البحث الخامس

أولا: الملخص باللغة العربية

علم التشفير المنكور تم تقديمه بواسطة كانيتى و آخرون عام ١٩٩٧ لضمان أن المُرسل أو المستقبل لرسالة سرية صحيحة يمكنه أن يخدع الخصم أن هذه الرسالة وهمية .

فى هذا البحث تم التركيز على التشفير المنكور من جانب المُرسل فقط ، و قد تم دراسة عدة أنظمة من أهمها النظام المقدم من ماجد حماده إبراهيم ، و قد تم تحليل تلك النظام و تبين أنه يعانى من ثلاث مشكلات رئيسية:

١. النظام غير قادر على معرفة و تمييز الرسالة المزيفة من مجموعة رسائل صحيحة.
٢. النظام غير آمن ضد مشكلة المعادلات التربيعية المتبقية QRP.
٣. عملية فك التشفير بطيئة جداُ لأن هذا النظام يعتمد بشكل كبير على حسابات الجذر التربيعى حتى يحصل على الرسالة الصحيحة بدون مشكلة QRP.

بدراسة تلك المشكلات الثلاث ، تبين أن المشكلة الأولى تم السيطرة عليها من قِبل هولادير و باسو ، بحيث يمكن من خلال تلك النظام إستخراج الرسالة المزيفة من مجموعة رسائل صحيحة ، و لكن مازال يعانى من باقى المشكلات سالفة الذكر.

فى هذا البحث ، تم تقديم نظام تشفير منكور جديد ذات المفتاح العام من جانب المُرسل. من خلال تلك النظام فإن المُرسل يستطيع بسهولة خداع الخصم برسالة زائفة على أنها صحيحة و تم عمل مقارنة بين النظام الجديد و النظامين السابقين و تبين من خلال نتائج البحث الآتى:

١. النظام الجديد آمن ضد مشكلة المعادلات التربيعية المتبقية QRP .
٢. عملية فك التشفير أسرع بكثير من الأنظمة السابقة ، و هذا سيؤثر بدوره فى التطبيقات المختلفة التى يُستخدم فيها نظام التشفير المنكور.

من ناحية أخرى ، تم تطبيق تلك النظام على نموذج كيفية التصويت على الإنتخابات عبر الإنترنت بحيث يعمل نظام التشفير المنكور الجديد على تأمين و سلامة التصويت دون تدخل الخصم ام من ليس له الحق فى التصويت.