) نظام التوثيق المتعدد المستوى

في الشكل ذي الرقم (1) نلاحظ ان كل مستوى يرتبط مع مستويات ثانوية، وان هناك مدراء للإدارة مسؤولاً عن مراقبة سلوك المستخدم ومنح المستخدمين استحقاقاتهم ويسمى المدير الهوية (IM Identity Manager) ولتوضيح كيفية عمل النظام لنفترض ان المدير يحتاج إلى فحص النتائج لمستخدم معين والذي اختبر بطريقة التوثيق، إذ يبدأ بالمستوى الأول ($level_0$) إذ يوجد مستخدمين موثقين مسبقا ولكن عند الحاجة فضلاً عن مستخدم جديد يجب أن يكون مدققاً مبدئيا بإحدى طرق التوثيق مثل كلمة السر التي تم تحديدها لغرض الانتقال وإعطاء ترخيص للدخول فقط قبل إجراء عملية الفحص (تكون مختلفة عن كلمة السر الموجودة في المستوى الثانوي)، وبجب أن تكون كلمة السر مختلفة عن تلك التي تستخدم للتسجيل. عند اجتياز المستخدم اختبار التحقُّقَ عندها يكون المدير قد رشح المستخدم إلى الجزءِ الأولِ مِنْ مستوى (01) اي l_{01} ليمنح المستعملِ حق القراءة (R) فقط إلى قالب الطباعة واستخدام المعلومات غير مصنفة (D). فضلاً عن أن هذا المستخدم يجب أن يبقى في مستواه(l_{01}) المحدد ومساويا للفترة الزمنية نفسها (p_{01}) التي حددت من قبل المدير في كل مستوى من المستويات الثانوية وإذا وصلت الفترة الى نهايتها عندها يجب على المدير ان يقوم بفحصه مع اضافة طرق التوثيق مثل كلمة السر والاسئلة الخاصة لكي يحوله إلى المرحلة المقبلة التي تكون ذات مستوى أعلى (l_{02}) ويحدد المدير في هذه المرحله التقديرات (العلامات) لكل طريقة توثيقية معتمدا على الوزن (w) لكل طريقة توثيق الموضحة بالجدول ذي الرقم (3)، من جهة أخرى إذا فشل المستخدم في الاختبار فعندها يكون مرفوضاً ويقوم المدير بتحديد المرتبة (R) لكل مستخدم ويعتمد على نجاحات الاختبارات لكل مستخدم لتؤهلهم الانتقال إلى مستوى ثانوي متأكد، على سبيل المثال ان الاختبار الناجح هو(2) فإن مرتبة المستخدم تكون (R_2) فقيم المراتب تنظم على أساس رتبة المستخدم ثم يعطي المدير توجيها مناسبا حول درجة الفعالية المناسبة لكل مستخدم ومرحلته موضحة في تقرير المدير ضمن قطاعه النتيجة

جدول ذو الرقم (1) يوضح الأوزان في طريق التوثيق المختلفة

المستويات الانتقالية الثانوية (من... الى...)	طرق الترخيص	الأوزان (w)
مستوى 01 - مستوى 02	كلمة السر	35
	الأسئلة المتعددة	65
مستوى 02 –مستوى 11	الأسئلة المتعددة	25
	طريقه ديفي-هلمان	75
مستوى 11-مستوى 12	طريقه ديفي-هلمان	30
	DES	70
مستوى 12-مستوى 2	طريقه ديفي-هلمان	10
	DES	20
	RSA	50

