وزارة التعليم العالي والبحث العلمي
جامعة ديالى
كلية العلوم
قسم الحاسوب

تصميم نموذج الاختبار الالكتروني امن باستخدام طريقة التشفير AES

للطالبة

ولاء طاهر لطيف

اشراف

م. م وسن سعد احمد

1441 A.H. **2020 A.D**

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

﴿ وَلَوْ أَنَّمَا فِي ٱلْأَرْضِ مِن شَجَرَةٍ أَقْلَٰمٌ وَٱلْبَحْرُ يَمُدُّهُۥ
مِنۢ بَعْدِهِۦ سَبْعَةُ أَبْحُرٍ مَّا نَفِدَتْ كَلِمَٰتُ ٱللَّهِ
إِنَّ ٱللَّهَ عَزِيزٌ حَكِيمٌ ﴿٢٧﴾ ﴾

الاهداء

في مثل هذه اللحظات يتوقف اليراع ليفكر قبل ان يخط الحروف ليجعلها في كلمات تتبعثر الاحرف وعبثا ان يحاول تجميعها في سطور كثيرة تمر في الخيال ولا يبقى لنا في نهاية المطاف الا قليلا من الذكريات وصور تجمعنا برفاق كانوا الى جانبنا فواجب علينا شكرهم ووداعهم ونحن نخطو خطواتنا الاولى في غمار الحياة ونخص بالجزيل الشكر والعرفان الى كل من اشعل شمعة في دروب عملنا والى من وقف على المنابر واعطى من حصيلة فكره لينير دربنا الى الاساتذة الكرام والى الاصدقاء الاعزاء .

شكر وتقدير

الحمد لله الذي انزل القران شفاءا ورحمة للمؤمنين والصلاة والسلام على من اعطي السبع المثاني والقران العظيم وعلى اله اجمعين الذين رفعوا بهمهم العالية اعلام الدين وعلى اصحابه الذين امنوا به وازروه ونصروه واتبعوا النور الذي انزل معه الذين ابلوا البلاء الحسن بنصرته واقامة دينه.

وبعد...

احمد الله والثناء عليه جلت قدرته على توفيقه باتمام هذا الجهد العلمي المتواضع فيطيب لي ويبهج نفسي ان اتوجه بالشكر والامتنان الى الاهل الذين ساندونا وكانوا نعم العون في كل الظروف والشكر والتقدير للاساتذة جميعا.

ملخص البحث

نموذج الاختبار الالكتروني بطريقة التشفيرتم إنشاء هذا النظام لغرض اضافة طبقة حماية لنموذج الاختبار الالكتروني وذلك من خلال عملية التشفير وقد تمت عملية التشفير باستخدام خوارزمية AES وهي من الخوارزميات الحديثة والقوية جدا فيكاد من الصعب فك تشفير الرسالة المشفرة الناتجة من هذه الخوارزمية بدون المفتاح.

تهدف هذه الدراسة إلى تطوير العمل ومواكبة التطورات العصرية وزيادة طبقة الحماية لنموذج الاسئلة وسهولة استرداد الاسئلة بطريقة سريعة جدا , تم انشاء هذا البرنامج باستخدام لغة البرمجة فيجوال بيسك دوت نت vb.net وتم ربطها بقاعدة بيانات من نوع sql وتمت عملية التصميم باستخدام html في بيئة asp .

جدول المحتويات(الفهرس)

الفصل الاول

مقدمة

1.1مقدمة

إن نظام نموذج الاختبار الالكتروني بطريقة التشفير هو موقع الكتروني ، مصمم لدعم وتحسين واضافة طبقة حماية للاسئلة بطريقة الكترونية.

تم انشاءه لاغراض مهمة جدا وعديدة نذكر اهمها الحماية فمن خلال عملية التشفير القوية تم اضافة طبقة حماية قوية جدا لنموذج الاختبار الالكتروني ولانه نظام الكتروني فتكون البيانات مخزونة ضمن قاعدة بيانات من نوع sql يمكن استدعاء البيانات منها بسهولة تامة.

علم التشفير هو دراسة وممارسة بعض التقنيات لتأمين عملية التواصل بوجود أشخاص أخرين والذين يسمون أعداء. بصوره عامة، علم التشفير يهتم بإنشاء وتحليل بعض الأنظمة التي تمنع الأعداء أو العامة من قراءة الرسائل الخاصة. أي بوسائل تحويل البيانات (مثل الكتابة) من شكلها الطبيعي المفهوم لأي شخص إلى شكل غير مفهوم بحيث يتعذّر على من لا يملك معرفة سرية محددة معرفة فحواها. فهنالك مجالات عديدة يتم استخدام عملية التشفير فيها مثال على ذلك في الرياضيات والحاسوب ولامراسلات في الحروب حيث كانت اول عملية تشفير بسيطة تدعى قيصر.ولكن مع تقدم التكنلوجيا ومواكبة التطورات الحديثة فاصبحت تلك الخوارزميات كقيصر مكشوفة فيلجأ الكثيرون الى مواكبة التطورات وذلك لاجل الحصول على اعلى حماية ممكنة. ففي بحثنا قمنا باستخدام خوارزمية AES فهي خوارزمية حديثة وقوية جدا كما سنذكر تفاصيلها لاحقا.

1.2 المشاكل التي سيقوم النظام بحلها

بسبب ضعف الحماية الالكترونية وعدم وجود امان للبيانات المخزنة الكترونيا ، واجهنا الكثير من المشاكل التي تشمل:

1. حل مشكلة الحماية بالدرجة الاساس فيقوم نظامنا باضافة طبقة حماية قوية جدا باستخدام احدى الطرق الحديثة للتشفير. واضافة الى الحماية فيقوم نظامنا بعملية التنظيم من خلال اعطاء ID لكل صاحب مادة يختلق عن ID للشخص الاخر وكذلك لكل شخص يقم بعمل اسئلة للاختبار يجب ان يكون لديه مفتاح key لايعرفه احدا سواه.

1.3الاهداف

تهدف هذه الدراسة إلى تطوير العمل واضافة طبقة حماية قوية جدا إلى العمل الإلكتروني ومواكبة التطورات والدقة في العمل ومنع المتطفلين من الاطلاع على الاسئلة الخاصة بنموذج الاختبار الالكتروني بطريقة تشفير حديثة بواسطة خوارزمية AES .

1.4 مجال البحث

يركز العمل البحثي على **الحماية** بشكل اساسي من خلال اضافة طبقة حماية الى نموذج الاختبار الالكتروني بطريقة التشفير وسنقوم بتوضيح كيف تتم عملية التشفير وكيف يتم فك التشفير وما هي عملية التشفير ودراسة كافة الادوات التي تم استخدامها في بحثنا كما سنوضحها جميعا لاحقا.

1.5 خلفية العمل

تم استخدام لغة البرمجة فجوال بيسك دوت نت vb.net وتم استخدام قاعدة بيانات من نوع SQL،اخيرا تم استخدام برنامج الفجول ستوديو الاصدار 2012 للعمل.

الفصل الثاني

الجانب النظري

2.1 مقدمة

عُرف علم التشفير أو التعمية منذ القدم، حيث استخدم في المجال الحربي والعسكري. فقد ذكر أن أول من قام بعملية التشفير للتراسل بين قطاعات الجيش هم الفراعنة. وكذلك ذكر أن العرب لهم محاولات قديمة في مجال التشفير. و استخدم الصينيون طرق عديدة في علم التشفير والتعمية لنقل الرسائل أثناء الحروب. فقد كان قصدهم من استخدام التشفير هو إخفاء الشكل الحقيقي للرسائل حتى لو سقطت في يد العدو فإنه تصعب عليه فهمها. وأفضل طريقة استخدمت في القدم هي طريقة القصير جوليوس وهو أحد قياصرة الروم. أما في عصرنا الحالي فقد باتت الحاجة ملحة لاستخدام هذا العلم "التشفير" وذلك لإرتبط العالم ببعضه عبر شبكات مفتوحة. وحيث يتم استخدام هذه الشبكات في نقل المعلومات إلكترونياً سواءً بين الأشخاص العاديين أو بين المنظمات الخاصة والعامة، عسكرية كانت أم مدنية. فلابد من طرق تحفظ سرية المعلومات. فقد بذلت الجهود الكبيرة من جميع أنحاء العالم لإيجاد الطرق المثلى التي يمكن من خلالها تبادل البيانات مع عدم إمكانية كشف هذه البيانات[7].

