التشفير المركب باستخدام نظام ASCII وبأكثر من مفتاح

Combined Cryptography Using The ASCII With Many Keys

رسالة أعدت لنيل درجة الماجستير في الرياضيات

إعداد الطالب : وسام أحمد

بإشراف

أ.د. عبد الباسط الخطيب أ.د. محمد نور شمة

الملخص

هدف التشفير الحفاظ على سرية الرسائل المبثوثة عبر قنوات الاتصال المختلفة كالراديو والهاتف والجوال والبريد الالكتروني و الحكومات الالكترونية.. الخ.

و قد استعمل العرب مصطلح التعمية كناية عن عملية تحويل نص واضح إلى نص غير مُعَمَّى باستعمال طريق محددة ، يستطيع من يفهمها أن يعود و يفهم النص ، لكن كثر في الوقت الحالي استعمال مصطلح التشفير رديفاً لمصطلح التعمية .

هناك طرائق عِدّة للتشفير نذكر منها التشفير بطريقة Hill ، وقد قمنا بتطويرها لتصبح ملائمة للمتغيرات الحديثة ، فبدلا من الترميز بالحروف الانكليزية استخدمنا جميع الحروف و العلامات المستخدمة في نظام ASCII ، كما استخدمنا دالة النظير الجمعي $f(X)=(A\overline{X}+B)$ عناصرها (A, X, B) مصفوفات لها شروط خاصة بحيث تصبح قادرة على تشفر وتفك الشيفرة لرسالة كاملة دفعة واحدة اعتماداً على حساب المصفوفات ذات المراتب العليا بدلاً من طريقة هِل (Hill ciphers) المعتمدة على الترميز المتعدد للرسالة الواحدة (polygraphic).

تعريف ١ :

ليكن لدينا $1\le a<n$ نقول عن العدد a إنه أولي نسبياً مع العدد n إذا كان القاسم المشترك الأعظم لهما هو الواحد أي إذا تحقق : $\gcd(a,n)=1$

تعريف ٢ :

نسمي M_n مجموعة جميع الأعداد الأولية نسبياً مع العدد n أي أن :

$$M_n=\{a\in N;1\le a<n,\ \gcd(a,n)=1\}$$

تعريف ٣ :

نقول إن العدد الصحيح b هو النظير الجمعي للعدد $0\le a<n$ بالمقاس n إذا كان باقي قسمة $a+b$ على العدد n هو الصفر أي إذا تحقق : $a+b=n$

مبرهنة ١:

يوجد نظير ضربي للعدد a قياس $n\in N$ إذا وفقط إذا كان $\gcd(a,n)=1$

تعريف ٤ (مصفوفة هِلْ Hill):

هي مصفوفة عددية مربعة من المرتبة k ($k=1,2,3..$) نرمز لها A_k وتحقق

ما يلي : $|A_k| \in M_{256}$ أي أن :$\gcd(|A_k|\ ,\ 256\ )=1$ فمثلاً من أجل $k=1$ نحصل على مصفوفة مربعة مؤلفة من عنصر واحد نرمز لها A_1 وعندما $k=2$ نحصل على مصفوفة مربعة مؤلفة من أربعة عناصر نرمز لها A_2 وعندما المرتبة k نحصل على مصفوفة مربعة مؤلفة من k^2 من العناصر نرمز لها A_k .

تعريف ٥ (مصفوفة الانسحاب):

هي مصفوفة عددية مربعة من المرتبة k حيث $k=1,2,3..$ نرمز لها B_k بحيث يتحقق :

$$B_k=[\ b_{i,j}\ ];\ 0 \le b_{i,j} < 256$$

تعريف ٦ (مصفوفة النص الواضح) :

ليكن لدينا P النص الواضح (Plaintext) نشكل منه مصفوفة حروف من المرتبة k ، نرمز لها P_k بحيث نحصل عليها بتبديل الحروف بحسب الأعمدة فنضع الحرف الأول في النص مكان العنصر p_{11} و الحرف الثاني في النص مكان العنصر p_{21} وهكذا حتى نصل إلى العنصر الأخير p_{kk} . وبتبديل كل حرف بمقابله العددي في المصفوفة P_k نحصل على مصفوفة الأرقام X .