الخطوة المهمة في هذا البحث تكمن في إدارة وفحص تعددية المستخدم في مستوياتها الثانوية. وسيتم وصف عملية الانتقال لبعض المستويات وتعمل المستويات الباقية بالأسلوب نفسه، لنبدأ مع المستخدم بالمستوى ($level_{01}$) إذ يرغب المدير في فحص المستخدم (U_i) بعد أن يبقى فتره طويلة من الوقت (p_{01}) يعمل في المستوى الثاني لكي ينقله إلى المستوى الأعلى القادم ولإنجاز هذه المهمة يواجه المستخدم اختباراً توثيقياً أخر الذي يكون من طريقتين من طرق التوثيق مثل (كلمة السر) وطلب بعض الاسئلة المعروفة فقط لدى المستخدم الشرعي ، ويعتمد قرار المدير على النتيجة في هذا الاختبار وكذلك فإن المدير حدد بعض المؤشرات (الاوزان) لكل طريقه توثيق كما مبين بالجدول ذي الرقم (2) الذي يكرس الاوزان لكل مستوى وقد تتفاوت من مستوى لاخر وحسب قرار مدير التعريف لهذة المستويات. إذا فشل المستخدم في اختبار كلمة السر فيبقى آنذاك في المستوى الثانوي الأصلي $level_{01}$ لكنه إذا يمرر عده اسئلة استجوابية فعندها يقرر المدير تمريره إلى مستوى الحد الأعلى القادم $level_{02}$ لكنه مع حصر وتقييد الامتيازات الجديدة لذلك المستوى مثل اعتبار الامتياز لبعض الملفات. نسمي هذا القرار انتقال جزئي أو مرور جزئي ونفترض في هذه المرحلة بان الكثير من الامتيازات قد منحت الى المستخدم مع انتقال جزئي إذ سيكون قد اعطي النسبة المئوية المعينة في مجمل الامتيازات المسموحة لتعيين المستوى الثانوي وتحديده، من جهة أخرى فإن أي مستخدم يمكنه أن يمنح كل الامتيازات في المستوى الثانوي هذا عندما يجتاز طرق التوثيق بنجاح بالطريقة نفسها فان كل مستخدم في المستوى ($level_{02}$) يجب ان يقيم فترة معينة من الزمن عندها يجب ان يمر باختبار مجموعة أخرى من الطرق التوثيقية الإضافية التي تختلف عن الطريقتين الأوليتين (كلمة السر، الأسئلة المتعددة) تعتمد على التشفير والدخول على قاعدة بيانات مشفرة فعند اختبار المستخدم يعمل على فك الشفرة ومن هذه الطرق طريقة التشفير (RSA) وطريقة التشفير القياسية (DES)

فضلاً عن طريقة ديفي-هلمان إذ يضع تقديرات (أوزان) لكل طريقة من طرق الترخيص توزع حسب نوعية الطريقة ودرجة وثوقيتها، والجدول ذو الرقم (2) يوضح المستويات الثانوية لكل مرحلة وملخص عمليات الانتقالات إلى المستويات الثانوية.

جدول ذو الرقم (2) يوضح شروط الانتقال بين المستويات الثانوية

المستوى الأصلي	المستوى الجديد	طرق الترخيص	الأوزان	شرط الانتقال
المستوى 01	المستوى 02	كلمة السر أسئلة متعددة	35 65	اذا كان (w1=35)يبقى بالمستوى الاصلي نفسه اذا كان (w2=65) ينتقل الى المستوى 11 مع مقيد بالصورة والتنفيذ اذا كان (w1=35 &w2=65) ينقل كاملا الى المستوى 11
المستوى 02	المستوى 11	اسئلة متعددة طريقة ديفي-هلمان	25 75	اذا كان (w1=25)يبقى بالمستوى الاصلي نفسه 02 اذا كان (w2=75) ينتقل الى المستوى 11 مع مقيد بالصورة والتنفيذ هذا كان (w1=25 &w2=75) ينقل كاملا الى المستوى 11
المستوى 11	المستوى 12	طريقة ديفي-هلمان DES	30 70	اذا كان (w1=30)يبقى بالمستوى الاصلي نفسه 11 اذا كان (w2=70) ينتقل الى المستوى 12 مع مقيد بالصورة والتنفيذ هذا كان (w1=30 &w2=70) ينقل كاملا الى المستوى 12
المستوى 12	المستوى 2	طريقة ديفي-هلمان DES RSA	10 40 50	وصول كامل (يتحقق مرور كامل من كل طرق الترخيص)

كما تم توضيحه سابقا، يوجد لكُلّ مستوى ثانوي مُشرف يُسمى مديرَ هويةِ (IM). على سبيل المثال مدير المستوى الثانوي level01 يقوم بإيجاز المدير (IM01) ومدير المستوى IM11. كُلّ مدير مسؤول عن مراقبة نشاطاتِ المستخدم وكذلك يَمْنحُ إمتيازاتَ مختلفةً وحاسِمَة للمستخدمين ليقرر من يرسل إلى مستوى أعلى أَو يبقى في مستواه الأصلي. كُلّ IM يَجِبُ أَنْ يصدر تقريراً إدارياً الذي يمكن أن يُستَعملَ لتَعْقيب ومُرَاقبَة تطبيقات كُلّ المستخدمين. هذا التقريرِ سَيُزوّدُ المدير الأعلى للتطبيقِ بتوضيح وثوقية كُلّ مستخدم وقَدْ يُستَعملُ لتَقييم أصالته. إذا كان مستخدم معيّن لديه إخفاق من الوصول، هنا يقوم المدير الأعلى بإهْمال هذا المستخدم كلياً مِنْ التطبيقِ. من الناحية الأخرى إذا تصرّفُ بَعْض المستخدمين في سلوك أكثر تَحقيقاً، يقررّ المدير حول ذلك المستخدم بمنحه مستوى لترخيص أعلى خصوصا أولئك الذين يصلون المستوى الثانوي (ll2)، سَنَعطي تفصيل نشاطات هؤلاء المدراءِ في قسمِ النتيجةِ. وأخيراً، الفترة P2 في الحدّ الأعلى 2 l تستعمل ليس كفترة للانتقال إلى المستويات الأخرى، لكن هذه الفترةِ يُمكنُ أَنْ تَكُونَ مستعملة من قبل مديرِ ذلك المستوى لتَأهيل المستخدمين.

