استمارة مستخلصات رسائل وأطاريح الماجستير والدكتوراه في جامعة البصرة

الكلية : العلوم اسم الطالب : فرح عبد الحسين بدر

القسم : حاسبات اسم المشرف: د. رعد عبد الحسن مهجر

التخصص : شبكات وامنية معلومات الشهادة : ماجستير

عنوان الرسالة أو الاطروحة:

نظام مقترح لحماية المعلومات المتبادلة بأستخدام تقنيات التشفير مع تقنية الاخفاء في النسخة السادسة من بروتوكول الانترنت

ملخص الرسالة أو الاطروحة:

امنية المعلومات تعتبر من المواضيع ذات الاهمية والتي لها تأثير فعال على حياتنا اليومية. لذلك يجب حماية المعلومات المتبادلة وخصوصا اذاكانت المعلومات مهمة وحساسة كالمعلومات العسكرية . في الاطروحة تم اقتراح نظام لتأمين المعلومات المتبادلة عن طريق استخدام تقنيات التشفير مع تقنيات الاخفاء. في البداية يتم تشفير البيانات بأستخدام خوارزمية (CBC-RC6) بأستخدام مفتاح تشفير متفق عليه يتم توليده عن طريق مولد ارقام عشوائية مقترح , بعد التشفير يتم استخدام طريقة (message authentication code) مقترحة لتوثيق المرسل , وبعد حساب قيمة (MAC) يتم اخفاء النص المشفر بالاضافة الى قيمة (MAC) في النسخة السدسة من بروتوكول الانترنت.

College: Science Name of student: **Farah Abdul-hussain badr**

Dept: Computer Science Name of supervisor: ***Assist .prof. Dr.*** **Ra'ad A. Muhajjar**

Specialization: Networks and information security Certificate: master

Title of Thesis:

A Proposed System For Secure Data Communications Using Cryptography And IPv6 Steganography

Abstracts of Thesis:

Security is an important topic in any communication. This thesis combines cryptography method with steganography to enable sending confidential data by utilizing IPv6 protocol header as the cover to conceal the secret messages. In cryptography, RC6 was executed in CBC mode to encrypt/decrypt N blocks of the data. The key was generated using a proposed PRNG. For entity authentication or (origin authentication) a proposed MAC was implemented to the encrypted data to obtain the MAC value that will be sent along with the encrypted data to the receiving endpoints. After obtaining the encrypted data along with the MAC, both will be embedded in IPv6 flow label field.