تعريف ٧ (مصفوفة النص المشفر):

ليكن لدينا النص المشفر C (Ciphertext) نشكل منه مصفوفة عددية مربعة من المرتبة k حيث $k=1,2,3..$ نرمز لها بالرمز X_k بحيث نحصل عليها بتبديل حروف ASCII بالمقابل العددي مرتبة كما وردت في النص المشفر .

تعريف ٨(مصفوفة النظير الجمعي) :

لتكن لدينا مصفوفة الأرقام $X=(x_{ij})$ ، بتبديل كل عنصر من عناصر المصفوفة X بنظيره الجمعي نحصل على مصفوفة النظير الجمعي $\overline{X}$.

تعريف ٩:

مفتاح التشفير (Enciphering Key) : هو الدالة المركبة من الدالة المصفوفية لمصفوفة النظير الجمعي $f(X)=(A\overline{X}\ +B)$ والدالة الخطية $g(X)=A'X+B'$ التي تستخدم في وصف عملية التشفير و تعطينا النص المشفر .

أهم نتائج البحث :

طريقة النظير الجمعي في التشفير:

هي إبدال كل حرف ASCII في الرسالة المبثوثة بحرف آخر من ASCII من خلال دالة المصفوفية $F(X)=A_k\overline{X}\ +B_k$ حيث أن: A_k و B_k مصفوفتين من المرتبة k حيث

$k = 1,2,3..$)، وأن $\overline{X}$ مصفوفة النظير الجمعي للمصفوفة X المراد تعميتها لها نفس مرتبة المصفوفتين A_k و B_k .

فإذا كان عدد حروف النص الأصلي أقل من k^2 نملئ أماكن الحروف الناقصة بآخر حرف من حروف النص الأصلي أما إذا زادت عن k^2 فإننا ننشئ مصفوفة جديدة X_1 نقوم بتعميتها لاحقاً بعد تشفير المصفوفة X .

مبرهنة (٢) :

إن تشفير كل نص واضح P (من الحروف ASCII) من خلال الدالة المصفوفية لمصفوفة النظير الجمعي من الشكل : $F(X) = A_k \overline{X} + B_k$ " يتم بشكلٍ وحيد .

مبرهنة (٣) :

إن فك التشفير عن كل نص مشفر C (من الحروف ASCII) من خلال دالة مصفوفية خطية من الشكل : $\overline{X} = A_k^{-1}(F(X) - B_k)$ " يتم بشكلٍ وحيد .

خوارزمية النظير الجمعي في التشفير المركب:

إذا كان لدينا نص واضح P نشفره وفق الدالة المصفوفية المركبة كما يلي :

١ . نرتب حروف النص الواضح في المصفوفة P_k .

٢ . نستبدل المصفوفة P_k بمصفوفة الأرقام X الموافقة ، ثم نطبق عليها الدالة $g(X) = AX + B$.

٣ . نستبدل كل رقم في المصفوفة $g(X)$ بنظيره الجمعي بالمقاس ٢٥٦ .

٤ . نضرب المصفوفة C_k بمصفوفة النظير الجمعي الرقمية $\overline{g(X)}$ ونضيف للناتج المصفوفة D_k فنحصل على المصفوفة العددية $C_k \overline{g(X)} + D_k$.

٥ . نصلحها لتصبح جميع الأرقام بالمقاس ٢٥٦ ثم نستبدلها بالحروف المقابلة لها فنحصل على النص المشفر **C** المطلوب .

ملاحظة هامة :

لتشفير نص واضح (فك التشفير عن نص مشفر) كبير الحجم لابد من استخدام برامج حاسوبية تتعامل مع المصفوفات والعمليات عليها ،أجرينا في هذا البحث مثال باستخدام لغة البرمجة ***Matlab*** ، و بنظام التشغيل ويندوز XP.

Abstract

The goal of the "Cryptography" is to preserve the confidentiality of messages delivered via various channels of communication radio , telephone , mobile phone , e-mail and e-government , etc .