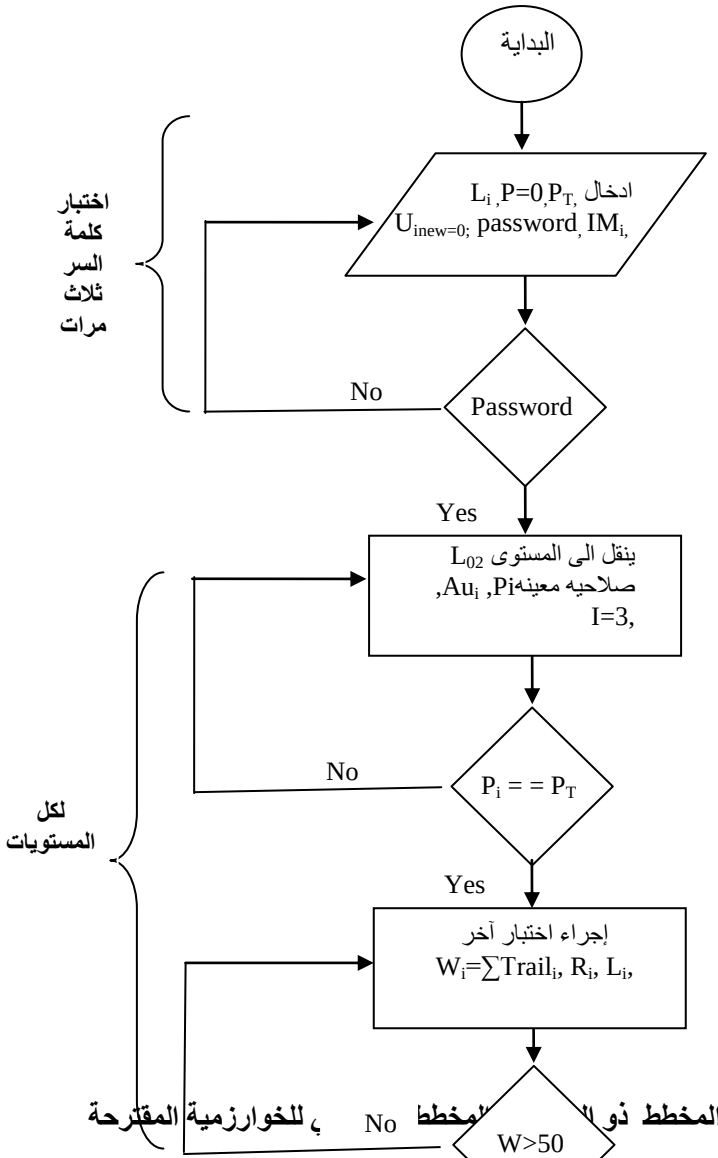
5. الخوارزمية المقترحة

تم تصميم النظام الحاسوبي باستخدام نظام (Matlab-7) لتطبيق خوارزمية أمنية متعددة المستويات وبالاعتماد على المعطيات الآتية:

1. مجموعة المستويات الرئيسة والثانوية $L=\{l_0,l_1,....,l_m\}$
2. مجموعة المستخدمين U={u1,u2,….un}
3. مجموعة طرق التحقق AU ={au1,au2, ……auk}
4. مجموعة الامتيازات P={p1,p2,….pl}
5. مجموعة أنواع البيانات T={D,C,B,A}
6. مجموعة مدراء المستويات الثانوية والرئيسة M={IM0{l0},,IM0{l0},IM1{l1}IM1{l1},……Imn{ln}}
7. الاوزان (الدرجة) يرمز لها بالرمز (w) لكل طريقه توثيق
8. مجموعه الاختبارات لكل مستخدمTrail [Ui]
9. مجموعه المرتبة لكل مستخدم عند إجراء الاختبار

R={Rl01(n) Rl02 (n),,,,,,,,,,,, Rlkm (n)} , where n= l

عند إجراء الاختبار على المستخدمين الجدد ليتسنى لمدراء المستويات من إصدار تقريره حسب نتائج الاختبار(Trail) التي يتم إجراؤها لكل مستوى معتمدا على الاختبارات ومقدار الأوزان (W) الموزعة لكل اختبار التي تمكن المدير من نقله إلى مستوى أعلى أو بقائه ويحدد مستواه والمرتبة المقررة له والشكل ذو الرقم (1) يمثل المخطط الانسيابي للخوارزمية المقترحة