استخدم التشفير منذ أقدم العصور في المراسلات الحربية وكذلك في الدبلوماسية والتجسس في شكليهما المبكرين. يعتبر العلماء المسلمون والعرب أول من اكتشف طرق استخراج المعمَّى وكتبها وتدوينها .تقدمهم في علم الرياضيات أعطاهم الأدوات المساعدة الأزمة لتقدم علم التعمية، من أشهرهم يعقوب بن إسحاق الكندي صاحب كتاب علم استخراج المعمَّى وابن وَحشِيَّة النبطي صاحب كتاب شوق المستهام في معرفة رموز الأقلام، المؤلف الذي كشف اللثام عن رموز الهيروغليفية قبل عشرة قرون من كشف شامبليون لها وكذلك اشتهر ابن دريهم الذي كان لا يشق له غبار في فك التشفير فكان تعطى له الرسالة معماة فما هي إلا أن يراها حتى يحولها في الحين إلى العربية ويقرئها وله قصيدة طويلة يشرح فيها مختلف الطرق في تعمية النصوص وكان يحسن قراءة الهيروغليفية من أمثلة استخدام التعمية قديما هو ما ينسب إلى يوليوس قيصر من استعمال ما صار يعرف الآن بخوارزمية ROT13 لتعمية الرسائل المكتوبة باللاتينية التي يتبادلها مع قواده العسكريين، وهو أسلوب تعمية يُستبدل فيه كل حرف بالحرف الذي يليه بثلاثة عشر موقعا في ترتيب الأبجدية اللاتينية، مع افتراض أن آخر حرف في الأبجدية يسبق الأول في حلقة متصلة .ومازال العمل والبحث في مجال علم التشفير مستمراً وذلك بسبب التطور السريع للكمبيوتر والنمو الكبير للشبكات وبخاصة الشبكة العالمية الإنترنت.[7]

2.2 التشفير

التشفير (بالإنجليزية: Encryption) يتناولها علم المعلومات (التي تكون بشكل نص بسيط عند التخزين على وسائط التخزين المختلفة أو عند نقلها على شبكات نص مجرد (plaintext) بحيث تصبح غير مقروءة لأحد باستثناء من يملك معرفة خاصة أو مفتاح خاص لإعادة تحويل النص المشفر إلى نص مقروء. عملية الفك هذه تتم عن طريق ما يدعى مفتاح التشفير كما موضح في الشكل رقم 1.1 كيف تتم عملية التشفير . نتيجة عملية التشفير تصبح المعلومات مشفرة وغير متاحة لأي أحد لأغراض سرية عسكرية أو سياسية أو أمنية كما نلاحظ في الشكل (1.1) كيف تجري عملية التشفير. [6]

شكل 1.1 كيف تتم عملية التشفير (Encryption)

بمجرد إرسال حزم البيانات من المكالمات الصوتية والدردشة و البريد الإلكتروني أو حتى استخدام بطاقة الائتمان في الإنترنت ربما جميع هذه البيانات قد تتعرض للتنصت أو حتى السرقة، لذا وجب علينا استخدام التشفير أثناء القيام بهكذا عمليات حساسة.

يطلق على التشفير باللغة الإنجليزية بالـ Encryption أو الـ Ciphering, حيث أن الكلمة الأولى مأخوذة Cryptography وهي تعني الكتابة السرية أما الثانية فهي مأخوذة من كلمة Cipher والتي يقال بأنها تعود الى الكلمة العربية "تصفير" أو جعل القيمة مساوية لـ "صفر" أي بلا قيمة أو بلا معنى [8] .

2.2.1 مصطلحات ومفاهيم علم التشفير

A. علم التشفير (Cryptography) هي كلمه تعني بالإغريقية كلمتان

Cryptography → krypton + graphy

(اخفاء) + (الكتابة)

علم التشفير هو من العلوم التي تستخدم الحساب للتشفير (encrypt) وفك التشفير (decrypt) بالنسبة للبيانات وبالتالي تتيح تخزين وارسال البيانات بطريقه سريه بحيث لا يستطيع احد قراءتها ماعدا المصرح.[8]

B. التشفير (Encryption):

هي عملية تحويل النص او البيانات الى شكل غير مفهوم بغرض اخفاء هذه البيانات او هو عملية تحويل نص صريح(plain text) الى نص مشفر (cipher text) غير صريح بواسطة مفتاح سري (secret key)

او عملية ارجاع النص المشفر (cipher text) الى نص صريح (plain text) تعرف بعملية فك التشفير (decryption).[8]

C. المفتاح (key):

وهو عباره عن كلمه السر المستخدمة في خوارزمية التشفير او فك التشفير ويعتبر من اهم الاشياء التي يجب اخفائها حيث انه يعتبر من الاشياء السرية التي لا يعرفها الا المخول لهم.[8]

D. الخوارزمية(Algorithm):

هي عباره عن الخطوات اللازمة لحل مسألة ما، وقد تكتب هذه الخوارزمية باللغة العربية او الإنجليزية وقد يعبر عنها برسم اشكال هندسيه معينه.

النص الاصلي قبل عملية التشفير--> plaintext

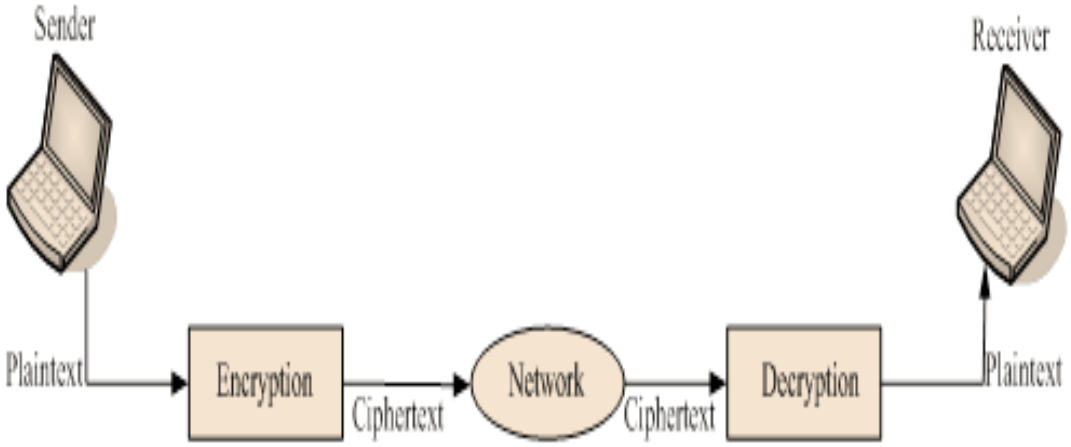
النص المشفر بعد عملية التشفير--> ciphertext

تحويل النص العادي الى نص مشفر --> encryption

فك التشفير أي تحويل النص المشفر الى نص عادي <-- decryption [8]

E. مثال بسيط عن الية التشفير (Basic Terminology)

كما نلاحظ العملية في الشكل 1.2



شكل 1.2 عملية التشفير (Encryption) وفك التشفير (Decryption)

F. فن كسر الشفرة (cryptanalysis)

هو العلم الذي يستخدم لكسر الخوارزميات وإيجاد نقط الضعف بها. أي إنه العلم الذي يستطيع تحويل الكتابة المكتوبة بطريقة سرية تستخدم التشفير وتحويل النص المشفر إلى نص غير مشفر، والتشفير وتحليل الشفرات هما جانبان من عملية التشفير. فن كسر الشفرة يقوم باسترجاع النص الصريح(plain text) من النص المشفر (cipher text) بدون معلومية المفتاح key.[8]

2.2.2 أهداف التشفير

1. السرية أو الخصوصية (Confidentiality) : هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح لهم الإطلاع عليها.

2. تكامل البيانات (Integrity) من قبل الأشخاص الغير مصرح لهم بذلك.

3. إثبات الهوية (Authentication) : وهي خدمة تستخدم لإثبات هوية التعامل مع البيانات (المصرح لهم).[5]

2.2.3 الاستعمالات الحديثة للتشفير

في العصر الحديث، تعد آلة إنجما التي استخدمها الجيش الألماني في الحرب العالمية الثانية، أبرز مثال على استخدام التعمية لتحقيق تفوق على العدو في مجال الاتصالات، وكانت الأبحاث التي جرت بشكل منفصل في كل من المؤسستين العسكريتين الأمريكية والبريطانية في سبعينيات القرن العشرين فتحا جديدا فيما صار يعرف الآن بتقنيات التعمية القوية المعتمدة على الحوسبة، وارتبطت التعمية بعلوم الجبر ونظرية الأعداد ونظرية التعقيد ونظرية المعلومات.
توسع نطاق تطبيقات التعمية كثيرا في العصر الحديث بعد تطور الاتصالات وحدوث ثورة الاتصالات بما تتطلبه أحيانا من استيثاق وحاجة إلى ضمان عدم التصنت ومنع التجسس والقرصنة الإلكترونيين وتأمين سبل التجارة الإلكترونية [5] .

