/التشفير بطريقة هل باستخدام نظام EBCDIC/

/Cryptography by HILLs Method using the EBCDIC System/

إعداد الطالب :عبد القادر قدورة

بإشراف : د . عبد الباسط الخطيب د . محمد نور شمه

الملخص

تقدم ورقة البحث هذه تطوير طريقة هِلْ (Hill ciphers) ١٩٢٩ م وذلك من خلال:

١. الاعتماد على ترميز EBCDIC(Coding EBCDIC) المضاف إليه عنصر مما يجعل عدد محارفه(٢٥٧) عددا أوليا وبالتالي تكون جميع الأعداد الأصغر منه أولية نسبيا معه .

٢. استخدام دالة النظير الضربي $f(X)=(A\hat{X}+B)\bmod(257)$ عناصرها (A, X, B) مصفوفات لها شروط خاصة بحيث تصبح قادرة على تشفير رسالة كاملة دفعة واحدة اعتماداً على حساب المصفوفات ذات المراتب العليا ، مما يجعلها صعبة الكسر الأمر الذي يحافظ على أمن المعلومات داخل النصوص والرسائل المبثوثة .

٣. قابلية تطبيق الطريقة حاسوبياً لتعطي نتائج سريعة و كبيرة .

/Cryptography by HILLs Method using the EBCDIC System/

Abstract

In this paper, we try to introduce a modern method about the cryptology(Hill ciphers).

Our method is based on :

- Coded EBCDIC used in current computers.
- Using of a symmetric product function ($f(X)=A.\hat{X}+B$) such that A, X and B are a specified matrixes .
- Rely on the encoding EBCDIC (EBCDIC Coding) added to it an element which makes the number of marks 257 and all the smaller numbers of 257 are a relatively preliminary with 257 .
  -Its application by using computers to provide effective results [5].

Key word: Cryptology Hill**,** EBCDIC system **,** Plaintext ,Ciphertext