# مناقشة اطروحة دكتوراه في كلية تكنولوجيا المعلومات عن تحسين الامن باستخدام خوارزمية للتشفير الكتلي غير المتجانسة مقترحة

---

تم مناقشة
اطروحة دكتوراه في كلية تكنولوجيا المعلومات للطالب احسان احمد محمد عن اطروحته
 الموسومة بـ :" تحسين الامن باستخدام
خوارزمية للتشفير الكتلي غير المتجانسة مقترحة "
بأشراف الدكتور
عبد الكريم عكلة
وتكونت اللجنة
من الاستاذ الدكتور ستار بدر سدخان رئيسا وعضوية كلا من الاستاذ الدكتور وسام سمير
 بهية
والاستاذ المساعد الدكتور صلاح عبد الهادي والاستاذ المساعد الدكتور سعد عبد
الرضا والدكتورة سراب مجيد حميد
وبين الباحث
احسان احمد ان في اطروحته هذه ثلاث خوارزميات معتمدة التشفير الكتلي حيث ان
الخوارزمية المقترحة الاولى هي من نوع فيستل 
معتمدة على التشفير الكتلي حيث تم
تصميمها مع طول الكتلة 128  بت وطول المفتاح 140 بت تنفذ
كلها خلال 20  جولة لإعطاء خوارزمية
 امنية
عالية يمكن استخدامها في اغراض مختلفة .
اما الخوارزمية
المقترحة الثانية فهي عبارة عن خوارزمية تشفير كتلي غير فيستل مقترنة بمجموعة
متعددة من خوارزمية تشفير كتلي غير
 فيستل
مقترنة بمجموعة متعددة من 32 بت كطول كتلة تنفذ في شفرات كتل متعددة متجانسة تعتمد على مجال
التطبيق ويتم ادخال 48 بت كطول للمفتاح 
المطبق يتم ادخاله تلقائيا كل هذا يتم تنفيذه في
جولة واحدة لإعطاء خوارزمية امنية عالية وسريعة تستخدم في اغراض مختلفة .
والخوارزمية
المقترحة الثالثة هي خوارزمية تشفير كتلي غير متجانسة والتي تم تصميمها للربط بين
خوارزميات التشفير الكتلي يجب 
ان يتم اختيارها في نمط مختلف (الخوارزميتين
المقترحتين سابقا) في نموذج جديد بغض النظر عما اذا كانت الخوارزميات المختارة 
هي
نفس طول الكتلة وطول المفتاح ام لا وكذلك يجب ان يكون وقت التنفيذ مساويا لكل من
الخوارزميات
بعد ذلك يتم
ادخال 256 بت كمدخل للخوارزمية الثالثة كطول كتلة و 332 بت كطول للمفتاح السري الذي يتم اخاله
تلقائيا.

  