استخدام طريقة فستل لتشفير النصوص ذات الأطوال الفردية

نزار خلف حسين الدخيّل

قسم الرياضيات ، كلية علوم الحاسبات والرياضيات ، جامعة تكريت ، تكريت ، العراق

(تاريخ الاستلام: ١٠ / ٨ / ٢٠٠٨ ---- **تاريخ القبول:** ١٥ / ١٢ / ٢٠٠٨)

الملخص

أن طريقة فستل للتشفير تعتبر من أهم طرق التشفير الكتلي (*block cipher*)، وتعتمد هذه الطريقة على تشفير النصوص ذات الطول الزوجي أي أن هذه الطريقة تستلزم أن يكون طول النص المراد تشفيره طولاً زوجياً، في هذا البحث نحاول أن نستخدم نفس الطريقة ولكن لتشفير النصوص ذات الطول الفردي بشكل خاص، وجعل الطريقة عامة وليست خاصة بالنصوص ذات الطول الزوجي فقط.

مشكلة البحث

مشكلة البحث هي أن طريقة فستل للتشفير لاتشفر الرسائل التي بطول فردي أي أنها تشفر الرسائل التي بطول زوجي فقط مما يجعل الطريقة مقتصرة على نوع من الرسائل فقط وليست عامة لكل الرسائل.

هدف البحث

إن الهدف من البحث هو تعميم طريقة فستل للتشفير لكي يمكننا استخدامها لتشفير كافة الرسائل بغض النظر عن أطوالها الفردية أو الزوجية أي أن الطريقة تصبح عامة لجميع الرسائل.

المقدمة

التشفير هو العلم الذي يتم فيه استخدام الطرق التي يتم من خلالها تحويل الرسائل المفهومة إلى رسائل غير مفهومة ومن ثم أعادة هذه الرسالة الغير مفهومة إلى رسالة مفهومة، وعلى الرغم من أن تقنيات التشفير تلعب دوراً كبيراً في تحديث نظم أمن الحاسبات، إلا أن الأدوات المستخدمة لتشفير البيانات بطيئة وتعاني من الثغرات التي تسهل الهجوم عليها[1]، وهناك طريقتين رئيسيتين للتشفير هما طريقة التشفير السيلي (*stream cipher*) وطريقة التشفير الكتلي (*block cipher*) ، وفي هذا البحث سنتناول طريقة التشفير الكتلي، حيث أننا سنأخذ طريقة فستل للتشفير وهي أحدى طرق التشفير الكتلي، وسنتناول تلك الطريقة بالتفصيل ونحاول أن نقترح طريقة لتشفير النصوص ذات الطول الفردي باستخدام طريقة فستل للتشفير وذلك لان طريقة فستل تستلزم أن يكون طول النصوص زوجي لكي يتم تشفيرها مما يعني أن هذه الطريقة ليست عامة لكل النصوص وما نحاول تحقيقه في هذا البحث هو تعميم هذه الطريقة لتشمل كل النصوص حتى وإن كانت بأطوال فردية، فعندما يكون طول النص زوجي فانه يتم تجزئته إلى قسمين بينما عندما يكون طول النص فردي فان التقسيم يكون حسب العدد الفردي وإلى k من الأقسام عندما يكون ذلك العدد الفردي يقبل القسمة على k بحيث أن k أصغر عدد صحيح يقبل القسمة علية ذلك العدد الفردي.

الجانب النظري

(١-١) التشفير

(*cipher*) هو طريقة تحويل النص الواضح إلى صيغة غير مفهومة(مشفرة) باستعمال حروف أو أرقام تعويضية أو الدمج بينهما بحيث أنها تعمل عمل الحروف الأصلية أو بواسطة تبديل موضع الحروف للرسائل النصية، ونحتاج في عملية التشفير إلى مفتاح (*key*) ويسمى مفتاح التشفير وهو عبارة عن مجموعة جزئية من البيانات تستخدم في عملية التشفير ويكون معلوم فقط لمرسل البيانات ومستقبلها، حيث تسمى عملية تشفير النص(*encipher*) وعملية حل الشفرة (*decipher*) وهي العملية العكسية لعملية التشفير أي تحويل النص المشفر(*Ciphertext*) إلى النص الصريح(*plaintext*).

(١-٢) التشفير الكتلي (*block cipher*):-

التشفير الكتلي هوعبارة عن دالة E المعرفة بالشكل $E : P \times K \to C$ حيث أن K هو مفتاح التشفير و P هو النص الصريح و C هو النص المشفر والدوال الاتية

$$E_K : P \to C$$

$$D_K : C \to P$$

حيث أن E_K دالة التشفير(*Encipher function*) و D_K دالة حل التشفير (*Decipher function*)وحيث أن $D = E^{-1}$ ، وبعبارة أخرى فإن الدالة E دالة قابلة للانعكاس.[4]

وهذا يعني أن التشفير الكتلي يُشفر على شكل قطع مع الاعتماد على مفتاح التشفير ، ومن أهم أنواع التشفير الكتلي هي تشفير الضرب (*product cipher*) وتشفير التزحيف (*Shift cipher*) وتشفير فستل (*feistel cipher*) وهو الذي سنركز عليه في بحثنا هذا.

