# شفرةهيل Hill Cipher

**تعتبر شفره هيل هي أول شفره تتعامل فيها مع 3 حروف في نفس الوقت ، وسميت بهذا الاسم**

**نسبه إلى مخترعها Lester S Hill وهي تعتمد في عملها على الجبر الخطي . ولكي تستطيع ،**

**التشفير بها يجب أن يكون لديك أساسيات التعامل مع المصفوفات ( ضرب المصفوفات بالذات ).**

**قبل أن نبدأ بالتشفير ، يجب أن يكون جدول الحرف قريب لديك.**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

$c_1 = (k_{11P1} + k_{12P2} + k_{13P3}) \bmod 26$

$c_2 = (k_{21P1} + k_{22P2} + k_{23P3}) \bmod 26$

$c_3 = (k_{31P1} + k_{32P2} + k3_{3P3}) \bmod 26$

$C = KP \bmod 26$

$C = E(K, P) = KP \bmod 26$

**و علينا أولا اختيار المفتاح ، مثلا كان مكون من تسعه حروف ، سوف تكون المصفوفة ( الخاصة بالمفاتيح) 3*3 ، أي ثلاثة صفوفه وثلاثة أعمده.**

**متال على التشقير بـــ(hill cipher) .**

**لدي جملة التشفير التالية GYBNQKURP**

**بعد أعطاء كل حرف قيمته ، نقوم بوضعه داخل المصفوفة 3*3 على شكل وتكون شكل**

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

**وليكن النص الاصلي هو ACT . وفي حال كان أكبر من ذلك يتم تقسيمه إلى بلوكات ،**

**كل واحد يتكون من ثلاثة حروف**

**نقوم بوضع النص الأصلي داخل مصفوفة1 *3.**

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

**الآن نقوم بعمليه ضرب المصفوفتين ، نضرب الصف الأول في المصفوفة الأولى بالعمود في**

**المصفوفة الثانية نضع الناتج في المصفوفة الجديدة . وهكذا لباقي الصفوف نقوم بضربها بالعمود .ونأخذ الناتج بعمليه باقي القسمة MOD 26.**

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \mod 26$$

**اذا الناتج من هذا النص بعد تحويل هذه الأرقام إلى حروف (بمساعده جدول الحروف)**

**، أي النص المشفر هو POH**

**ولفك التشفير ، كل ما عليك هو إيجاد معكوس المصفوفة ، وتقوم بضربه في النص المشفر مع أخذ باقي القسمة على 26 ، كما هو موضح بالصورة:**

**$P = D(K, P) = K^1C \bmod 26 = K^1K=P$**

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \mod 26$$

**هناك في الحقيقة أنواع كثيرة من هذه الشفرات ، منها Hill Cipher - 3 ، وفي هذه الحالة المصفوفة يجب أن تكون من3*3 . وهو الذي تحدثنا عنه من قليل،**

**وفي حال النوع 2-Hill Cipher يجب أن تكون من 2*2.**

**وبشكل عام اذا كان لدينا شفره منn-Hill Cipher فأنه سوف يكون لدينا مصفوفة من n*n .**

# الشفرة ألأمنه THE ONE-TIME PAD

هذه الشفره هي الشفره الأكثر أمانا على مدى تاريخ التشفير ، لم ولن يستطيع أحد كسر شفرات هذا النوع أبدا ، واستخدمت هذه الشفرات في الكثير من الحكومات وأجهزه الاستخبارات.

طريقه الشفره كالتالي ، هو عمل( مثلا نطلق عليه )كتاب one-time pad

بداخل هذا الكتاب توجد صفحات Sheets بداخل كل صفحه من هذه الصفحات أرقام عشوائية لا تتكرر أبدا ، هذه الأرقام العشوائية تمثل الازاحه المستخدمة (أي كل رقم منها هو مفتاح).

في حال شفرت نص بهذه الطريقه أقوم بإرسال النص المشفر و رقم الصفحة إلى الطرف الأخر ، وأقوم بقطع الصفحة من الكتاب وأحرقها بالنار ، اذا لزم الأمر أي يتم القضاء عليها

والطرف الأخر يكون لديه نسخه مماثله من الكتابone-time pad ويقوم بفك التشفير عن طريق رقم الصفحة ، و بعدما يتم فك التشفير والحصول على النص الأصلي ، يتم أيضا قطع الصفحة أيضا

مثال ، لدي الشفره التالى ENGAGE WARP DRIVE

والصفحة الأولى تتكون من:

9 20 13 0 21 1 13 19 9 5 25 12 25 4 7 25 0 8 8 7 24 2 6 18 16 10 23 5 11

12 13 6 22 22 17 3 8 0 0 19 4 15

أقوم بجمع الحرف الأول E مع الرقم الأول 9 لينتج N و أجمع الحرف الثاني N مع الرقم الثاني 20 لينتج H وهكذا.....

اذا تبقت أرقام في الصفحة ، أو لم تبقى هناك أي أرقام ، أقوم بتدمير الصفحة ،

شكل النص بعد التشفير :

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plaintext letter | E | N | G | A | G | E | W | A | R | P | D | R | I | V | E | | | | | | |
| Shift value | 9 | 20 | 13 | 0 | 21 | 1 | 13 | 19 | 9 | 5 | 25 | 12 | 25 | 4 | 7 | 25 | 0 | 8 | 8 | 7 | 24 |
| Ciphertext letter | N | H | T | A | B | F | J | T | A | U | C | D | H | Z | L | | | | | | |
| Plaintext letter | | | | | | | | | | | | | | | | | | | | | |
| Shift value | 2 | 6 | 18 | 16 | 10 | 23 | 5 | 11 | 12 | 13 | 6 | 22 | 22 | 17 | 3 | 8 | 0 | 0 | 19 | 4 | 15 |
| Ciphertext letter | باقي الارقام في الصفحه ، لا تستخدم | | | | | | | | | | | | | | | | | | | | |

وهكذا نلاحظ أنه يستحيل كسر الشفره هنا ، لأن المفتاح عشوائي ولن يتكرر أبدا ، وفي هذه الحالة لن يتم كسر الشفره.

هذه الطريقه لن تستخدم هذه الأيام بسبب صعوبة الاحتفاظ بهذا الكتاب ، وصعوبة إرساله إلى الطرف الأخر ، أيضا صعوبة أضافه صفحات جديدة فيه ولكن في حاله كنت مرسل كتاب إلى الطرف الأخر من قبل ، يمكنك إرسال شفرات بهذا النوع ، ولن يكشفها أي أحد على الإطلاق ، إلا في حال أنكشف الكتاب(one-time pad ) !

بسم الله الرحمن الرحيم

الجمهورية اليمنية
وزارة التعليم العالي والبحث العلمي


كليه :علوم الحاسوب ونظم المعلومات
المستوى: الثالث
القسم:تقنيه معلومات

نعوان البحث:-

# HILL CIPHER AND ONE TIME PAD CIPHER

عمل الطالب:

محمد ضيف الله الزيداني

أشراف الدكتور:-
عبد الرحمن الصبري