2.3 خوارزمية معيار التشفير المتقدم AES (Advanced Encryption Standard)

و هو اشهر انواع التشفير المتناظر Symmetric Cryptography

ايضا يعرف بأسم Rijndael و هى جمع بين اسم مخترعيه Joan Daemen و Vincent Rijmen ، و هو احد اشهر نظم الخوارزميات عالميا و اوسعهم انتشارا [9].

إن خوارزمية التشفير المتماثل الأكثر شيوعًا والمستخدمة على نطاق واسع والتي من المحتمل أن تتم مواجهتها في الوقت الحاضر هي معيار التشفير المتقدم (AES). تم العثور عليه على الأقل ست مرات أسرع من Triple DES.

كان هناك حاجة لاستبدال DES لأن حجمه الرئيسي كان صغيرًا جدًا. مع زيادة قوة الحوسبة ، اعتبرت عرضة لهجوم بحث مفتاح شامل. تم تصميم Triple DES للتغلب على هذا العيب ولكن مشكلتها الاساسية هي البطئ.

تشفير فيستيل (feistel cipher):

اقترح فيستيل أنه يمكن تطوير تشفير تبديل الحروف البسيط عن طريق تطبيق مفهوم ضرب التشفير، حيث يمكن تطبيق تشفيرين متتالين أو أكثر بحيث تكون النتيجة النهائية، من وجهة نظر التعمية، أقوى من أي من مركباتها.[12]

من الجدير التعليق على الحقيقة التالية: معظم بنى أنظمة التشفير الكتلي المتناظر الهامة والمستخدمة في هذه الأيام مبنية على أساس بنية نظام تشفير فيستيل، الذي يعود لحوالي ربع قرن ماضي والمبني على أساس اقتراح شينون عام 1945.[12]

ميزات AES كالتالي :[11]

- تشفير كتلة متماثل (symmetric block cipher) و مفتاح متماثل (Symmetric key)
- بيانات 128 بت ، مفاتيح 256/192/128/64/18 بت (وهناك ايضا مفاتيح ذات 512 بيت وذلك في الحالات السرية).
- أقوى وأسرع من Triple-DES

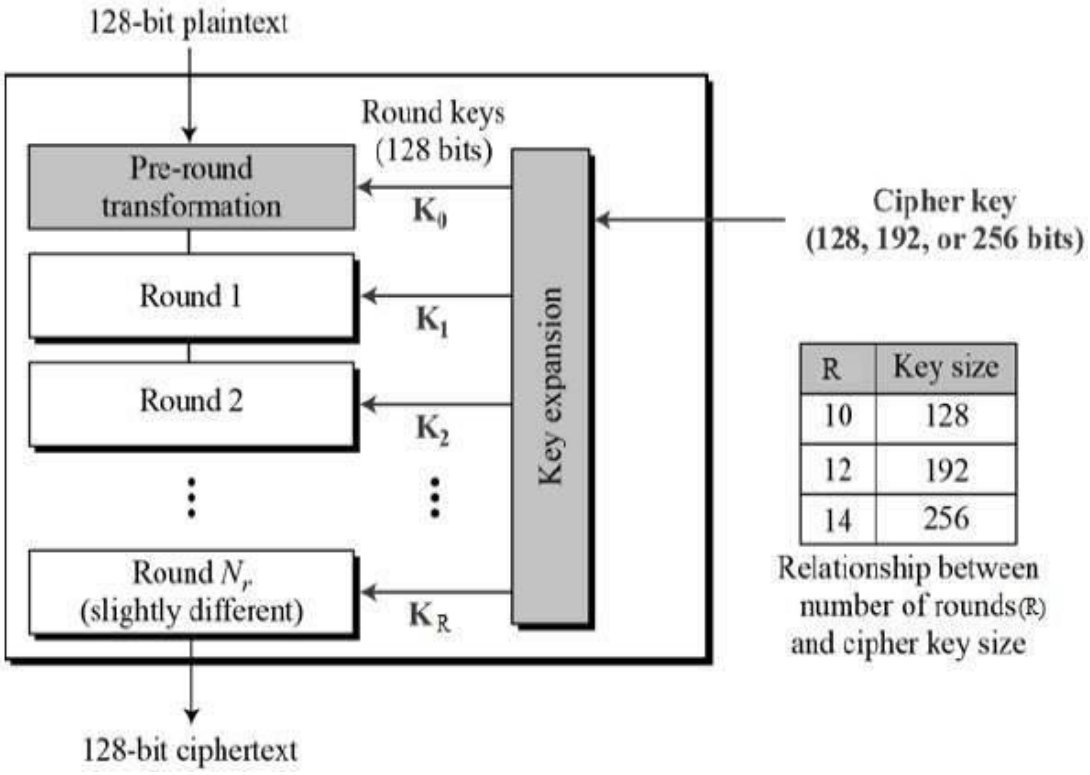
تشغيل AES :

AES هو تكراري عوضا عن تشفير Feistel. وهو يقوم على "مبدأ الاستبدال والتبديل". وهو يتألف من سلسلة من العمليات المرتبطة ، بعضها يتضمن استبدال المدخلات بمخرجات محددة (بدائل)(substitutions) والبعض الآخر ينطوي على خلط القطع حول (التباديل) (permutations).[11]

ومن المثير للاهتمام ، تقوم AES بإجراء جميع حساباتها على وحدات البايت بدلاً من البتات. وبالتالي ، تعامل AES 128 بت من كتلة نص الاصلي على أنها 16 بايت. يتم ترتيب هذه 16 بايت في أربعة أعمدة وأربعة صفوف للمعالجة كمصفوفة.

على عكس DES ، فإن عدد الجولات في AES متغير ويعتمد على طول المفتاح. يستخدم AES 10 جولات لمفاتيح 128 بت ، و 12 جولة لمفاتيح 192 بت و 14 جولة لمفاتيح 256 بت. تستخدم كل جولة من هذه الجولات مفتاحًا دائريًا مختلفًا من 128 بتًا ، يتم حسابه من مفتاح AES الأصلي.

يتم عرض مخطط هيكل AES في الرسم التوضيحي التالي

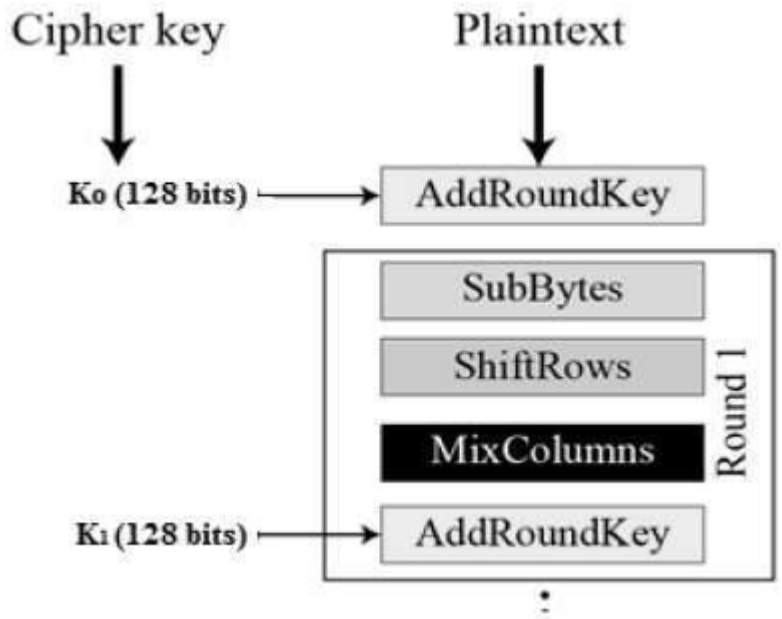


R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

عملية التشفير

نقتصر هنا على وصف جولة نموذجية من تشفير AES. تتكون كل جولة من أربع عمليات فرعية. يتم تصوير عملية الجولة الأولى كما موضح ادناه :[11]