(١-٣) تشفير فستل (*feistel cipher*) :-

أن المبدأ الأساسي لتشفير فستل هو أن النص الصريح يُقسم إلى نصفين وكل نصف يستخدم لتشفير النصف الأخر بعدد محدد من الدورات أو المراحل(*rounds*) والناتج هو النص المشفر المؤلف من قطعتين (نصفين) مشفرتين. [4]

ويعرف أيضاً على الشكل التالي:-

* النص الصريح يجب أن يكون طوله عدد زوجي $2n$.
* النص الصريح طوله m ، ويقسم إلى نصفين $m = (m_0, m_1)$.
* المفتاح K يقسم إلى مفاتيح جزئية $(k_1, k_2, ..., k_h)$.

* كل مفتاح جزئي يستخدم مع دالة f_{k_i} حيث $i=1,2,...,h$ كدالة تشفير من قطعة بمواصفات معينة إلى قطعة بمواصفات أخرى على أن يبقى الطول نفسه n .

* f_{k_i} هي دالة تشفير القطعة.

وحيث أن الرسالة m تُشفر h من المرات أو h دورة .[2].

ويمكن أن نعرف دالة التحويل f_{k_i} بالشكل الأتي :-

فاذا كانت B مجموعة القطع التي بطول b حيث b عدد صحيح و k_i عبارة عن مفتاح جزئي من مفتاح التشفير K ، فأن $f_k : B \to B$ بحيث أن $f_k(m) = m + k$ حيث m قطعة بطول b.

والان لنبين استخدام طريقة فستل لتشفير رسالة بطول m

المرحلة (الدورة) i حيث $i=1,2,...,h$

$\mu_{i-1} = (m_{i-1}, m_i) \Rightarrow \mu_i = (m_i, m_{i+1})$ حيث أن $m_{i+1} = m_{i-1} + f_{k_i}(m_i)$ فمثلاً المرحلة 1 تكون الأتي

$\mu_0 = (m_0, m_1) \Rightarrow \mu_1 = (m_1, m_2)$ وحيث أن $m_2 = m_0 + f_{k_1}(m_1)$ أي أن كل قطعة سوف تُشفر القطعة التي تليها حيث أن القطعة m_0 مع المفتاح k_1 شفرت القطعة m_1 إلى القطعة m_2 والقطعة m_1 مع المفتاح الجزئي k_2 تُشفر القطعة m_2 إلى القطعة m_3 وهكذا بالنسبة للبقية.

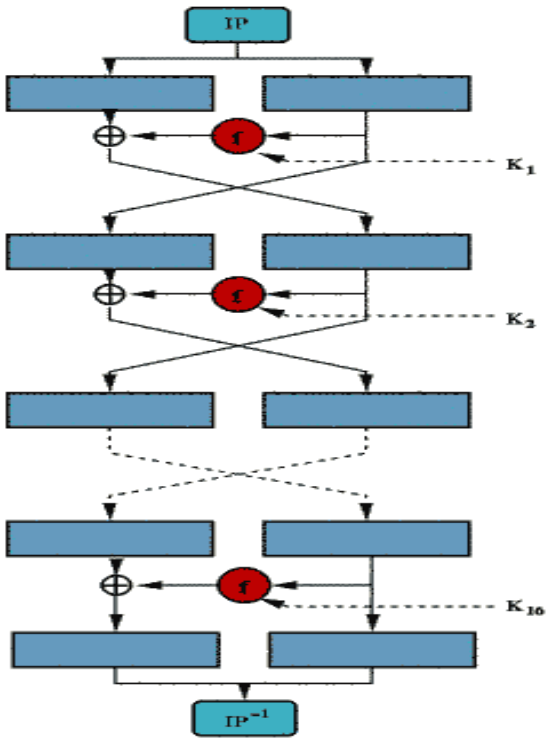
أما بالنسبة لحل الشفرة فيتم عن طريق القاعدة الاتية:

بما ان الرسالة التي تُشفر بطريقة فستل سيتم تشفيرها بـ h من الدورات فان عملية حل الشفرة تبدأ من المرحلة h ،

المرحلة (الدورة) i حيث $i=1,2,...,h$

$\mu_i = (m_{i+1}, m_i) \Rightarrow \mu_{i-1} = (m_i, m_{i-1})$ وحيث أن $m_{i-1} = m_{i+1} - f_{k_i}(m_i)$ فمثلاً المرحلة 4 تكون كالأتي $\mu_4 = (m_5, m_4) \Rightarrow \mu_4 = (m_4, m_3)$ وحيث ان $m_3 = m_5 - f_{k_4}(m_4)$ أي أن كل قطعة ستحل شفرة القطعة التي قبلها فالقطعة m_5 مع المفتاح الجزئي k_4 ستحل شفرة القطعة m_4 إلى القطعة m_3 والقطعة m_4 مع المفتاح k_3 تحل شفرة القطعة m_3 إلى القطعة m_2 وهكذا بالنسبة للبقية.