المخطط ذو ال المخطط ب للخوارزمية المقترحة

7. تحليل النظام

عند تقييم مقدار المعلومات لل نظام او أي نظام مشابه نجد ما يأتي:

1. أن درجة توثيق المعلومات للنظام متعدد المستويات في توثيق المستخدمين تكون اقل من حجم المعلو ستوى الواحد إذا تم التعامل مع كل مستوى بصورة مستقلة لكل مستوى من المستويات المتاحة تكون محدودة في توثيق وطبقا لدرجة التوثيق المتاحة لكل مستوى من المستويات، لذا فإن النظام يوفر وسيلة فعالة في حماية المعلومات الموزعة على مستويات أمنية مختلفة أعلى منها مستوى. لو فرضنا ان E(X) هي مدخلات في

النظام الواحد عندئذ تكون المدخلات في النظام المتعدد المستوى E(X)/n إذ إن n تمثل عدداً من المستويات الممكنة، ولتعزيز النظام الامني وتحسينه يكون تقسيم النظام إلى عدد كبير من المستويات على شرط ان يكون لكل مستوى قيمة متساوية من البيانات.

2. كلما كان عدد المستويات اكثر على افتراض لكل مستوى قيمة متساوية من البيانات وافتراض آخر بأن كمية المعلومات تتوزع الى عدة قيم، لذا فإن $E(X_{lin})$ ..... $E(x_{l01})$, $E(X_{l02})$, يكون مقدار المعلومات في كل مستوى ثانوي تكمن إلى عدة أنماط مختلفة إذ إن لكل مستوى نسبة مئوية من اجمالي الادخالات $E(X) = \sum_{i=0}^{n} E(X_i)$ ، نفترض ان النسبة المئوية هي $(C_1, C2, \ldots C_n)$ إذ إن كل مستوى يضم $E(X)*C_i$ والرمز i تمثل مستوى ثانوي مستقل.

3. من جهة أخرى تعدّ إمكانية كشف البيانات (المعلومات) في كل مستوى ثانوي يرتبط باحتمالية كشف المعلومات في المستوى الواحد الذي يضمه النظام. إن احتمالية كشف المعلومات في المستويات المتعددة تكون اقل من نسبة كشفها في حالة النظام ذي المستوى الواحد، لنفرض أن P(X) هو احتمالية كشف المعلومات في المستوى الواحد $P(L_1), P(L_2), \ldots, P(L_n)$ إذ إن $P(L_1) < P(L_2) < \ldots P(L_n)$ عندئذ يكون معدل الاحتمالية موضحه بالمعادلة ذات الرقم (1)

$$P(X) = (\sum_{i=1}^{i=n} P(L_i)) / n \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

4. المستوى المتعدد له امتيازات وأنواع البيانات مخولة في نمط تلك الامتيازات في مستوى المستخدمين التوثيقية وهذا يعني أن المستوى التوثيقي المنخفض (الأقل أهمية) للمستخدمين يكون له حقوق اعتيادية. لذلك عندما تكشف يكون لها تأثير قليل ولكن يعطي دلالة أو إشارة عن مصداقية المستخدم لذلك فإن السيطرة على الوصول المستعمل في هذا النظام هو تضييف (تبويب) سيطرة الوصول التي تخول الامتيازات على وفق أهمية أو درجة المستوى الفردي (المستقل). وكنتيجة لذلك فإن النظام متعدد المستويات يفترض ضمان حماية عالية وخصوصية استعمال وثوقية في التطبيق.

إن النتائج التي تم الحصول عليها تم وصفها بالتفصيل وبالاخص نقل المستخدمين الجدد من المستوى level01 إلى المستوى الثاني level02 وبتقرير فعالية الإدارة لكل مستوى، ولكن مستويات النقل الاخرى توصف باختصار تبعا للمستويات الأعلى المشابهة له.ا

اولاً: اجراء الاختبار للمستخدمين الجدد: يتم إجراء الاختبار على وفق الخطوات الآتيه:

أ. ادخال عدد المستخدمين: (10)

طريقة الترخيص : كلمة السر

نتيجه الاختبار : النجاح (P) او الفشل (F)