استبدال البايت (SubBytes)

يتم استبدال 16 بايت الإدخال عن طريق البحث عن جدول ثابت (S-box) في التصميم. والنتيجة هي مصفوفة من أربعة صفوف وأربعة أعمدة.[11]

Shiftrows

يتم تحويل كل من الصفوف الأربعة من المصفوفة إلى اليسار. يتم إعادة إدخال أي إدخالات "تسقط" على الجانب الأيمن من الصف. يتم إجراء عملية التشفيت (التحول) على النحو التالي -

1. لا يتم تغيير الصف الأول.
2. يتم تحويل الصف الثاني بمقدار (بايت) إلى اليسار.
3. يتم نقل الصف الثالث موقعين إلى اليسار.
4. يتم نقل الصف الرابع ثلاثة مواقع إلى اليسار.
5. والنتيجة هي مصفوفة جديدة تتكون من نفس 16 بايت ولكنها تحولت (تم تشفيت بياناتها) فيما يتعلق ببعضها البعض.[11]

MixColumns

يتم تحويل كل عمود من أربعة بايتات الآن باستخدام دالة رياضية خاصة. تأخذ هذه الوظيفة كمدخلات أربعة بايتات من عمود واحد وتخرج أربعة بايتات جديدة تمامًا ، والتي تحل محل

العمود الأصلي. والنتيجة هي مصفوفة جديدة أخرى تتكون من 16 بايت جديدة. وتجدر الإشارة إلى أن هذه الخطوة لم يتم تنفيذها في الجولة الأخيرة.[11]

Addroundkey

تكون 16 بايت من المصفوفة بحجم 128 بت و XORed إلى 128 بت من المفتاح الدائري (roundkey). إذا كانت هذه هي الجولة الأخيرة ، فإن الناتج هو نص التشفير. خلاف ذلك ، يتم تفسير 128 بت الناتجة على أنها 16 بايت ونبدأ جولة أخرى مماثلة.[11]

عملية فك التشفير

تشبه عملية فك تشفير نص تشفير AES عملية التشفير بالترتيب العكسي. تتكون كل جولة من العمليات الأربع التي أجريت بترتيب عكسي :[11]

1. Add round key أضف مفتاح دائري
2. Mix columns اخلط الأعمدة
3. Shift rows تغيير الصفوف
4. Byte substitution استبدال البايت

نظرًا لأن العمليات الفرعية في كل جولة تتم بطريقة عكسية ، على عكس Feistel Cipher ، يجب تنفيذ خوارزميات التشفير وفك التشفير بشكل منفصل ، على الرغم من أنها مرتبطة ارتباطًا وثيقًا.

تحليل AES

في التشفير الحالي ، يتم اعتماد AES على نطاق واسع ودعمه في كل من الأجهزة والبرامج. حتى الآن ، لم يتم اكتشاف أي هجمات تشفير عملية ضد AES. بالإضافة إلى ذلك ، تتمتع AES بمرونة مدمجة في طول المفتاح ، مما يسمح بدرجة من "التدقيق في المستقبل" مقابل التقدم في القدرة على إجراء عمليات بحث شاملة للمفاتيح.

ومع ذلك ، تمامًا كما هو الحال في DES ، لا يتم ضمان أمان AES إلا إذا تم تنفيذه بشكل صحيح وتم توظيف إدارة رئيسية جيدة.

2.3.1 استخدامات AES

بما أنَّ AES هو خوارزمية تشفير لذا فان له كثير من الاستخدامات التي تضم حماية المستخدم عبر الانترنت لتصل إلى حماية وضمان البيانات في العمل الالكتروني والبنوك والمعامل كما أن ل AES-استخدامات في المجالات العسكرية، ان ما ضمن ان AES نافع في كل هذه التطبيقات هو عدم وجود طريقة فعالة لكسره، كما أن بعض أشهر البرامج والبروتوكلات تعتمد على مقاومة AES للهجمات الإلكترونية ومنها:

- يستخدم في عملية تشفير البيانات النصية والانواع الاخرى للبيانات كالصوت والفيديو وغيرها.
- يستخدم AES في برامج (WINZIP) في حالة ان المُستخدم طلب تشفير البيانات بعد ضغطها.
- يُستخدم في برتوكول , TLS وهو برتوكول لإنشاء اتصال آمن.
- له كذلك استخدام في برتوكول IPsec وهو برتوكول لضمان الامان في اتصالات التي تعمل بواسطة IP عبر الانترنت [9] .

2.4 نبذة مختصرة عن الفجوال بيسك دوت نت VB.NET

لقد ظهرت لغة Visual Basic لأول مرة عام 1991، ومنذ ذلك الحين وحتى الآن تجري تعديلات على هذه اللغة وذلك بظهور إصدارات مختلفة، وآخر إصدار هو (فيجوال بيسك.نت 2017) اما الإصدار الذي سنعتمده في مشروعنا هو(فيجوال بيسك.نت 2012) ولا يوجد فرق كبير بينهما اما لماذا اخترنا اصدار 2012 نضرا لسرعته ويمكن تنصيبه على اغلب الحاسبات اما الاصدار 2017 فيحتاج مواصفات عالية جدا لتنصيبه.[1]

تعتبر لغة Visual Basicمن لغات برمجة ويندوز، فهي تستخدم لتصميم برامج تعمل تحت نظام التشغيل Windows وبالتالي يجب على من يريد تعلم هذه اللغة أن يكون ملماً بطريقة

التعامل مع نظام التشغيل ويندوز ، ويفضل أن يكون على دراية كافية بلغة البرمجة Basic (فالمتحولات وبنى التحكم و الملفات في Visual Basic تشابه وبشكل كبير مثيلاتها في Basic). [1]

إن Visual Basic من اللغات المسيرة بالأحداث شأنها في ذلك شأن معظم لغات برمجة ويندوز(Delphi و Visual C++)، واللغة المسيرة بالأحداث هي اللغة التي تعتمد فكرة تجزئة البرنامج إلى برامج جزئية تنفذ عند وقوع حدث ما كالضغط فوق أحد الأزرار أو تحريك مؤشر الفأرة فوق النافذة أو مرور فترة من الزمن . وبالتالي يجب عند البدء بالبرنامج تحديد الأحداث وكيفية الاستجابة لكل منه (إذا ضُغط زر كذا أفعل كذا وإذا تحرك مؤشر الفأرة فوق النافذة افعل كذا ....) . [1]

فهي تمكن المبرمج من تطوير وإنتاج التطبيقات المختلفة في وقت قصير، وبكفاءة عمل عالية ،وتندرج لغة Visual Basic تحت قائمة لغات الأحداث المحركة Object Oriented Languages ، وهذا يعني أن ما يحدثة المستخدم من أفعال مثل ضغط أحدالمفاتيح أو نقر زر الماوس يؤدي إلي تنفيذ الدوال المخصصة لذلك وبذلك يكون مستخدم البرنامج هو المسؤل عن ما يحدث ومتى يحدث ؟[3]

ويختلف ذلك كلياً عن اللغات التقليدية والتي لم تُتِحْ للمستخدم سوى رد الفعل التنفيذى فقط للكود الذي يتم كتابته. وتتكون البرامج من عدة شاشات وكل شاشة تحفل بالعديد من عناصر التحكم ، ومهمة المبرمج هنا هي تحديد ردود أفعال الشاشات والعناصر عن حدوث أحداث معينة بواسطة المستخدم ، وكل عنصر أو شاشة لها مجموعة من الخواص كالأبعاد والألون والبيانات المخزنة بها فتكون فلسفة البيسك المرئي Visual Basic هي التحاور بين العناصر المختلفة وتغيير صفاتها وبياناتها عندما يُحْدِثْ المستخدم بعض الأفعال.[3]

وأخيراً نقول : إن البرمجة بلغة Visual Basic هي برمجة ممتعة حقاً فمن خلال وقت قصير جداً نستطيع إنشاء برامج جيدة ومفيدة، وخصوصاً أن لغة Visual Basic سهلة التعلم مقارنةً مع لغات مثل C++,Visual أو Java .[1]

تطورت لغة الفيجوال بيسك بشكل كبير حتى أصبحت تحتوي على أدوات معقدة ولكن ليس بالضرورة معرفة جميع الأدوات التي تأتي مع فيجوال بيسك لتطوير تطبيق ما ... ولكن يكتفي المبرمج بمعرفة الأدوات التي يحتاج لها فقط ولكن هناك بعض الأساسيات التي يجب معرفتها وإتقانها من قبل المبرمجين لكي يصبحوا مطوري برامج على الفيجوال بيسك.[3]

يوجد العديد من العيوب في هذه البرمجيّة بالرغم من وجود العديد من الأفراد يستخدمونها، كوجود العديد من الإصدارات الغير مجانيّة والتي تحتاج إلى دفع عن طريق فيزا إلكترونيّة، كما أنّها لا تطرح كافة الأشكال، كما أنّ المترجم غير دقيق وهذا قد يساهم في ظهور الأخطاء أثناء عمليّة التنفيذ[2].