والشكل (١) يبن عملية التشفير بطريقة فستل [1] في حالة كون $h=16$



الشكل (١)

يبين الشكل أعلاه عملية التشفير لفستل حيث يتم في البداية تقسيم النص إلى نصفين نصف ايمن ونصف ايسر وبعد ذلك يتم استخدام دالة التحويل f_{k_i} مع المفتاح k_i على النصف الأيمن وجمعه مع النصف الأيسر والناتج من ذلك يمثل في المرحلة التي بعدها النصف الأيمن بينما النصف الأيمن في المرحلة الأولى يكون النصف الأيسر في المرحلة الثانية وهكذا حتى المرحلة ١٦.

ومما تقدم فأن طريقة فستل لا تشفر النصوص التي بطول فردي ومن هنا بدأنا في تعميم هذه الطريقة لتصبح عامة وتشفر كل النصوص وبأي طول كان فردياً أم زوجياً وذلك بمحاولة وضع تعريف جديد لها مع بعض الشروط الإضافية للتشفير ولحل التشفير.

(١-٤) معادلة نظام فستل المقترحة لحل مشكلة الطول الفردي للنصوص:-

لتكن M رسالة بطول m حيث m عدداً صحيحاً موجباً، وأنه بالإمكان كتابة m بالشكل الأتي $m = nb$ حيث أن كلاً من n, b عدداً صحيحاً موجباً و $n \geq 2$ عندما تكون m عددً غير أولي (لأنه في حالة كون m عدداً أولياً فأن n يجب أن تكون 1) ونقسم الرسالة بذلك إلى n من الأقسام بحيث نكتب $M = (m_0, m_1, ..., m_{n-1})$.

حيث أن كل قطعة m_i و $i = 0,1,...,n-1$ هي بطول b، و K مفتاح التشفير والذي بدوره يتكون من مفاتيح جزئية $k_1, k_2, ..., k_t$ وكل مفتاح جزئي k_i حيث $i = 1,2,...,t$ يعمل مع الدالة f كدالة تحويل f_{k_i} على مجموعة القطع التي

بطـول b، وأي رسـالة m تشـفر بـ $t-(n-2)$ مـن المراحـل (*round*) وحسب القاعدة الآتية:-

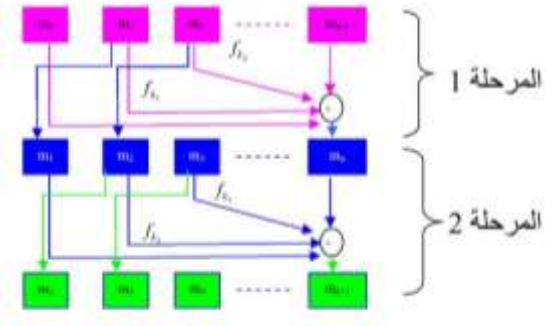
المرحلة i (التشفير)

$$(m_{i-1}, m_i, ..., m_{i-(n-2)}) \Rightarrow \mu_i = (m_i, m_{i+1}, ..., m_{i+(n-1)})$$

حيث ان

$$m_{i-1} = m_{i+(n-1)} - [f_{k_i}(m_i) + f_{k_{i+1}}(m_{i+1}) + ... + f_{k_{i+(n-2)}}(m_{i+(n-2)})]$$

والشكل (٢) يبين ذلك



الشكل (٢)

وتبدأ بالمرحلة 1 وتنتهي بالمرحلة $t-(n-2)$

أما حل الشفرة فيتحقق عن طريق عكس ترتيب قطع النص المشفر واستخدام المفاتيح الجزئية بترتيب معكوس أيضاً ولكون عدد المفاتيح الجزئيـة هـو t فـأن حـل الشـفرة يبـدأ مـن المرحلـة $t-(n-2)$ وحسب القاعدة الآتية :-

المرحلة i (الحل)

$$\mu_i = (m_{i+(n-1)}, m_{i+(n-2)}, ..., m_i) \Rightarrow \mu_{i-1} = (m_{i+(n-2)}, m_{i+(n-3)}, ..., m_{i-1})$$

حيث أن

$$m_{i-1} = m_{i+(n-1)} - [f_{k_i}(m_i) + f_{k_{i+1}}(m_{i+1}) + ... + f_{k_{i+(n-2)}}(m_{i+(n-2)})]$$

الجدول رقم (١)

الحرف	الرمز	الحرف	الرمز
a	٠	n	١٣
b	١	o	١٤
c	٢	p	١٥
d	٣	q	١٦
e	٤	r	١٧
f	٥	s	١٨
g	٦	t	١٩
h	٧	u	٢٠
i	٨	v	٢١
j	٩	w	٢٢
k	١٠	x	٢٣
l	١١	y	٢٤
m	١٢	z	٢٥

الجانب التطبيقي

لو كان لدينا النص الواضح "*transformations*" وكان لدينا المفتاح "product" فنتبع الخطوات الأتية للتشفير:

بما إن طول الرسالة هو $m=15$ فأننا وباستخدام التعريف المقترح لطريقة فستل نحاول كتابة m بالطريقة الأتية $m=nb$ بحيث أن n عدد غير أولي وبما انها عدد غير أولي في حالة كون m فأن $m=3\times5$ وعليه فأن $n=3$ و $b=5$، لذلك فأننا نكتب الرسالة بالشكل الأتي

$$M=(m_0,m_1,m_2) \Rightarrow M=(trans,\ forma,tions)$$

وباسـتخدام المفتـاح $K=$"*product*" والمتكـون مـن المفـاتيح الجزئية

$$k_1=p, k_2=r, k_3=o, k_4=d, k_5=u, k_6=c, k_7=t$$

وقاعدة التشفير الأتية وللمرحلة i

$$\mu_{i-1}=(m_{i-1},m_i,m_{i+1}) \Rightarrow \mu_i=(m_i,m_{i+1},m_{i+2})$$

$$\therefore \quad \mu_0=(m_0,m_1,m_2) \Rightarrow \mu_1=(trans,\ forma,ations)$$

يبدأ التشفير **بالمرحلة** $i=1$

$$\mu_0=(m_0,m_1,m_2) \Rightarrow \mu_1=(m_1,m_2,m_3)$$

$$\mu_0=(trans,\ forma,tions) \Rightarrow \mu_1=(\ forma,tions,m_3)$$

$$m_3=m_0+f_{k_1}(m_1)+f_{k_2}(m_2)$$

$$f_{k_1}(m_1)=\left\{\begin{array}{cccccc} m_1 & f & o & r & m & a \\ & 5 & 14 & 17 & 12 & 0 \\ k_1 + & 15 & 15 & 15 & 15 & 15 \\ \hline & 20 & 3 & 6 & 1 & 15 \\ & u & d & g & b & p \end{array}\right.$$

$$f_{k_2}(m_2)=\left\{\begin{array}{cccccc} m_2 & t & i & o & n & s \\ & 19 & 8 & 14 & 13 & 18 \\ k_2 + & 17 & 17 & 17 & 17 & 17 \\ \hline & 10 & 25 & 5 & 4 & 9 \\ & k & z & f & e & j \end{array}\right.$$

$$m_3=\left\{\begin{array}{cccccc} m_0 & t & r & a & n & s \\ & 19 & 17 & 0 & 13 & 18 \\ f_{k_1}(m_1) & u & d & g & b & p \\ & 20 & 3 & 6 & 1 & 15 \\ f_{k_2}(m_2) & k & z & f & e & j \\ & 10 & 25 & 5 & 4 & 9 \\ \hline & 23 & 19 & 11 & 18 & 16 \\ & x & t & l & s & q \end{array}\right.$$

$$\Rightarrow \mu_1=(m_1,m_2,m_3) \Rightarrow \mu_1=(\ forma,tions,xtlsq)$$

المرحلة $i=2$

$$\Rightarrow \mu_1=(m_1,m_2,m_3) \Rightarrow \mu_2=(m_2,m_3,m_4)$$

$$\mu_1=(\ forma,ations,xtlsq) \Rightarrow \mu_2=(tions,xtlsq,m_4)$$

$$m_4=m_1+f_{k_2}(m_2)+f_{k_3}(m_3)$$

$$f_{k_2}(m_2)=\begin{array}{|cccccc|}\hline m_2 & t & i & o & n & s\\ & 19 & 8 & 14 & 13 & 18\\ k_2 + & 17 & 17 & 17 & 17 & 17\\ \hline & 10 & 25 & 5 & 4 & 9\\ & k & z & f & e & j\\ \hline\end{array}$$

$$f_{k_3}(m_3)=\begin{array}{|cccccc|}\hline m_3 & x & t & l & s & q\\ & 23 & 19 & 11 & 18 & 16\\ k_3 + & 14 & 14 & 14 & 14 & 14\\ \hline & 11 & 7 & 25 & 6 & 4\\ & l & h & z & g & e\\ \hline\end{array}$$

$$m_3=\begin{array}{|cccccc|}\hline m_1 & f & o & r & m & a\\ & 5 & 14 & 17 & 12 & 0\\ f_{k_2}(m_2) & k & z & f & e & j\\ & 10 & 25 & 5 & 4 & 9\\ f_{k_3}(m_3) & l & h & z & g & e\\ & 11 & 7 & 25 & 6 & 4\\ \hline & 0 & 20 & 21 & 22 & 13\\ & a & u & v & w & n\\ \hline\end{array}$$

$$\Rightarrow \mu_2=(m_2,m_3,m_4)\Rightarrow \mu_2=(tions,xtlsq,auvwn)$$

المرحلة $i=3$

$$\mu_2=(m_2,m_3,m_4)\Rightarrow \mu_3=(m_3,m_4,m_5)$$

$$\mu_2=(tions,xtlsq,auvwn)\Rightarrow \mu_3=(xtlsq,auvwn,m_5)$$

$$m_5=m_2+f_{k_3}(m_3)+f_{k_4}(m_4)$$

$$f_{k_3}(m_3)=\begin{array}{|cccccc|}\hline m_3 & x & t & l & s & q\\ & 23 & 19 & 11 & 18 & 16\\ k_3 + & 14 & 14 & 14 & 14 & 14\\ \hline & 11 & 7 & 25 & 6 & 4\\ & l & h & z & g & e\\ \hline\end{array}$$