الجدول ذو الرقم (3) يوضح نتائج المستخدمين وقرار المدير

جدول ذو الرقم (3) يوضح نتائج اختبار المستخدمين الجدد

المستخدم	النتيجة	رقم الاختبار	قرار المدير
مستخدم ذو الرقم (1)	F	1	يدخل اختبار مره اخرى
مستخدم ذو الرقم (2)	P	1	يرحل الى المستوى (01)
مستخدم ذو الرقم (3)	P	1	يرحل الى المستوى (01)
مستخدم ذو الرقم (4)	F	1	يدخل اختبار مره اخرى
مستخدم ذو الرقم (5)	F	1	يدخل اختبار مره اخرى
مستخدم ذو الرقم (6)	F	1	يدخل اختبار مره اخرى
مستخدم ذو الرقم (7)	P	1	يرحل الى المستوى (01)
مستخدم ذو الرقم (8)	P	1	يرحل الى المستوى (01)
مستخدم ذو الرقم (9)	F	1	يدخل اختبار مره اخرى
مستخدم ذو الرقم (10)	F	1	يدخل اختبار مره اخرى

ب. إعادة الاختبار للذين لم يجتازوا من المحاولة الأولى كما موضح بالجدول ذي الرقم (4)

جدول رقم (4) يوضح نتائج اختبار الذين لم يجتازوا الاختبار

المستخدم	النتيجة	رقم الاختبار	قرار المدير
مستخدم ذو الرقم (1)	F	2	يدخل الاختبار مرة ثالثة
مستخدم ذو الرقم (4)	P	2	يدحل الى المستوى (01)
مستخدم ذو الرقم (5)	F	2	يدخل الاختبار مرة ثالثة
مستخدم ذو الرقم (6)	F	2	يدخل الاختبار مرة ثالثة
مستخدم ذو الرقم (9)	P	2	يدحل الى المستوى (01)
مستخدم ذو الرقم (10)	F	2	يدخل الاختبار مرة ثالثة

ج. إعادة الاختبار للمستخدمين الذين لم يجتازوا من المرحلة الثانية كما موضح بالجدول ذي الرقم (5)

جدول رقم (5) يوضح اختبار المرحلة الثانية

المستخدم	النتيجة	رقم الاختبار	قرار المدير
مستخدم ذو الرقم (1)	F	3	رفض المستخدم
مستخدم ذو الرقم (5)	P	3	يرحل الى المستوى (01)
مستخدم ذو الرقم (6)	F	3	رفض المستخدم
مستخدم ذو الرقم (10)	P	3	يرحل الى المستوى (01)

د. يصدر المدير تقريره وكما موضح بالجدول ذي الرقم (6):

جدول رقم (6) يوضح تقرير مدير المستوى

المستخدمون	رقم الاختبار	قرار المدير	المرتبة في المستوى (01) تسمى (R_{01})
مستخدم ذو الرقم (1)	3	رفض المستخدم	$R_{01}(3)$
مستخدم ذو الرقم (2)	1	يدخل الى المستوى (01)	$R_{01}(1)$
مستخدم ذو الرقم (3)	1	يدخل الى المستوى (01)	$R_{01}(1)$
مستخدم ذو الرقم (4)	2	يدخل الى المستوى (01)	$R_{01}(2)$
مستخدم ذو الرقم (5)	3	يدخل الى المستوى (01)	$R_{01}(3)$
مستخدم ذو الرقم (6)	3	رفض المستخدم	$R_{01}(3)$
مستخدم ذو الرقم (7)	1	يدخل الى المستوى (01)	$R_{01}(1)$
مستخدم ذو الرقم (8)	1	يدخل الى المستوى (01)	$R_{01}(1)$
مستخدم ذو الرقم (9)	2	يدخل الى المستوى (01)	$R_{01}(2)$
مستخدم ذو الرقم (10)	3	يدخل الى المستوى (01)	$R_{01}(3)$

ثانياً: الانتقال من المستوى (01) الى المستوى (02):

بالطريقة نفسها يتم إجراء الاختبار للنقل من المستوى(01) إلى المستوى (02) وذلك بزيادة طرق الاختبار بدلا من استخدام كلمة السر ويتم الآن إضافة طريقة أخرى مثلا طريقة (RSA) وكل طريقة لها وزن خاص بها تقسم على وفق كفاءة الطريقة مثلا (كلمة السر 35% وطريقة (RSA) (65%) ويتضمن تقرير المدير (IM) على أربعة احتمالات لوصف حالة المستخدم:

1. إذا اجتاز المستخدم الاختبارين ينقل الى المستوى (02).
2. إذا فشل في الاثنين يبقى بمستواه.
3. إذا اجتاز الاختبار الذي يكون وزنه اقل وفشل بالاختبار الذي وزنه اكبر يبقى في مستواه.
4. إذا اجتاز الاختبار الذي يكون وزنه اكبر وفشل بالاختبار الذي وزنه اقل ، يتم نقله الى المستوى (02) مع تقيد في الامتيازات.

ثالثاً: الانتقال من المستوى 02 الى المستوى 11

يتم إجراء اختبار باستخدام طريقة الأسئلة المتعددة وطريقة ديفي -هلمان

رابعاً: الانتقال من المستوى 11 الى المستوى 12

يتم إجراء اختبار باستخدام طريقة ديفي-هلمان وطريقة التشفير (DES).