لماذا Visual Basic ؟

حينما أصدرت (ميكروسوفت) أوّل نسخة من لغة Visual Basic عامَ 1991، لم يكن في حسبانِها أنّها ستكتسبُ كلّ هذه الشهرةِ وستحقّق كلّ هذه الشعبيّة ! [4]

إنّ لغة BASICالقديمة تُعَدّ من أسهل لغاتِ البرمجة، ولكّنها لم تستطع الصمود في المنافسة مع لغاتِ البرمجة الأخرى بسبب قدراتِها المحدودة.

كانَ ذلك كذلك، حتّى أصدرت (ميكروسوفت) إصدارات VB المتتابعة، لتنتقل لغة BASIC من قِفار الدوس المجدبة إلى مراعي الويندوز الخصبة، مانحةً للمبرمج القدرة على إنشاءِ برامج ذات واجهة مرئيّة، بأسهلِ طريقةٍ وفي أسرعِ وقت.

ومنذئذٍ ولغة VB تتصدّر قائمة مبيعات لغات البرمجة، لتدخلَ في بناءِ التطبيقاتِ التجاريّة وتطبيقاتِ قواعد البياناتِ البسيطة، وبرامج الوسائط المتعدّدة Multimediaوالكثير من الألعاب.

ولكن للأسف.. دائما وأبدا كانت VB أدنى من باقي لغاتِ البرمجة، فتطبيقاتُها أبطأ نسبيّا وأكبر حجما، وتعاني من بعض أوجهِ القصورِ في الأداء.

ولقد استمرّت (مايكروسوفت (Microsoftفي تطوير VB عبرَ ستّ إصداراتٍ مختلفة، وفي كلّ إصدارٍ جديدٍ كانت تعالجُ بعضَ المشاكلِ القديمةِ وتضيفُ المزيدَ من القدرات، لتضيقَ الفجوةُ شيئًا فشيئا بين VB وباقي لغات البرمجة.

ثمّ أخيرا أقدمت (ميكروسوفت) على الخطوة التي طال انتظارها.. أصدرت نسخة جديدةً بكلّ المقاييس منVB ، بنتها من جذورها From scratch لتجعلها ندّا حقيقيّا لـVC++ ، بحيثُ يمكنك أن تقولَ بثقة: إنّ العصرَ الذهبيَّ لـ VC++ آخذٌ في الأفول بلا رجعة، حيثُ سينحصرُ استخدامها في تصميم المحرّكات Engines التي تدخل في بناء تطبيقات أخرى، أو في كتابة الكود الذي يتيح للكمبيوتر التحكمّ في آلات أخرى، ولكنّ استخدامها سيتراجع بلا شكّ في تطبيقات الإنترنت والتطبيقات التجاريّة وتطبيقات قواعد البيانات والوسائط المتعدّدة ومعظم الألعاب وما شابه، نظرًا لصعوبتِها وتعقيدِها وطول الوقت اللازم للبرمجة بها!

وأعتقدُ أنّ هذا هو السبب الذي دفع (ميكروسوفت) لإصدار اللغة الجديدةC# ، التي تُعتبر توأما لـ VBإلا إنّها تستخدم قواعد C ++ في كتابة الأوامر، ممّا يشكّلُ لمبرمجي VC++ إغراءً

تصعبُ مقاومته للانتقالِ إليها.

ولكن مهما كانت سهولةC# ، فإنّ VB يصرعُها في هذا المضمار، فهو أقربُ ما يكونُ للّغةِ الإنجليزيّة العاديّة، ولا يحتوي على الرموزِ الكثيرةِ المملّة التي تملأC++ ، مثل ؛ ، ++ ، == ، ||.... إلى آخر هذه الرموزِ التي تجعلُ احتمالاتِ الخطإ عند كتابةِ الكودِ أعلى، وتجعلُ البرنامجَ أصعبَ فهمًا وأقلَّ ألفةً عندَ قراءته.

مرحى لكلّ مبرمجي ..VB لقد صاروا على قمّة برمجة السوق!!

2.5 لغة HTML

لغة ترميز النص التشعبي (Hypertext Markup Language) اختصار إتش تي إم إل HTML)، هي لغة ترميز تستخدم في إنشاء وتصميم صفحات ومواقع الويب، وتعتبر هذه اللّغة من أقدم اللّغات وأوسعها استخداما في تصميم صفحات الويب. HTML هيكل صفحة الويب وتعطي متصفّح الإنترنت وصفا لكيفيّة عرضه لمحتوياتها، فهي تعلمه بأنّ هذا عنوان رئيسي وتلك فقرة وغير ذلك الكثير. وتستخدم الـ HTML ما يعرف بالوسوم "tags" لإصدار التعليمات إلى المتصفّح، هذه الوسوم توضع بين علامتي أكبر من "<" وأصغر من ">" الّتي تنقسم إلى نوعين:[13]

1. وسم البداية كـ <html> , , <h1> , <body>
2. وسم النهاية كـ </html> , , </h1> , </body>

بتجميع وسم البداية و وسم النهاية نحصل على عنصر HTML .

تبدأ أكواد HTML بالوسم <html>، وتنتهي بالوسم<html/>. يقوم متصفح الوب بترجمة السطور البرمجيّة بلغة HTML إلى محتوى مرئي سهل القراءة لزوار الموقع.

عرفت لعدم حساسيتها لحالة الأحرف أو لترتيب بعض الخصائص؛ لكلّ عنصر HTML خصائص تتحكّم في كيفيّة ظهوره. وذلك لكي تكون عمليّة تصميم المواقع عمليّة سهلة ولينة وبدون أي تعقيدات.HTML من اللّغات المدعومة بمعايير قياسيّة محددّه يفضّل الالتزام بها من قبل W3C فالالتزام بمعايير الـ HTML أثناء تصميم المواقع يمنح الصفحة قابليّة أكثر للعرض والاستخدام على أنواع وإصدارات مختلفة من المتصفحات. من ناحية أخرى فإن HTML مركبة بشكل نحوي يدعىDOM ؛ الّذي يحدّد معيارا للوصول والتلاعب HTML ، عمليّة تصميم المواقع مع DOM تجعل صفحة الموقع تظهر وكأنّها شجرة من الرسوم .

تاريخها:

في عام 1980، قام الفيزيائي Tim Berners-Lee والذي كان عاملا في المؤسسة الأوروبية للأبحاث النووية سيرن باقتراح واعداد نموذج بدئي لنظام يمكن باحثي سيرن من استخدام ومشاركة المستندات. وفي عام 1989 قام بكتابة مذكرة يقترح فيها نظام نص فائق hypertext مبني على الإنترنت، وقام بوصف لغة HTML وبكتابة برامج المزود والمتصفح في أواخر عام 1990.

كان أول وصف للجمهور من الاتش تي ام ال وثيقة تسمى علامات الاتش تي ام ال ذكر لأول مرة على شبكة الانترنيت عن طريق بيرنرز لي في أواخر عام 1991. فهو يصف 18 من العناصر الأولى التي تتألف منها ، نسبيا التصميم بسيط في الاتش تي ام ال بأستثناء علامة الارتباط التشعبي ،هذه تأثرت بقوة في (الاس جي ام ال كويد) ،اسست ال (الاس جي ام ال) على شكل وثائق في منزل سيرن . أحد عشر من هذه العناصر لا تزال موجودة في الاتش تي ام ال .

