نگرش نخبگانی در مهندسی استخوان دانشگاه صنعتی اصفهان شماره 11 مهر 1371

(۷۱)

پیکالگوریتم جدید رمزگذار سریع داده‌ها

محمدرضا میرفاطحی

چکیده:

اگر چه الگوریتم رمزگذاری DES موجود دنیا محصول می‌شده‌است، اما نقاط ضعف مادهٔ آن نیز مورد توجه بوده و پیشنهاداتی برای رفع‌کردن آنها مطرح شده‌است. دو عیب مهم الگوریتم DES که روزنهای امیدی را برای شکستن آن گشته‌اند، به‌ترتیب به‌ویژه انتدازه‌ساختار تولید کلید‌های داده‌ی فرعي که به‌عبارت به‌سولت و سرعت در جستجوی فضای کلید می‌شود کذب وجود خواهد نامطلوب در جمع‌های جانشینی \((S)\) می‌باشد و در جگی‌های آماری اولویت را ارائه نمی‌دهد و در جگی‌های دیگر حمله به سیستم و شکستن آن می‌گشته‌اند.

در این مقاله با الهام از مزایای بارز الگوریتم DES الگوریتم جدیدی ارائه می‌شود که در آن در ساختار تولید کلید‌های فرعي تجدید نظر کلی و جدی به عمل آمده‌است. همچنین در آن امکان استفاده از کلید‌های با طول متغیر فراهم شده‌است، به‌طوری‌که حملهٔ جستجوی فضای کلید ناموفق می‌شود. اشکال‌های آزمایش‌هایی به‌جای انتخاب جمع‌های \(S\) قویتر خواهیم کرد و در پایان پیشنهاداتی برای تبدیل سرعت عمل‌هایی رمزگذار مطرح خواهیم شد.

۱- الگوریتم جدید FDE و بدلیل اساسی به‌كار رفتن در آن
گوریتم DES

\[\text{FDE}[\text{در برآورد ساختن میان‌برای انتخاب} \quad 2\text{در مورد DES}]\]

*دانشیار دانشگاه‌برق و کامپیوتر دانشگاه صنعتی اصفهان

**فاز/تحصیل کارشناسی ارشد دانشگاه‌برق و کامپیوتر دانشگاه صنعتی اصفهان

***مربی دانشگاه‌برق و کامپیوتر دانشگاه صنعتی اصفهان

1. قرار باقل است که خواندن‌های محرر با الگوریتم DES آشنا باشد کام دارد. مراجع [۱] [۱] باین منظور معرفی می‌شوند.

2. Fast Data Encryption

3. Shannon
یکی از روش های معمول انتقال دادن با به کارگیری متوالی تبدیلات جانشینی و نیز معمول انتقال تابع (FDE) از معرفی تبدیلات اساسی مورد استفاده در گروئیم است. هر گروه از تابع و میزان هریک از متغیرهای مشخص شده یک قابل 42 بیتی متن اصلی یا متن رمز شده توسط دو تابع R و L (زیرaccur می باشد) و راستی باشند که یا یک بیتی با وزن بیشتر نمایش داده می شود. تابع های X1، X2، X3 و فرمول های Z1، Z2 و قابلیت های زیر معرف کلیدهای فرمی 12 بیتی هستند. تبدیلات اساسی در گروئیم یکسروت زیرعریف می شوند:

\[ G_{X_{i+2},X_{i+1},X_i}(L,R) \overset{\Delta}{=} (L \oplus R \oplus X_i \oplus X_{i+1}, R \oplus X_i \oplus X_{i+2}) \]

\[ F_{X_{i+1},Z_i}(L,R) \overset{\Delta}{=} (S_{Z_{i+1}}^{-1}(P^{-1}(L)), P(S(Z_i(R))) \]

\[ G'_{X_{i+2},X_{i+1},X_i}(L,R) \overset{\Delta}{=} (L \oplus X_i \oplus X_{i+2}, R \oplus L \oplus X_i \oplus X_{i+1}) \]

\[ T(L,R) \overset{\Delta}{=} (R,L) \]

\[ h_1(L,R) \overset{\Delta}{=} (L,R) \]

که بیانکننده تقسیم یک قابل به دو زیرقابل سمت راستی و سمت چپ است. هریک از تبدیلات فوق معرکوس پذیرند و بسیاری می توان تحقیق کرد که معرکوس هریک از

<table>
<thead>
<tr>
<th>1. Diffusion</th>
<th>2. Confusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Substitution</td>
<td>4. Permutation</td>
</tr>
</tbody>
</table>
یک الگوریتم جدید برای زیرست

به صورت زیر است:

\[ G^{-1} x_{i+2} x_{i+1} x_i = G x_i, x_{i+1}, x_{i+2} \]  \hspace{1cm} (6)

\[ F^{-1} Z_{i+1} Z_i (L_R) = L (P Z_{i+1} (L), S Z_{i+1} (P^{-1} (R))) \]  \hspace{1cm} (7)

\[ G^{-1} x_{i+2} x_{i+1} x_i = G^{-1} x_i x_{i+1} x_{i+2} \]  \hspace{1cm} (8)

\[ T^{-1} (L_R) = T (L_R) \]  \hspace{1cm} (9)

\[ h^{-1} (L_R) = LR \]  \hspace{1cm} (10)

که به‌اختصار کنار گذاشته شده‌اند. تصاویر فرانک ایده‌زا و مهم و جالب است که اهمیت آنها پس از تغییرات معنوی الگوریتم FDE اشکال برنا می‌گیرد. این سه ویژگی عبارتند از:

\[ T \cdot G = G^{-1} \cdot T \]  \hspace{1cm} (11)

\[ T \cdot G^{-1} = G \cdot T \]  \hspace{1cm} (12)

\[ T \cdot F^{-1} Z_{i+1} Z_i = F Z_{i+1} \cdot T \]  \hspace{1cm} (13)

صحت رابطه (11) با توجه به شکل 1 واضح است.