خامساً: الانتقال من المستوى 12 إلى المستوى 2

يتم إجراء الاختبار بطريقة ديفي-هلمان وطريقة التشفير(DES)وطريقة (RSA)

8. الاستنتاجات

ان الطريقة المقدمة في هذا البحث لتوفير مستويات مختلفة من الترخيص خصوصا على الأنظمة الحساسة والتي تكون دائما معرضة للهجوم من المخادعين او المتطفلين على الانظمة حيث إن الخاصية الأكثر أهمية في هذا النظام هي ان المستخدمين الذين يعملون في مستوى واحد يجب ان يختبروا بطرق توثيقية مختلفة لكي ينتقلوا إلى المستوى التوثيقي الأعلى في مستوى الحماية. يكون المستخدمين مخولين بامتيازات معينة وبمقدار من الامتيازات المحكمة المعتمدة على ما يخوله هذا المستوى لذلك اذا كان المستخدم في مستوى منخفض يكون له امتيازات بسيطه لانجاز انواع بيانات بسيطة ولأجل نقل المستخدم إلى مستوى أعلى فإنه يتم أختبار مصداقيته عن طريق إجراء العديد من الاختبارات وعند اجتيازه الاختبار يقرر المدير الذي هو مسؤول عن التوثيق بإصدار تقريره بنقله إلى مستوى حماية أعلى أما في حالة فشله في الاختبار فيقرر المدير أن يبقى بمستواه نفسه.

احد مميزات هذا النظام هو وجود أنماط أو طرق توثيقية مختلفة والتي تكون مسيطر عليها بالاعتماد على مرتبة (درجة الحماية) لهذه المستويات المبينة بالجدول ذي الرقم (1) لذلك فإن المدير لكل مستوى يحدد الامتيازات المعينة للمستخدمين بعد أن يجري اختبارات تخولهم بتحديد أنواع البيانات.

أخيراً ينبغي على كل مدير ان يعطي لكل مستوى ثانوي تقريرا يصف فيه نشاطات المستخدمين، ولهذا التقرير أهمية كبيرة لأنه يعكس سلوك المستخدمين وعدد المحاولات غير الناجحة المبذولة ويكون وكيلاً أو مرشداً لكل توثيقات المستخدمين الذي يعتمد كوسيلة فعالة في تعزيز نظام الحماية ليحقق مفهوم نظام لإدارة المحمي.

المصادر

المصادر باللغة العربية

1. الحمامي، علاء حسين، الحمامي، محمد علاء (2008)، " اخفاء المعلومات والعلامات المائية"، جامعة الشارقة، البحرين.

المصادر باللغة الانكليزية

2. Bell D. & LaPadula L. (1997), "*Secure computer systems*", Unified exposition and, mastics interpretation. MITRE technical report, MITRE Corporation, Bedford Massachusetts.
3. Farag **A.** & Osama S. (2001), "*Multilevel Security Computer Networks*", Msc Thesis, Dept. of Computer Science and Engineering, Faculty of Electronic engineering, Menoufia University, Menouf, Egypt.
4. J. K. Millen & T. F. Lunt. (1992), Security for Object-Oriented Database Systems. In" *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy,"* Oakland, California, pages 260-272.
5. Laddad R. (2003), "*Aspect in Action: Practical Aspect-Oriented Programming*". Manning.
6. Lampson B.W. (1969), "*Dynamic protection structures*", Proc. AFIPS FJCC, Vol. 35, AFIPS Press, Niontvale, N.J., pp. 27-38.
7. M. Schaefer. If A1 is the Answer, What Was the Question? An Edgy Naif's Retrospective on Promulgating the Trusted Computer Systems evaluation criteria. In Annual Computer Security Applications Conference, pages 204-228. IEEE Press, 2004.
8. N. Foley Simon, "Multilevel Security and Quality of Protection", Department of Computer Science, University College, Cork, Ireland. , Cork Constraint Computation Centre, University College Cork, Ireland, Dipartiment di Scienze, Universitµa \G. D'Annunzio" di Chieti-Pescara, Italy**.**
9. Patel D., Collins R., Vanfleet W. M., Calloni B. A., Wilding M. M., MacLearn L., & Luke J. A. (2002), "*Deeply Embedded High Assurance (Multiple Independent Levels of Security/Safety) MILS Architecture*", Center for research on

economic development and policy reform, Retrieved on 2005-11-06.