لغة ترميز النص التشعبي هي لغة العلامات التي تستخدم متصفحات الويب لتفسير وتأليف النص والصور وغيرها من المواد في صفحات الويب المرئية أو المسموعة. يتم تعريف وترميز الخصائص الافتراضية لكل بند من الاتش تي ام ال في المتصفح ،وهذه الخصائص يمكن تغيرها او تحسينها بواسطة استخدام مصمم صفحة ويب اضافية من الاسي اس اس . تم العثور على العديد من عناصر النص في عام 1988 (اي اس او) تقرير التقنية (تي ار 9537) تقنيات لاستخدام (الاس جي ام ال) الذي يغطي بدوره ملامح اللغات تنسيق النص في وقت مبكر مثل تلك المستخدمة من قبل الأمر الجريان السطحي وضعت في s1960 في وقت مبكر

ل CTSS (التوقيت متوافق نظام تقاسم) نظام التشغيل: وقد استمدت هذه الأوامر التنسيق من الأوامر المستخدمة من قبل عمال التجميع على تنسيق المستندات يدويا . ومع ذلك، يستند مفهوم SGML من معمم العلامات على عناصر (نطاقات متداخلة مع سمات المشروح) بدلا من مجرد آثار الطباعة ، مع أيضا الفصل بين هيكل و العلامات ، وقد تم HTML انتقلت تدريجيا في هذا الاتجاه مع CSS . بيرنرز لي يعتبر تطبيق HTML من SGML تم تعريفه رسميا على هذا النحو من قبل فريق عمل هندسة الإنترنت (IETF) مع منتصف عام 1993 نشر أول اقتراح ل مواصفات HTML : " لغة توصيف النص التشعبي (HTML) " إنترنت مشروع من قبل بيرنرز لي و دان كونولي ، الذي تضمنت نوع الوثيقة SGML تعريف لتعريف النحوي .[13]

2.6 قواعد البيانات

بطريقة بسيطة مجرّدة من مفاهيم التقنية، قاعدة البيانات هي مكان لحفظ بيانات معينة على نحو مستمر بهدف الرجوع إليها وقت الحاجة، فدفتر أرقام الهواتف الذي كنا نستعمله في الماضي يُعدّ قاعدة بيانات؛ والكم الهائل من الفواتير المحاسبية الورقية المحفوظة في خزانات الأقسام المالية في الشركات قديماً، أيضاً هو قاعدة بيانات. وقِس على ذلك العديد من الأمثلة الواقعية والملموسة. [10]

نستنبطُ من هذا التعريف البسيط وجود خاصية هامة لقاعدة البيانات، ألا وهي "الاستمرارية" أو "الدوام" في حفظ البيانات.

في الجانب التقني والبرمجي، فإن قاعدة البيانات Database هي عبارة عن مستودع تُحفظ البيانات فيه داخل جهاز الحاسوب أو الخادوم، ويتمتع هذا المستودع بخاصية الاستمرارية في حفظ البيانات. ونعني بخاصية الاستمرارية هنا أنه في حال إطفاء جهاز الحاسوب أو إعادة تشغيله أو انقطاع التواصل معه، فإن قاعدة البيانات وما تحتويه من بيانات تبقى موجودة ومحفوظة دون أي خلل.

هناك عدة انواع لقواعد البيانات منها:

- قواعد بيانات مايكروسوفتMicrosoft SQL Server

- قواعد بيانات MySQL
- قواعد بيانات أوراكل Oracle
- قواعد بيانات PostgreSQL

ونحن سنركز في بحثنا على النوع الاول فقط.

2.6.1 قواعد بيانات مايكروسوفتMicrosoft SQL Server

من قواعد البيانات الشهيرة، والذي تأتي أيضا بأكثر من إصدار، لتلبي احتياجات المستخدمين المختلفة وبيئات عملهم، ولكي تتعامل مع البيانات في هذا النوع تحتاج لاستخدام النسخة الخاصة من SQL والمسماة T-SQL اختصارا ل Transact SQL والتي هي عبارة عن نسخة SQL مضاف عليه ادوال خاصة وتعديلات على طريقة حذف وتعديل السجلات.[10]

الفصل الثالث

الجانب العملي

3.1 مقدمة

كما وضحنا تم استخدام اللغة البرمجية فجوال بيسك دوت نت visual basic.net لغة البرمجة الاساسية وتم استخدام Html في تصميم الواجهات الخاصة بالنظام فجميع الواجهات المعروضة في هذا الجزء العملي مصممة من خلال لغة html,asp.net وكذلك تم استخدام Css كلغة تلوين في تصميم html وتم استخدام sql في انشاء قواعد البيانات وتم استخدام بيئة asp لكون asp بيئة تجمع كل ماذكرناه اعلاه وتم استخدام برنامج الفجوال ستوديو Visual studio كونه يوفر كافة المتطلبات اعلاه.

3.2 نبذة مختصرة عن برنامج الفجوال ستوديو

مايكروسوفت فيجوال استوديو: هو عبارة عن بيئة تطوير متكاملة رئيسية ولغة برمجة من شركة مايكروسوفت تستند إلى لغة بيسك الشهيرة ، حيث تتيح برمجة واجهة المستخدم الرسومية والبرامج النصية إلى جانب ويندوز فورم ومواقع وتطبيقات وخدمات الويب ، لاقت الفيجوال بيسك نجاحاً كبيراً منذ أن بدأت مايكروسوفت بإصدارها ، حيث يعتبرها المبرمجون سهلة مقارنةً بلغات أخرى مثل C و C++ ، وهي تناسب تطبيقات قواعد بيانات الشركات الغير معقدة وبرامج العملية فهي بسيطة وتؤدي الغرض المطلوب.

يحتوي فيجوال استوديو على محرر أكواد يدعم خاصية إعادة كتابة الكود ، كما يحتوي على مترجم يكشف الأخطاء الإملائية في الأكواد ، كما يضم مصمم نماذج لبناء واجهة مستخدم رسومية ومصمم ويب ومصمم فئات ومصمم مخططات لقواعد البيانات ومصمم لتقارير الكريستال ، كما يدعم العديد من اللغات مثل (C , C++ فيجوال ، جافا والفيجوال بيسك والسي شارب) والعديد من لغات البرمجة الاخرى.

- **مواصفات برنامج Visual Studio 2012:**

يتضمن Visual Studio 2012 جميع الأدوات اللازمة لتكون قادراً على إنشاء جميع أنواع المشاريع لأنظمة تشغيل Microsoft ، ولكن علاوة على ذلك ، فإنه أيضاً قادر تماماً على إنشاء مواقع ويب أو حتى برامج للهواتف المحمولة والأجهزة اللوحية ، من خلال الميزات التالية:

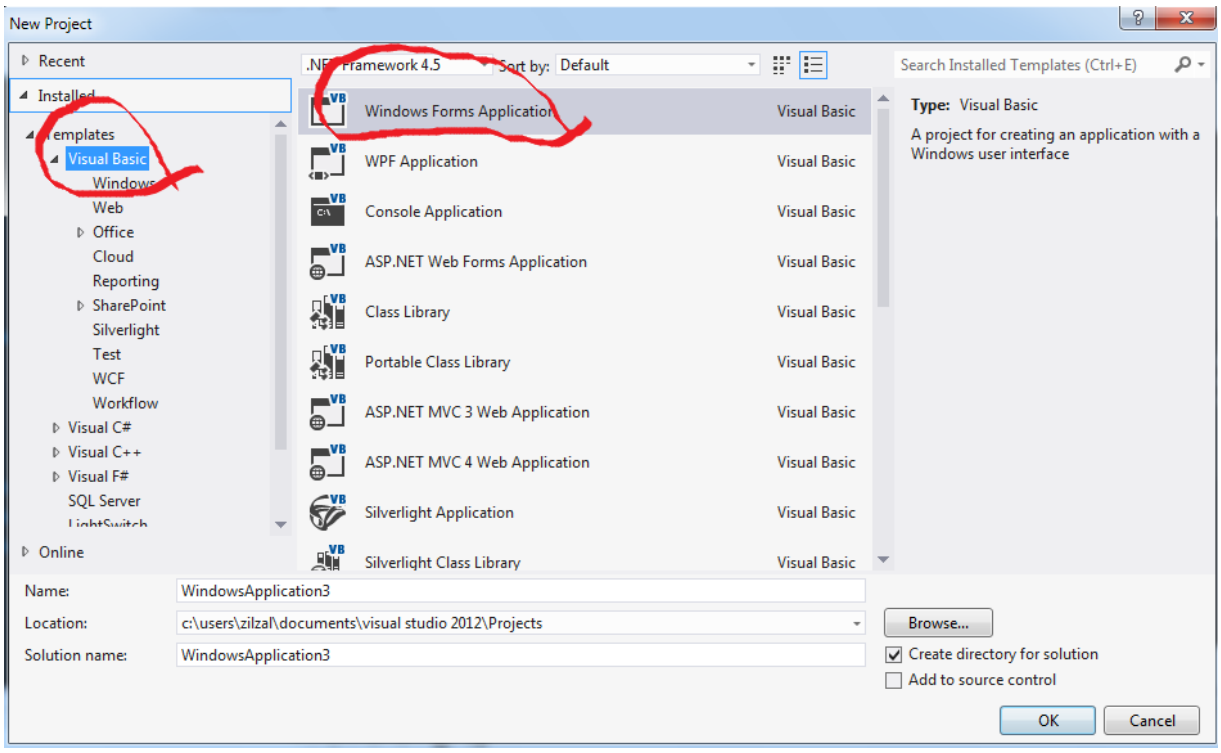
محرر الأكواد: يحتوي فيجوال استوديو على محرر أكواد يدعم تعليم الصيغة والإكمال التلقائي لتساعد المبرمج في كتابة المتغيرات و الدوال والدورات بسرعة ، ويدعمها المحرر في كتابة جميع لغات البرمجة والترميز التي يحتوي عليها فيجوال استوديو ،يدعم محرر الأكواد إمكانية وضع علامات مرجعية في الكودللمساعدة في التصفح السريع.