There are many ways to obscure restrict ourselves to cryptography Hill method . We develop this method to be suitable for modern variable , instead of coding by the English letters , we use all the letters and labels used in the ASCII (256 marks).On the other hand , we use a symmetric additive function ($f(X) = A.\overline{X} + B$) such that A , X and B are a specified matrices so as to break encryption and code to the letter in full version along one matrix depending on the calculation of large arrays of salary rather than the way of Hill (Hill cipher) based on the multi-coding of a single message (polygraphic). Before explaining this method , we have to cite some of the concepts and definition .

Throughout this paper , M_n denotes the set off all relatively prime numbers to the positive integer n :$M_n = \{1 \leq a < n; \gcd(a,n) = 1\}$.

Definition 1. Let a be the number such that $1 \leq a < n$. We say that a relatively prime modulo n , if we have that the greatest common divisor is 1 , then we have $\gcd(a,n) = 1$.

Definition 2. The two positive number a and b are symmetric additive modulo n if: $a + b = n$

Lemma 1 . For every positive number a, there is a symmetric product number modulo n if and only if $gcd(a,n) = 1$

Definition 3. (Matrix Hill) It a square matrix with integers of order k $(k = 1,2, \dots)$

With symbol A_k and verifies the following : $|A_k| \in M_{256}$. If $k = 1$,then we get a square matrix composed of one element with symbol A_1 , and when $k = 2$,

then we get a square matrix composed of four elements with symbol A_2 ,and for k, we get a square matrix composed of k^2elements with symbol A_k .

Definition 4. (Matrix withdrawal) It is a square matrix with integers of order k ($k = 1,2, \dots$) with symbol B_k such that $B_k = [b_{i,j}]; 0 \leq b_{i,j} < 256$.

Definition 5. (Matrix of clear text) Suppose we have *P* a plaintext ,to form a matrix P_k of letters with rank k ; $k = 1,2,3, \dots$,so we get it by replacing the letters columns according to the first letter put in place the text component and crafts second place in the text elements $P_{1,1}$, and so on until we reach the last element $P_{k,k}$.

Definition 6. (Matrix circulated text) We have a ciphertext C , which forms a square matrix of numerical ranking branded k; $k = 1,2,3, \dots$, so we get it replacing the ASCII characters X_k for the number of Table 1 also ranked in the ciphertext

Definition 7. (Matrix symmetric additive text) Suppose we have $P = (p_{i,j})$ a plaintext matrix ,and X is it's equivalent numbers matrix ,then $\bar{X}$ meaning that replacing every element in the matrix X with its symmetric additive modulo 256 .

Definition 8. (Enciphering key) The key encryption or code is function valued matrix $F(X) = A_k\bar{X} + B_k$, which is used to describe the process of cryptography ,and give us the ciphertext .

Main Result

The modern cryptography : The developed method of Hill consists of replacing of all ASCII letters in the messages delivered by another ASCII letters through symmetric additive function $F(X) = A_k\overline{X} + B_k$ such as A_k and B_k are matrices of rank k; $k = 1,2,3, \dots$, and $\overline{X}$ matrix symmetric additive number to this matrix has same order as the matrix A_k , and the matrix B_k .

- If the number of letters of the original text is less than k^2 , then we fill the missing letters by the last letter of the original text .

- **Lemma 2 .** The cryptography of a coded plaintext P with ASCII system through a linear function given by $F(X) = A_k \overline{X} + B_k$, is determined only in a one method .
- **Lemma 3 .** every cipher text by ASCII system is deciphered in only one way according to the inverse of the linear function $\bar{X} = {A_k}^{-1}(F(X) - B_k)$.

The Algorithm of Cryptography

If we have a plaintext P , and we want to encryption according to a function valued matrix $F(X) = A_k \overline{X} + B_k$, then

1. Arrange plaintext letters in the matrix P_k .
2. Replace P_k with the matrix array X approval from Table 1 , then we get the numerical matrix $g(X) = A_k X + B_k$ . .
3. Find the symmetric additive for every element in $g(X)$ from Table 2.
4. Make the product of the matrix array C_k with $g(X)$and add to output matrix D_k , we get the numerical matrix $C_k \overline{g(X)} + D_k$.
5. Organize it to become all numbers compared with 256 and then replace the corresponding letters from Table 1 to get the cipher text C required .

Encryption Algorithm Dismantling : Conducted in a manner contrary to the way the previous .