10. Popescu B.C., Crispo B. & Tanenbaum A. S. (2004), "*Support for multi-level security policies in drm architectures*". In 13th New Security Paradigms Workshop.
11. Rivest R. L., Robshaw M. J. B., Sidney R., & Yin Y. L. (1998), "*The RC6TM Block cipher*", M.I.T Laboratory for Computer Science, U. S. A., San Mateo.
12. Sandhu R. S. (1993), "*Lattice based access control models*". IEEE Computer, 26(11):9-19.
13. Schellhorn G., Reif W., Schairer A., Karger P. A., Austel V. & Toll D. (2000), "*Verification of a formal security model for multiplicative smart cards*". In ESORICS, pages 17-36, 29. F.B. Schneider. Enforceable**.**
14. Stewart Black, Vijay Varadharajan (1990), "**A** Multilevel Security Model for a Distributed Object-Oriented System" Networks and Communications Laboratory HP Laboratories Bristol June.
15. T. F. Keefe, W. T. Tsal & M. B. Thurasingham (1988), *"A Multilevel Security Model for Object-Oriented Systems"*, Proc. 11th National Security Conference.
16. Wayne J. V., Korolev S. G. & Thomas H. C. (2003), "*A Framework for Multi-mode Authentication: Overview and Implementation, Guide Computer Security Division*", Information Technology Laboratory, National Institute of Standards and Technology.
17. Welch I. S. & Stroud R. J. (2003), "*Re-engineering security as a crosscutting concern*". Computer. J, 46(5):578–589.

الملحق (أ)
طريقه ديفي-هلمان

تعتمد هذه الطريقه على استخدام مفتاح سري لفك الشفرة وتعتمد على صعوبة حساب اللوغارتمات وكما يأتي:

يعرف جذر اولي p حيث يؤثر فتراته من ((p-1)-**1**)، لهذه الطريقة، يوجد عددان معروفان بصوره عامه هما: عدد اولي p وعدد الذي يكون α الذي يكون الجذر الأولي إلى q. اذا رغب المستفيدان A, B في تبادل المفتاح فيما بينهما يختار A رقماً عشوائياً X^A بحيث إن يكون اصغر من q يتم حساب

$$Y_a= \alpha^{XA} \bmod q$$

وبالطريقة نفسها يختار B بصورة مستقلة عدد اولي q ويختار رقماً عشوائياً $X^B<q$ ويحسب

$$Y_B= \alpha^{Xb} \bmod q$$

ويحتفظ كل جانب بقيمةXبصورة سرية ويجعل قيمةYمتوفرة علنا إلى الجانب الآخر.

يحسبA المفتاح K وكما يأتي:

$$K= (Y_A)^{XA} \bmod q$$

أما B فيحسب المفتاح كما يأتي:

$$K=(Y_A)^{Xb} \bmod q$$

وهاتان المعادلتان ينتجان قيمة واحدة هي المفتاح السري

الملحق – ب -
طريقه التشفير (RSA)

سميت بهذا الاسم نسبة إلى مكتشفيها (Ron Rivest, Adi Shamir, and Leonard Adleman) التي تعدّ واحدة من طرق التشفير المفضلة باستخدام مفتاح التشفير العام (public key) ويمكن إيضاح هذه الخوارزميه بما يأتي:

حيث ان مفتاح التشفير العام (*n,e*) ومفتاح التشفير الخاص (*n,d*)

يتم اظهار المفتاحين اللذين هما مفتاح التشفير العام (e,n)0 ومفتا ح التشفير الخاص (d,n)

أ. يتم توليد عددين أوليين (p,q) وعدد ثالث كبير (e).

ب. يتم حساب n=p*q المفتاح العام (e,n)

ج. بعد ذلك يتم حساب المفتاح السري

$d = e^{-1} \bmod \Phi(n)$ حيث إن

$\phi(n) = (q-1)(p-1)$ والحد Φ (n) بدالة قسمة ايلور. لحساب d كما يأتي:

$$d = \frac{GCD(\Phi(n)) * \Phi(n) + 1}{e}$$

التأكد من أن d,e هما عددان صحيحجان وإن

$$e * d (\bmod \Phi(n) = 1$$

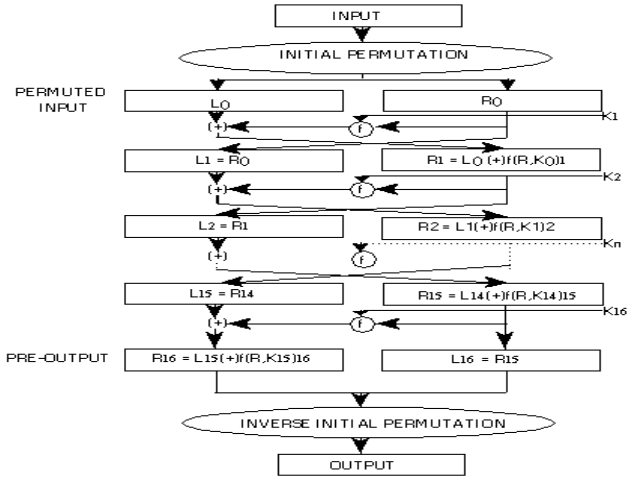
د. المفتاح السري (e,n)

