استمارة مستخلصات رسائل و أطاريح الماجستير والدكتوراه في جامعة البصرة

الكلية : العلوم
القسم: حاسبات
التخصص: امنية معلومات
اسم الطالب: محمد حسن حالوب العبيج
اسم المشرف: حيدر محمد عبدالنبي
الشهادة: ماجستير

عنوان الرسالة أو الأطروحة:

بريد الكتروني امن باستخدام انظمة تشفير بالمنحني البيضاوي المعتمدة على الخوارزمية الجينية

ملخص الرسالة أو الأطروحة :

البريد الالكتروني عبارة عن رسالة يمكن تبادلها بين مجموعة من الأشخاص (المرسل والمستلم) باستخدام شبكة الاتصالات. حالياً يستخدم الاشخاص والشركات وقطاع الاعمال البريد الالكتروني في الاتصالات الرسمية. هناك الكثير من التهديدات على خدمة البريد الالكتروني وأحد أهم هذه التهديدات هي التنصت. بعض البريد الالكتروني مهمة جدا ويجب ان يكون لها مستوى من الأمان اثناء تبادل الرسائل.

الدراسة الحالية تستخدم دالة التجزئة لاضافة تكامل البيانات بتطبيق خوارزمية التجزئة الامنة. هذه الدراسة تستخدم خوارزمية التوقيع الرقمي بالمنحني البيضاوي لاضافة الوثوقية وعدم التنصل لرسالة البريد الالكتروني.

تشفير رسالة البريد الالكتروني هو حل للتغلب على التنصت. لهذا، المهاجم يمكنه الحصول على رسالة البريد الالكتروني لكن لا يستطيع قرأتها بدون المفتاح. خوارزمية التشفير، المستخدمة هنا، هي تشفير بالمنحني البيضاوي. هذه الخوارزمية تمتلك تشفير قوي ومستوى عالي من الامان ومفتاح صغير الحجم بالمقارنة مع خوارزمية RSA.

الاسهامات لهذه الاطروحة كالتالي: (١) اقتراح طريقة جديدة تعتمد على الخوارزمية الجينية لاختيار المعلمات الأكثر تاثيراً (a و b) للتشفير بالمنحني البيضاوي. (٢) اقتراح اربع طرائق تشفير: تحديث التشفير بالمنحني البيضاوي المتناظر، وتعديل تشفير بالمنحني البيضاوي لمينزيز–فانستون، وتشفير هجين بالمنحني البيضاوي المتناظر والغير المتناظر، وتشفير هجين بالمنحني البيضاوي لمينزيز–فانستون والجمل.

الطرائق المقترحة تمت مقارنتها مع تقنيات سابقة. وجد أنه هذه الطرائق افضل من التقنيات السابقة بدلالة وقت المعالجة للتشفير وفك الشفرة ومستوى الأمان.

اخيرا، النتائج كانت مشجعة والطريقة المقترحة المعتمدة على الخوارزمية الجينية وطرائق التشفير الأربعة المقترحة الأخرى أعطت نتائج جيدة مقارنة بالتقنيات الاخرى.

College: Science
Dept: Computer Science
Specialization: Information security
Name of student: Mohammed Hassan Haloop Alabiech
Name of supervisor: Dr. Haider M. Abdul–Nabi
Certificate: Master

Title of Thesis:

Secure Email Using Genetic Algorithm – Based Elliptic Curve Cryptography Systems

Abstracts of Thesis:

Email is a message that can be exchanged between group of people (sender and receiver) using communication network. Nowadays people, companies, and business sectors are using email in the official communications. There are a lot of threats on the email service and the most importantly one is the eavesdropping. Some emails are very important and must have a level of security during exchange of messages.

The current study uses hash function to add data integrity by applying Secure Hash Algorithm-1(SHA-1). This study uses Elliptic Curve Digital Signature Algorithm to add authentication and non-repudiation to the email message.

Encrypt of an email message is a solution to overcome the eavesdropping. Hence, the attacker can have the email message but cannot read it without the key. The encryption algorithm, which is used here, is Elliptic Curve Cryptography. This algorithm has a strong encryption, high level of security, and small key size compared to the RSA algorithm.

The contributions of this thesis are: (i) proposes a new method based on genetic algorithm to select the most effective parameters (a and b) for the Elliptic Curve Cryptography; and (ii) proposes four encryption methods: updated symmetric Elliptic Curve Cryptography, modified Menzes-Vanston Elliptic Curve Cryptography, hybrid symmetric and asymmetric Elliptic Curve Cryptography, and hybrid Menzes-Vanston Elliptic Curve Cryptography and AlGamal Elliptic Curve Cryptography.

The proposed methods are compared against previous techniques. It is found that these methods outperform the previous techniques in terms of the encryption/decryption processing time and the level of security.

Finally, the findings are encouraging and the proposed method based on genetic algorithm and the other four encryption methods give good results compared with other techniques.

Finally, the findings are encouraging and the proposed method based on genetic algorithm and the other four encryption methods give good results compared with other techniques.