$$f_{k_4}(m_4)=\begin{array}{|cccccc|}\hline m_4 & a & u & v & w & n\\ & 0 & 20 & 21 & 22 & 13\\ k_4 + & 3 & 3 & 3 & 3 & 3\\ \hline & 3 & 23 & 24 & 25 & 16\\ & d & x & y & z & q\\ \hline\end{array}$$

$$m_5=\begin{array}{|cccccc|}\hline m_2 & t & i & o & n & s\\ & 19 & 8 & 14 & 13 & 18\\ f_{k_3}(m_3) & l & h & z & g & e\\ & 11 & 7 & 25 & 6 & 4\\ f_{k_4}(m_4) & d & x & y & z & q\\ & 3 & 23 & 24 & 25 & 16\\ \hline & 7 & 12 & 11 & 18 & 12\\ & h & m & l & s & m\\ \hline\end{array}$$

$$\Rightarrow \mu_3=(m_3,m_4,m_5)\Rightarrow \mu_3=(xtlsq,auvwn,hmlsm)$$

المرحلة $i=4$

$$\mu_3=(m_3,m_4,m_5)\Rightarrow \mu_4=(m_4,m_5,m_6)$$

$$\mu_3=(xtlsq,auvwn,hmlsm)\Rightarrow \mu_4=(auvwn,hmlsm,m_6)$$

$$m_6=m_3+f_{k_4}(m_4)+f_{k_5}(m_5)$$

$$f_{k_4}(m_4)=\begin{array}{|cccccc|}\hline m_4 & a & u & v & w & n\\ & 0 & 20 & 21 & 22 & 13\\ k_4 + & 3 & 3 & 3 & 3 & 3\\ \hline & 3 & 23 & 24 & 25 & 16\\ & d & x & y & z & q\\ \hline\end{array}$$

$$f_{k_5}(m_4)=\begin{array}{|cccccc|}\hline m_5 & h & m & l & s & m\\ & 7 & 12 & 11 & 18 & 12\\ k_5 + & 20 & 20 & 20 & 20 & 20\\ \hline & 1 & 6 & 5 & 12 & 6\\ & b & g & f & 1m & g\\ \hline\end{array}$$

$$m_6=\begin{array}{|cccccc|}\hline m_3 & x & t & l & s & q\\ & 23 & 19 & 11 & 18 & 16\\ f_{k_4}(m_4) & d & x & y & z & q\\ & 3 & 23 & 24 & 25 & 16\\ f_{k_5}(m_5) & b & g & f & m & g\\ & 1 & 6 & 5 & 12 & 6\\ \hline & 1 & 22 & 14 & 3 & 12\\ & b & w & o & d & m\\ \hline\end{array}$$

$$\Rightarrow \mu_4=(m_4,m_5,m_6)\Rightarrow \mu_4=(auvwn,hmlsm,bwodm)$$

المرحلة $i=5$

$$\mu_4=(m_4,m_5,m_6)\Rightarrow \mu_5=(m_5,m_6,m_7)$$

$$\mu_4=(auvwn,hmlsm,bwodm)\Rightarrow \mu_5=(hmlsm,bwodm,m_7)$$

$$m_7=m_4+f_{k_5}(m_5)+f_{k_6}(m_6)$$

$$f_{k_5}(m_4)=\begin{array}{|cccccc|}\hline m_5 & h & m & l & s & m\\ & 7 & 12 & 11 & 18 & 12\\ k_5 + & 20 & 20 & 20 & 20 & 20\\ \hline & 1 & 6 & 5 & 12 & 6\\ & b & g & f & 1m & g\\ \hline\end{array}$$

$$f_{k_6}(m_6)=\begin{array}{|cccccc|}\hline m_6 & b & w & o & d & m\\ & 1 & 22 & 14 & 3 & 12\\ k_6 + & 2 & 2 & 2 & 2 & 2\\ \hline & 3 & 24 & 16 & 5 & 14\\ & d & y & q & f & o\\ \hline\end{array}$$

مراحل وعليه فأننا سوف نبدأ من المرحلة 6 في عملية حل التشفير وكما يأتي:

النص المشفر هو

$$C=(m_6,m_7,m_8)\Rightarrow C=(bwody,eyqnh,hbkda)$$

وباستخدام المفتاح $K=$"product" والمتكون من المفاتيح الجزئية

$$k_1=p,k_2=r,k_3=o,k_4=d,k_5=u,k_6=c,k_7=t$$

وقاعدة حل التشفير الأتية وللمرحلة i

$$\mu_i=(m_{i+2},m_{i+1},m_i)\Rightarrow \mu_{i-1}=(m_{i+1},m_i,m_{i-1})$$

$$m_{i-1}=m_{i+2}-\left[f_{k_{i+1}}(m_{i+1})+f_{k_i}(m_i)\right]$$

المرحلة $i=6$

$$\mu_6=(m_8,m_7,m_6)\Rightarrow \mu_6=(hbkda,eyqnh,bwodm)$$

$$\mu_6=(m_8,m_7,m_6)\Rightarrow \mu_5=(m_7,m_6,m_5)$$

$$\mu_6=(hbkda,eyqnh,bwodm)\Rightarrow \mu_5=(eyqnh,bwodm,m_5)$$

$$m_5=m_8-\left[f_{k_7}(m_7)+f_{k_6}(m_6)\right]=m_8-f_{k_7}(m_7)-f_{k_6}(m_6)$$

$$f_{k_6}(m_6)=\begin{array}{|ccccc|}\hline m_6 & b & w & o & d & m\\ & 1 & 22 & 14 & 3 & 12\\ k_6+ & 2 & 2 & 2 & 2 & 2\\ \hline & 3 & 24 & 16 & 5 & 14\\ & d & y & q & f & o\\ \hline\end{array}$$