أما لتشفير النص حيث إن كل نص (Mi) يتحول إلى نص مشفر (Ci)
وباستخدام المفتاح العام يتم التشفير كالاتي:

$$C_i \equiv M_i^E \bmod e(n)$$

الملحق (ج)
طريقة التشفير (DES)

تعد خوارزمية Data Encryption System (DES) أحد أهم الخوارزميات التناظرية المستخدمة بشكل كبير لذلك من الضروري استعراض الأنماط الأساسية التي تعمل بها الخوارزمية مع بيان ميزات ومساوئ كل نمط فضلاً عن الحالة التي يستخدم بها .تم اعتماد طول المفتاح ليكون 64 بت ولكن يستعمل منها فقط 56 بت فقط بشكل فعال وتستعمل البقية كخانات تدقيق للأخطاء، خوارزمية DES ثلاث مرات بمفاتيح مختلفة.



حيث إن Ln يمثل المقطع الايسر من 32 بت وRn يمثل المقطع الايمن من 32 بت وان kn مفتاح مكون من 64 بت

يمكن تلخيص التشفير بهذه الطريقة بالخطوات الآتية:

- يتم تطبيق عملية XOR على الكتلة الأولى من الرسالة الأصلية P1 مع شعاع التهيئة والذي هو عبارة عن بيانات عشوائية يجب أن تتغيرفي كل جلسة تشفير (IV) وتكون نفسها لدى من المرسل والمستقبل ومن ثم يتم تشفير الناتج مما ينتج الكتلة المشفرة الأولى C1.
- تطبق عملية XOR على الكتلة المشفرة Cn والكتلة Pn+1ويتم تشفير الناتج مما يعطي الكتلة المشفرة Cn+1.

يمكن تلخيص خطوات التشفير في هذا النمط كالاتي :

1. يتم تهيئة شعاع مكون من ثمانية بايتات بقيمة تختلف من stream لآخر

```
L' = R
R' = L(+)f(R,K)
```

2. نقوم بتشفير شعاع التهيئة الناتج لينتج لدينا مسجل إزاحة من ثمانية بايتات

$$K_n = KS(n, KEY)$$

3. نجري عملية XOR المتمثلة بالدالة (f)على ثمانية البتات الأولى من الرسالة الأصلية وثمانية البتات الأولى من اليسار من مسجل الإزاحة لينتج لدينا ثمانية البتات الأولى من النص المشفر.

$$L_n = R_{n-1}$$

$$R_n n = L_{n-1} (+) f(R_{n-1}, K_n)$$

4. يتم إزاحة مسجل الإزاحة إلى اليسار بمقدار ثمانية بتات ونقوم بوضع الخانات الثمانية الناتجة عن تشفير الخطوة السابقة في أقصى اليمين مسجل الإزاحة
5. يتم تشفير مسجل الإزاحة.
6. نجري عملية XOR على ثمانية البتات التالية من الرسالة الأصلية مع ثمانية البتات الأولى من اليسار من مسجل الإزاحة لينتج لدينا ثمانية البتات الثانية من النص المشفر.
7. يتم تكرار الخطوات من 4 إلى 6 حتى يُشّفر النص كاملاً.

ويتم فك التشفير في هذا النمط كالآتي:

1. يتم تهيئة شعاع مكون من ثمانية بايتات بقيمة مساوية للقيمة المستخدمة في التشفير
2. يتم تشفير شعاع التهيئة الناتج لينتج لدينا مسجل إزاحة من ثمانية بايتات.
3. نجري عملية XOR على ثمانية البتات الأولى من النص المشفر وثمانية البتات الأولى من اليسار من مسجل الإزاحة لينتج لدينا ثمانية البتات الأولى من النص الأصلي.
4. يتم ازاحة مسجل الإزاحة إلى اليسار بمقدار ثمانية بتات ونقوم بوضع الخانات الثمانية الناتجة عن فك التشفيرمن الخطوة السابقة (ثمانية البتات الأخيرة من النص الأصلي) في أقصى يمين مسجل الإزاحة
5. يتم تشفير مسجل الإزاحة.
6. نجري عملية XOR على ثمانية البتات التالية من النص المشفر مع ثمانية البتات الأولى من اليسار من مسجل الإزاحة لينتج لدينا ثمانية البتات الثانية من النص الأصلي.
7. يتم تكرار الخطوات من 4 إلى 6 حتى فك تشفير كامل النص.