متعقب الأخطاء: يضم البرنامج متعقب الأخطاء والذي تدعمه جميع لغات البرمجة المدعومة ، فهو يكشف أخطاء وقت التشغيل والأخطاء الإملائية ، كما يتيح وضع نقاط توقف عند سطور الكود والتي يتوقف البرنامج عن العمل عندما يصل لهذا السطر.

نافذة Immediate Window: تسمح بتجريب الدوال قبل كتابتها.

- **هل يمكنني العمل بلغة فجوال بيسك دوت نت VB.Net على فيجوال استوديو 2012:**

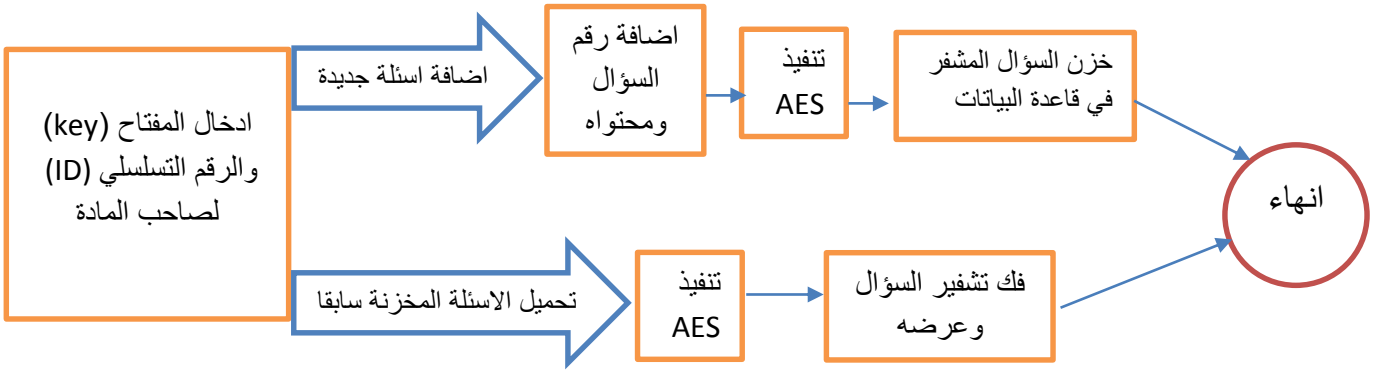
نعم ، يمكنك استخدام **فجوال بيسك دوت نت VB.Net** في Visual Studio 2012 عن طريق إختيار قالب Visual Basic أولاً ، يجب تثبيت دعم هذه اللغة أثناء تثبيت Visual Studio.



- **هل يمكنني تحديث Visual Studio 2012 إلى Visual Studio 2015:**

يمكنك تثبيت إصدار جديد مثل 2015 أو 2017 ولكنه يتم تثبيته بجانب الإصدار القديم ، ويبقى بإمكانك تشغيل كليهما ، إذا لم تعد بحاجة إلى الإصدار القديم ، يمكنك إلغاء تثبيته. يتم ذلك بهذه الطريقة لأن المطورين ما زالوا في بعض الأحيان يحتاجون إلى الإصدارات القديمة للتوافق.

3.2 التنفيذ



الاجزاء الرئيسية لتنفيذ نظام تشفير تموذج الاختبار الالكتروني

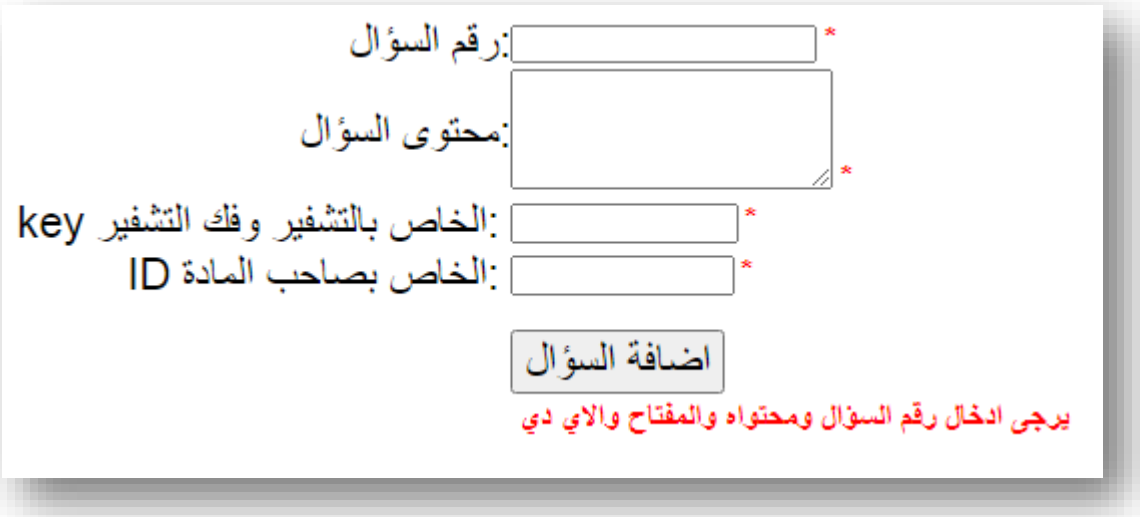
* الواجهة الرئيسية للنظام

كما موضع اعلاه تحتوي الواجهة الرئيسية على ايقونتين الاولى هي حول النظام وتتضمن معلومات عامة عن النظام والثانية هي الدخول الى النظام والتي سنشرحها اتيا:

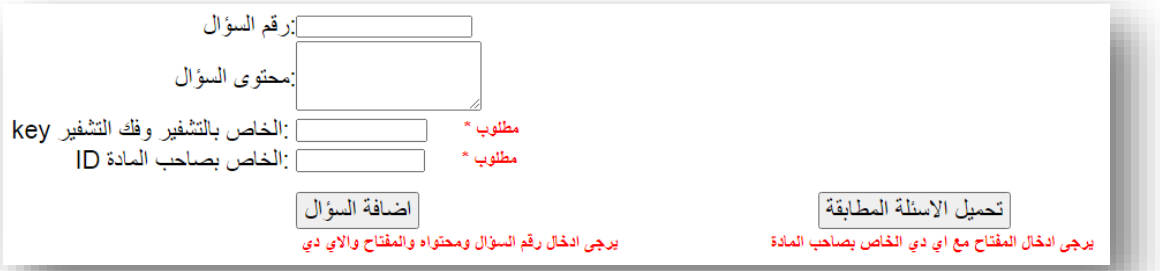
تحتوي واجهة نظام التشفير على العناصر التالية:

1. رقم السؤال.
2. محتوى السؤال.
3. key الخاص بالتشفير وفك التشفير.
4. ID الخاص بصاحب المادة.
5. اضافة السؤال.
6. تحميل الاسئلة المطابقة.