$$f_{k_7}(m_7)=\begin{array}{|ccccc|}\hline m_7 & e & y & q & n & h\\ & 4 & 24 & 16 & 13 & 7\\ k_7+ & 19 & 19 & 19 & 19 & 19\\ \hline & 23 & 17 & 9 & 6 & 0\\ & x & r & j & g & a\\ \hline\end{array}$$

$$m_5=\begin{array}{|ccccc|}\hline m_8 & h & b & k & d & a\\ & 7 & 1 & 10 & 3 & 0\\ f_{k_7}(m_7) & x & r & j & g & a\\ - & 23 & 17 & 9 & 6 & 0\\ f_{k_6}(m_6) & d & y & q & f & o\\ - & 3 & 24 & 16 & 5 & 14\\ \hline & 7 & 12 & 11 & 18 & 12\\ & h & m & l & s & m\\ \hline\end{array}$$

$$\Rightarrow \mu_5=(m_7,m_6,m_5)\Rightarrow \mu_5=(eyqnh,bwodm,hmlsm)$$

المرحلة $i=5$

$$\mu_5=(m_7,m_6,m_5)\Rightarrow \mu_4=(m_6,m_5,m_4)$$

$$\mu_5=(eyqnh,bwodm,hmlsm)\Rightarrow \mu_4=(bwodm,hmlsm,m_4)$$

$$m_4=m_7-f_{k_6}(m_6)-f_{k_5}(m_5)$$

$$f_{k_5}(m_5)=\begin{array}{|ccccc|}\hline m_5 & h & m & l & s & m\\ & 7 & 12 & 11 & 18 & 12\\ k_5+ & 20 & 20 & 20 & 20 & 20\\ \hline & 1 & 6 & 5 & 12 & 6\\ & b & g & f & m & g\\ \hline\end{array}$$

$$m_7=\begin{array}{|ccccc|}\hline m_4 & a & u & v & w & n\\ & 0 & 20 & 21 & 22 & 13\\ f_{k_5}(m_5) & b & g & f & m & g\\ & 1 & 6 & 5 & 12 & 6\\ f_{k_6}(m_6) & d & y & q & f & o\\ & 3 & 24 & 16 & 5 & 14\\ \hline & 4 & 24 & 16 & 13 & 7\\ & e & y & q & n & h\\ \hline\end{array}$$

$$\Rightarrow \mu_5=(m_5,m_6,m_7)\Rightarrow \mu_5=(hmlsm,bwodm,eyqnh)$$

المرحلة $i=6$

$$\mu_5=(m_5,m_6,m_7)\Rightarrow \mu_6=(m_6,m_7,m_8)$$

$$\mu_5=(hmlsm,bwodm,eyqnh)\Rightarrow \mu_6=(bwodm,eyqnh,m_8)$$

$$m_8=m_5+f_{k_6}(m_6)+f_{k_7}(m_7)$$

$$f_{k_6}(m_6)=\begin{array}{|ccccc|}\hline m_6 & b & w & o & d & m\\ & 1 & 22 & 14 & 3 & 12\\ k_6+ & 2 & 2 & 2 & 2 & 2\\ \hline & 3 & 24 & 16 & 5 & 14\\ & d & y & q & f & o\\ \hline\end{array}$$

$$f_{k_7}(m_7)=\begin{array}{|ccccc|}\hline m_7 & e & y & q & n & h\\ & 4 & 24 & 16 & 13 & 7\\ k_7+ & 19 & 19 & 19 & 19 & 19\\ \hline & 23 & 17 & 9 & 6 & 0\\ & x & r & j & g & a\\ \hline\end{array}$$

$$m_8=\begin{array}{|ccccc|}\hline m_5 & h & m & l & s & m\\ & 7 & 12 & 11 & 18 & 12\\ f_{k_6}(m_6) & d & y & q & f & o\\ & 3 & 24 & 16 & 5 & 14\\ f_{k_7}(m_7) & x & r & j & g & a\\ & 23 & 17 & 9 & 6 & 0\\ \hline & 7 & 1 & 10 & 3 & 0\\ & h & b & k & d & a\\ \hline\end{array}$$

$$\Rightarrow \mu_6=(m_6,m_7,m_8)\Rightarrow \mu_6=(bwodm,eyqnh,hbkda)$$

وبما أن طول مفتاح التشفير هو $t=7$ و $n=3$ فأن $t-(n-2)=7-(3-2)=6$ وهذا يجعل عدد مراحل التشفير هو 6 وبهذا فأن

$$C=E(transformations)=bwodmeyqnhhbkda$$

ولحل شفرة النص المشفر "bwodmeyqnhhbkda" وباستخدام المفتاح "product" فأننا نتبع الأتي:

