المملكة العربية السعودية
جامعة الملك سعود
كلية العلوم
قسم الرياضيات

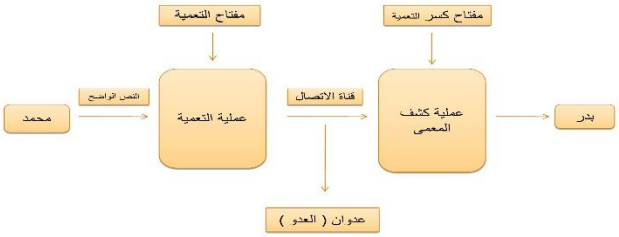
Kingdom of Saudi
Arabia King Saud
university College
of Science
Mathematics

انظمة التعمية التقليدية

المقدمة :

يعرف علم التعمية على أنه العلم الذي يهتم بالوسائل المثلى لإخفاء المعلومات في الرسائل ذات الطبيعة السرية .

والوضع ادناه يبين تبادل الرسائل بين شخصين مع عملية التعمية وكشف المعمى :



و يتكون نظام التعمية من الخماسي (P, C, K, E, D) حيث :

١/ P مجموعة منتهية من الرموز تسمى النص الواضح .

٢/ C مجموعة منتهية من الرموز تسمى النص المعمى .

٣/ K مجموعة منتهية من المفاتيح تسمى فضاء المفاتيح .

٤/ لكل $k \in K$ توجد دالة تعمية $e_k \in E$ تقابلها دالة كشف المعمى $d_k \in D$ بحيث يكون $e_k : P \to C$ و $d_k : C \to P$ و

$d_k\left(e_k(x)\right) = x$ لكل $x \in P$.

ملخص البحث :

تطرقنا الى أساسيات نظرية الأعداد ومن ذلك قابلية القسمة والتطابقات ، والى أنظمة التعمية التقليدية حيث تنقسم إلى ستة أنظمة ومن ذلك نظام الازاحة وتعريفه :

في نظام الإزاحة يكون $P = C = K = \mathbb{Z}_{29}$. و دالتا التعمية و كشف المعمى هما :

$e_k(x) \equiv x + k \pmod{29}$ لكل $x \in P$ و $k \in K$ و $d_k(x) \equiv x - k \pmod{29}$ لكل $x \in C$

وكذلك نعرف نظام هيل كالتالي :

في نظام هيل يكون $n \in \mathbb{Z}^+$ ويكون $P = C = (\mathbb{Z}_{29})^n$ ويكون $K = \{A \in M_n(\mathbb{Z}_{29}) : gcd(det\, A, 29) = 1\}$ لكل $A \in K$

و $X \in (\mathbb{Z}_{29})^n$ ، فإن دالتي التعمية وكشف المعمى تعرفان على النحو التالي :

$d_A(X) \equiv A^{-1}X \pmod{29}$ و $e_A(X) \equiv AX \pmod{29}$

، والى تحليل هذه الأنظمة عبر تحليل التردد واستنفاد المفاتيح وغيرها من الطرق فنجد ان نظام الازاحة سهل الكسر باستخدام تحليل التردد حيث معرفة حرف واحد من النص الواضح ومايقابلة من النص المعمى كاف لمعرفة مفتاح التعمية .

النتائج والتوصيات :

التقدم السريع للاتصالات والحاسبات الآلية أدى إلى اهتمام أكبر في علم التعمية من أجل الحماية الأمنية و المالية والاقتصادية للمعلومات المنقولة عبر شبكات الاتصال ، وكون نظام تعمية معين آمناً اليوم فهذا لا يضمن استمرار أمنه في المستقبل.

قام بعمل البحث الطالب: سعد ناصر العوام
إشراف الدكتور: شعلان القرني