سنسرد شرح كل عنصر من العناصر السابقة وكما موضح في التالي:

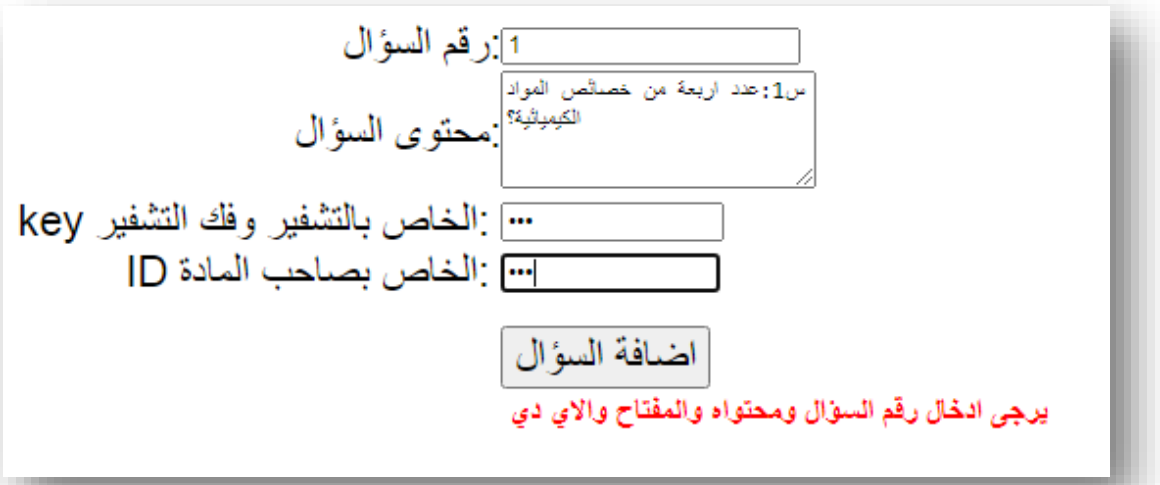


عندما نقوم بالضغط على اضافة سؤال ففي بداية الامر يقوم النظام بفحص الحقول المطلوبة فان كانت فارغة يرسل علامة التحذير الحمراء امام الحقل الفارغ لكي يتم ملئه بالبيانات فيقوم النظام بعد التاكد من ادخال البيانات بشكل صحيح باضافة هذه البيانات الى قاعدة البيانات لاجل استدعائها فيما بعد.



وعند الضغط على تحميل الاسئلة المطابقة ايضا يطلب من عندنا ادخال مفتاح التشفير وID الخاص بصاحب المادة.

فمن الطبيعي ان يكون لكل شخص يقوم باضافة الاسئلة للنظام ID خاص بيه لاجل عملية استرداد البيانات فيما بعد بواسطة الضغط على تحميل الاسئلة المطلوبة.



بعد ان نقوم بملئ البيانات رقم السؤال ومحتوى السؤال والمفتاح الخاص بالاسئلة فيجب ان نلاحظ انه يجب ان يكون المفتاح هو نفسه لكافة الاسئلة الخاصة بهذا الشخص المحدد بالاعتماد على ID الخاص بهذا الشخص والذي سيتم اختياره بشكل عشوائي من قبل الشخص الذي سيقوم باضافة الاسئلة الى النظام.

وبعد ان تتم عملية اضافة الاسئلة الى النظام نقوم بادخال المفتاح Key وID الخاص بالشخص المطلوب لاجل عملية استرداد الاسئلة من قاعدة البيانات وعرضها.

وكما موضح اعلاه تم استدعاء السؤال الذي تم اضافته الى قاعدة البيانات وجلب الشفرة الخاصة به من قاعدة البيانات لاجل ان يتم فكها باستخدام المفتاح الذي تم ادخاله بواسطة الشخص المحدد.

وكما موضح في الاعلى بالامكان ان يتم اضافةعدد غير محدد من الاسئلة الى نفس الشخص المحدد (ID) بشرط ان يتم ادخال نفس المفتاح لهذا الشخص المحدد(ID) ويتم استدعائها فيما بعد بواسطة استخدام المفتاح Key و ID فقط.

user1	NWpGbVBTiY...	*NULL*
user2	U3C4BhNEe4jP...	*NULL*
user3	/eHGsQfJ708zK...	*NULL*
user4	Ld2aMwSO3J6X...	*NULL*
user5	jKNxbjD0VrYiGI...	5
6	8hFqWvWwByf...	6
1	5T1IlTxgMmyG...	900
1	UFm5O9Cutmb...	900
1	UFm5O9Cutmb...	800
NULL	*NULL*	*NULL*

اما بخصوص ماتحتويه قاعدة البيانات فانها تحتوي فقط على السؤال المشفر اما السؤال المفكوك شفرته فلا يتم خزنه في قاعدة البيانات وانما يتم فك تشفيره بواسطة خوارزمية AES برمجيا باستخدام المفتاح وبدون خزن السؤال المفكوك شفرته في قاعدة البيانات وكذلك تحتوي قاعدة البيانات على ID الخاص بالشخص المحدد لاجل ان يتم تمييزه عن بقية الاشخاص وكذلك تحتوي على رقم السؤال.

الفصل الرابع

الاستنتاج والتوصيات

4.1 الاستنتاج

مع التقدم التقني المستمر، يتزايد انتشار الهجمات الالكترونية باستمرار. وحاليا، **لا توجد طريقة معروفة لاختراق تشفير AES، مما يجعله قوة دافعة قوية في مجال الحماية وأساسي لحماية معلوماتك** والحد من مخاطر أي هجمات. يتكامل تشفير AES بالفعل مع العديد من أنظمة البرامج والأجهزة، وإذا تم الاعتماد عليه بشكل كامل، فإن قدراته تبدو بلا حدود.

ولاجل عملية الحماية يجب ان تتم مواكبة التطورات التكنولوجية في عصورنا الحديثة فتم استخدام طريقة التشفير باستخدام خوارزمية معيار التشفير المتقدم AES (Advanced Encryption Standard) وذلك لاجل اضافة طبقة حماية عالية جدا الى البيانات التي يتم ادخالها الى قاعدة البيانات ويتم خزنها بشكل مشفر ومن ثم تتم عملية فك التشفير بعد استدعاء البيانات المشفرة من قاعدة البيانات واجراء عملية فك التشفير بواسطة المفتاح الخاص بعملية التشفير وفك التشفير.

اخيرا، وبالامكان استخدام نظامنا بشكل الكتروني (اونلاين) ويتم ادخال البيانات من اي مكان في الكرة الارضية شرط توفر خدمة الانترنت. ولاجل ان تتم عملية استعادة البيانات فيجب ان يكون لديك المفتاح الخاص بعملية التشفير وفك التشفير.

4.2 التوصيات

اقتراحاتنا للعمل في المستقبل هي :

1. نطمح لإضافة أدوات جديدة لرفع مستوى الامان الى اقصى حد ممكن.
2. بالامكان استخدام النظام في جامعتنا على سبيل المثال كونه نظام سلس وبسيط وغير معقد وصعب جدا كسر حمايته.

المصادر

[1] Z.Guan, F.Huang and W. Guan, "Chaos-Based Image Encryption Algorithm," Physics Letters A, Vol. 346, No. 1-3, 2005, pp. 153-157. doi:10.1016/j.physleta.2005.08.006

[2] H.H.Nien, C.K.Huang, S.K.Changchien, H.W.Shieh, C.T.Chen and Y.Y.Tuan, "Digital Color Image Encoding and Decoding Using a Novel Chaotic Random Generator," Chaos Solitons and Fractals, Vol. 32, No. 3, 2005, pp. 1070-1080. doi:10.1016/j.chaos.2005.11.057

[3] Q.Alsafasfeh and A. Alshabatat, "Image Encryption Based on Synchronized Communication Chaotic Circuit," Journal of Applied Sciences Research, Vol. 7, No. 4, 2011, pp. 392-399.

[4].vb4arab programming resource

[5]. اكاديمية حسوب، إبراهيم البحيصي ،2017.

[6] Symmetric-key encryption software 2017.

[7] "New cloud attack takes full control of virtual machines with little effort". Ars Technica2016 .

[8] "علم التشفير أو التعمية "، للدكتور فؤاد حمزة عبد الشريفي ، 2016.

[9] " خوارزميات Algorithms/ElGamal /AES/DES"، ستار تايمز ، 2008.

[10] .Ramez Elmasri & Shamkant B. Navathe (2010) FUNDAMENTALS OF Database Systems SIXTH EDITION.

[11] advanced encryption standard , tutorialspoint,2015.

[12] معيار تشفير المعطيات, marefa.org ,2018.

[13]. "نظام الادارة الالكتروني "، نور الهدى فالح , هدى عبد الحسين ,احمد وعد عبد علي ,حمزة شعلان نفنف ،2019.