

دراسة بحثية في كلية تكنولوجيا المعلومات تناقش " توليد مفتاح امن باستخدام شبكة بتري "

ناقشت دراسة
بحثية في كلية تكنولوجيا المعلومات اعتمدها الباحثة رند عبد الواحد محمد علي
والموسومة :
" توليد مفتاح امن باستخدام شبكة بتري "
وتناولت الدراسة
التشفير هو العلم الذي يهتم بحماية المعلومات المهمة من الاشخاص الغير مخولين.
تكون عملية
التشفير بالتشفير التدفقي على بت بت من النص الصريح عن طريق عملية XOR مع مفتاح
التشفير .
وهو اهم جزء بالتشفير التدفقي هو عملية توليد
المفتاح .
يعتمد النظام
المقترح على مجموعة مكونة من اربعة شبكات بتري ملونة وشبكة بتري عد
ادية التوليد
مفتاح معقد شبه عشوائي .
تمتلك البتري
نت موديل مثالي لتوليد مفتاح معقد طويل.
يتطلب هذا
النظام مفتاح قصير ذا طول 128 بت كقيمة ابتدائية متف عليها من قبل الطرفين المرسل
والمستقبل لتكون التاشير الابتدائي لشبكات البتري الملونة.
يختلف الناتج
المتولد من كل شبكات البتري الملونة من وقت الى اخر بالاعتماد على انتقال القيم
بين عقد الشبكة والتي تختلف من واحدة الى اخرى .
تزيد عملية ربط
شبكات البتري الملونة مع شبكات بتري عادية من اللاخطية للمفتاح المتولد.
استخدمت عملية
الترميز الرمادي واعادة ترتيب النص الصريح في النظام المقترح من اجل زيادة امن
النص المشفر المتولد. استخدمت مجموعة من الاختبارات العشوائية لاثبات
عشوائية وتعقيد المفتاح.