لأن طول النص المشفر هو $m=15$ ولأن العدد 15 ليس عدداً أولياً إلا أنه بالإمكان كتابته بالشكل $m=nb$ بحيث ان n اصغر عدد صحيح و $n\geq 2$ ولهذا فأن $5\times 3=15$ وهذا يجعل $b=5$ و $n=3$ ولأن طول المفتاح هو $t=7$ فان هذا النص تم تشفيره بـ $t-(n-2)$ من المراحل وهي $7-(3-2)=6$

$$f_{k_6}(m_6)=\begin{array}{|cccccc|}\hline m_6 & b & w & o & d & m\\ & 1 & 22 & 14 & 3 & 12\\ k_6 + & 2 & 2 & 2 & 2 & 2\\ \hline & 3 & 24 & 16 & 5 & 14\\ & d & y & q & f & o\\ \hline\end{array}$$

$$m_4=\begin{array}{|cccccc|}\hline m_7 & e & y & q & n & h\\ & 4 & 24 & 16 & 13 & 7\\ f_{k_6}(m_6) & d & y & q & f & o\\ - & 3 & 24 & 16 & 5 & 14\\ f_{k_5}(m_5) & b & g & f & m & g\\ - & 1 & 6 & 5 & 12 & 6\\ \hline & 0 & 20 & 21 & 22 & 13\\ & a & u & v & w & n\\ \hline\end{array}$$

$$\Rightarrow \mu_4=(m_6,m_5,m_4)\Rightarrow \mu_4=(bwodm,hmlsm,auvwn)$$

المرحلة $i=4$

$$\mu_4=(m_6,m_5,m_4)\Rightarrow \mu_3=(m_5,m_4,m_3)$$

$$\mu_4=(bwodm,hmlsm,auvwn)\Rightarrow \mu_3=(hmlsm,auvwn,m_3)$$

$$m_3=m_6-f_{k_5}(m_5)-f_{k_4}(m_4)$$

$$f_{k_4}(m_4)=\begin{array}{|cccccc|}\hline m_4 & a & u & v & w & n\\ & 0 & 20 & 21 & 22 & 13\\ k_4 + & 3 & 3 & 3 & 3 & 3\\ \hline & 3 & 23 & 24 & 25 & 16\\ & d & x & y & z & q\\ \hline\end{array}$$

$$f_{k_5}(m_4)=\begin{array}{|cccccc|}\hline m_5 & h & m & l & s & m\\ & 7 & 12 & 11 & 18 & 12\\ k_5 + & 20 & 20 & 20 & 20 & 20\\ \hline & 1 & 6 & 5 & 12 & 6\\ & b & g & f & 1m & g\\ \hline\end{array}$$

$$m_3=\begin{array}{|cccccc|}\hline m_6 & b & w & o & d & m\\ & 1 & 22 & 14 & 3 & 12\\ f_{k_5}(m_5) & b & g & f & m & g\\ - & 1 & 6 & 5 & 12 & 6\\ f_{k_4}(m_4) & d & x & y & z & q\\ - & 3 & 23 & 24 & 25 & 16\\ \hline & 23 & 19 & 11 & 18 & 16\\ & x & t & l & s & q\\ \hline\end{array}$$

$$\Rightarrow \mu_3=(m_5,m_4,m_3)\Rightarrow \mu_3=(hmlsm,auvwn,xtlsq)$$

المرحلة $i=3$

$$\mu_3=(m_5,m_4,m_3)\Rightarrow \mu_2=(m_4,m_3,m_2)$$

$$\mu_3=(hmlsm,auvwn,xtlsq)\Rightarrow \mu_2=(auvwn,xtlsq,m_2)$$

$$m_2=m_5-f_{k_4}(m_4)-f_{k_3}(m_3)$$

$$f_{k_3}(m_3)=\begin{array}{|cccccc|}\hline m_3 & x & t & l & s & q\\ & 23 & 19 & 11 & 18 & 16\\ k_3 + & 14 & 14 & 14 & 14 & 14\\ \hline & 11 & 7 & 25 & 6 & 4\\ & l & h & z & g & e\\ \hline\end{array}$$

$$f_{k_4}(m_4)=\begin{array}{|cccccc|}\hline m_4 & a & u & v & w & n\\ & 0 & 20 & 21 & 22 & 13\\ k_4 + & 3 & 3 & 3 & 3 & 3\\ \hline & 3 & 23 & 24 & 25 & 16\\ & d & x & y & z & q\\ \hline\end{array}$$

$$m_2=\begin{array}{|cccccc|}\hline m_5 & h & m & l & s & m\\ & 7 & 12 & 11 & 18 & 12\\ f_{k_4}(m_4) & d & x & y & z & q\\ - & 3 & 23 & 24 & 25 & 16\\ f_{k_3}(m_3) & l & h & z & g & e\\ - & 11 & 7 & 25 & 6 & 4\\ \hline & 19 & 8 & 14 & 13 & 18\\ & t & i & o & n & s\\ \hline\end{array}$$

