



دراسة وتقييم طرق التوقيع الرقمي الأكثر أمان للمعلومات

اسم الطالب: رمزي حميد القانوني
اشراف: د. نصر الدين بشير الزغبى
قسم الحاسب الالى - كلية العلوم

ماجستير - 2014

ركزت هذه الدراسة على خوارزميات التوقيع الرقمي ذات المفتاح المتماثل (خوارزميات التوقيع الرقمي ذات المفتاح الخاص والعام). وهذا الموضوع هو واسع الانتشار ولكن لم يتم تغطية كل المفاهيم المتعلقة به. بدايثنا قمنا بعرض مفصل لمفهوم امن المعلومات وكل المصطلحات المتعلقة به في الفصل الاول من الدراسة. ثم وضحنا مفهوم التوقيع الرقمي والطرق المستخدمة في التوقيع الرقمي وكذلك عرضنا خوارزميات التوقيع الرقمي وكان هذا في الفصل الثاني. اما في الفصل الثالث فقد قمنا بتوضيح خدمات الامان المتعلقة بخوارزميات التوقيع الرقمي. في الفصل الرابع ناقشنا الطريقة المقترحة لمقارنة ودراسة خوارزميات التوقيع الرقمي محل الدراسة وقمنا ايضا بعرض الدراسات السابقة ، كما قمنا بسرد نتائج الدراسة التي توصلنا اليها من خلال مقارنة نتائج الطريقة المقترحة مع نتائج الدراسات السابقة.





Abstract

This thesis focuses on the topic symmetric key digital signature algorithms (Public–Privet Key digital signature algorithms). This subject is very wide, but still it is tried to cover many of the topics related to it. Firstly, a brief introduction about information security is given and its related terms are discussed. Thereafter showed digital signature algorithms and its methods. After that, comes the security services related to digital signature algorithms and it is discussed in Chapter 3. In last chapter, discussed the proposed method of evaluation with previous studies and write the results.