$$\Rightarrow \mu_2=(m_4,m_3,m_2)\Rightarrow \mu_2=(auvwn,xtlsq,tions)$$

المرحلة $i=2$

$$\mu_2=(m_4,m_3,m_2)\Rightarrow \mu_1=(m_3,m_2,m_1)$$

$$\mu_2=(auvwn,xtlsq,tions)\Rightarrow \mu_1=(xtlsq,tions,m_1)$$

$$m_1=m_4-f_{k_3}(m_3)-f_{k_2}(m_2)$$

$$f_{k_2}(m_2)=\begin{array}{|cccccc|}\hline m_2 & t & i & o & n & s\\ & 19 & 8 & 14 & 13 & 18\\ k_2 + & 17 & 17 & 17 & 17 & 17\\ \hline & 10 & 25 & 5 & 4 & 9\\ & k & z & f & e & j\\ \hline\end{array}$$

$$f_{k_3}(m_3)=\begin{array}{|cccccc|}\hline m_3 & x & t & l & s & q\\ & 23 & 19 & 11 & 18 & 16\\ k_3 + & 14 & 14 & 14 & 14 & 14\\ \hline & 11 & 7 & 25 & 6 & 4\\ & l & h & z & g & e\\ \hline\end{array}$$

$$m_1=\begin{array}{|cccccc|}\hline m_4 & a & u & v & w & n\\ & 0 & 20 & 21 & 22 & 13\\ f_{k_3}(m_3) & l & h & z & g & e\\ - & 11 & 7 & 25 & 6 & 4\\ f_{k_2}(m_2) & k & z & f & e & j\\ - & 10 & 25 & 5 & 4 & 9\\ \hline & 5 & 14 & 17 & 12 & 0\\ & f & o & r & m & a\\ \hline\end{array}$$

$$\Rightarrow \mu_1=(m_3,m_2,m_1)\Rightarrow \mu_1=(xtlsq,tions,forma)$$

المرحلة $i=1$

$$\mu_1=(m_3,m_2,m_1)\Rightarrow \mu_0=(m_2,m_1,m_0)$$

$$\mu_1=(xtlsq,tions,forma)\Rightarrow \mu_0=(tions,forma,m_0)$$

$$m_0=m_3-f_{k_2}(m_2)-f_{k_1}(m_1)$$

$$m_0 = \begin{array}{lccccc} m_3 & x & t & l & s & q \\ & 23 & 19 & 11 & 18 & 16 \\ f_{k_2}(m_2) & k & z & f & e & j \\ - & 10 & 25 & 5 & 4 & 9 \\ f_{k_1}(m_1) & u & d & g & b & p \\ - & 20 & 3 & 6 & 1 & 15 \\ \hline & 19 & 17 & 0 & 13 & 18 \\ & t & r & a & n & s \end{array}$$

$$f_{k_1}(m_1) = \begin{array}{lccccc} m_1 & f & o & r & m & a \\ & 5 & 14 & 17 & 12 & 0 \\ k_1 + & 15 & 15 & 15 & 15 & 15 \\ \hline & 20 & 3 & 6 & 1 & 15 \\ & u & d & g & b & p \end{array}$$

$$f_{k_2}(m_2) = \begin{array}{lccccc} m_2 & t & i & o & n & s \\ & 19 & 8 & 14 & 13 & 18 \\ k_2 + & 17 & 17 & 17 & 17 & 17 \\ \hline & 10 & 25 & 5 & 4 & 9 \\ & k & z & f & e & j \end{array}$$

$$\Rightarrow \mu_0 = (m_2, m_1, m_0) \Rightarrow \mu_0 = (tions,\ forma, trans)$$

$$\therefore \quad M = D(bwodmeyqnhhbkda) = transformation$$

وهذا هو النص الصريح "transformations"

المصادر

[1] Blaze, M. "A cryptographic File System for Unix", ACM conference on communications and computer security,1993.

[2] Delp,J.Edward. "An Introduction to Cryptography" School of Electrical and Computer Engeneering, West Lafeayette, Indiana, IMA Digital Libraries, February 14,2001.

[3] H. Feistel, "Cryptography and Computer Privacy," Scientific American, v. 228, n. 5, May 73, pp. 15-23.

[4] Mirza, Fauzan. "Block Ciphers and Cryptanalysis", Royal Hollway University of London, 1997.

[٥] بروس بوزورث، ترجمة الدبوني، ميثم محمد زكري، سليمان، أديب حمدون، سدخان، ستار بدر/ الدار العربية للطباعة/ الرموز والشفرات والحاسبات مقدمة إلى أمن المعلومات (١٩٨٩).

Feistel method to encrypt text with lengths of odd

Nazar Khalaf Hussein AL-Dikhil

Department of mathematics, College of Computer Sciences & Mathematics, University of Tikrit,Tikrit, Iraq

(**Received:** 10 / 8 / 2008 ---- **Accepted:** 15 / 12 / 2008)

Abstract

The method of Feistel method for encryption is one of the most important methods of Block Cipher, and the method is based on the encrypted text of even length, i.e this method requires that the length of the text to be encrypted in length an even, in this research we try to use the same method to encrypt the text of odd length in particular, and make the method public.