رابطه (12) را می‌ترازی از روابط (11) و به صورت زیر الگوریتم کد:

\[ T \cdot G = G^{-1} \cdot T = T \cdot T \cdot G \cdot T \]  \hspace{1cm} (14)

و از نتیجه خواهیم داشت:

\[ T^{-1} = T \cdot G^{-1} \]
البته رابطه (12) نیز بسادگی و با استفاده از تعاریف اخیر به صورت زیر می‌پرسند:

\[ T \cdot F_{z_{i+1}z_i}^1 (L,R) = T(P(S_{z_{i+1}} (L)) , S_{z_i}^{-1}(P'(R))) \]

\[ = (S_{z_i}^{-1}(P'(R)), P(S_{z_{i+1}} (L))) \]

\[ = F_{z_{i+1}}^1 (R,L) \]

\[ = F_{z_{i+1}}^1 (T(L,R)) \]

\[ \Rightarrow T \cdot F_{z_{i+1}z_i}^1 = F_{z_{i+1}}^1 \cdot T \]

پس از آشنایی با تبدیلات اساسی فوق و بیانگری آنها، تبدیل رمزگذاری FDE را به صورت زیر تعریف می‌کنیم:
یک الگوریتم جدید رمزگذاری

\[ FDE \triangleq IP^{-1} \cdot h_1^{-1} \cdot G'_X \cdot x_4 \cdot x_3 \cdot x_2 \cdot z_2 \cdot G_3 \cdot x_4 \cdot x_1 \cdot x_0 \cdot \ldots \]

\[ G'_X \cdot x_4 \cdot x_3 \cdot z_2 \cdot x_3 \cdot x_2 \cdot x_1 \cdot T \cdot h_1 \cdot IP \]

(14)

به ترتیب چاپگشته‌های اولیه و نهایی پیدا و معکوس یکدیگرند.

به نمایش داده می‌شود. FDE در شکل 2 ساختار رمزگذاری

شکل 2 - ساختار رمزگذاری
استناد

از ویژگی‌های مهم و قابل توجه گروه‌بندی آن است که فرآیندهای رمزگذاری و FDE آن است که فرآیندهای رمزگذاری و DES (این مدل نخستین شیوه‌ای از الگوریتم گرفته‌شداست) صحت این ادعا با توجه به روابط زیر روش‌های می‌شود:

\[ FDE^{-1} = IP^{-1} \cdot h^{-1} \cdot T \cdot G^{-1} \cdot x_3 \cdot x_2 \cdot x_1 \cdot F^{-1} \cdot z_2 \cdot z_1 \cdot G^{-1} \cdot x_6 \cdot x_5 \cdot x_4 \cdot \]

\[ = IP^{-1} \cdot h^{-1} \cdot T \cdot G \cdot x_4 \cdot x_5 \cdot x_6 \cdot F^{-1} \cdot z_2 \cdot z_1 \cdot G^{-1} \cdot x_6 \cdot x_5 \cdot x_4 \cdot \]

\[ G \cdot x_4 \cdot x_5 \cdot x_6 \cdot F^{-1} \cdot z_2 \cdot z_1 \cdot G^{-1} \cdot x_6 \cdot x_5 \cdot x_4 \cdot \]

با اعمال روابط (11) و (12) به ترتیب و به دنبالین متعدد موارد می‌توان ارث تبدیل T را به مرحله بعدی منتقل کرد و در ترتیب رابطه نهایی برای FDE به صورت زیر به‌دست می‌آید:

\[ FDE^{-1} = IP^{-1} \cdot h^{-1} \cdot T \cdot G^{-1} \cdot x_4 \cdot x_5 \cdot x_6 \cdot F^{-1} \cdot z_2 \cdot z_1 \cdot G^{-1} \cdot x_6 \cdot x_5 \cdot x_4 \cdot \]

\[ G \cdot x_4 \cdot x_5 \cdot x_6 \cdot F^{-1} \cdot z_2 \cdot z_1 \cdot G^{-1} \cdot x_6 \cdot x_5 \cdot x_4 \cdot \]

مقایسه بین روابط (11) و (15) نشان می‌دهد که برای رمزگذاری و رمزگشائی به‌وسیله الگوریتم FDE، از روش‌بندی واحد استفاده می‌شود و فقط کانالی است ترکیب کلیدهای رجی 1، ظرفیت، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G، F، G，
یک الگوریتم جدید رمزگار

2- فرآیند تولید کلیدهای فرعي در دورهای متوالی الگوریتم FDE، مجموعاً 8 کلید فرعي بیکارگرفته می‌شوند که شامل 48 کلید 22 بیتی یعنی \( x_{22} \) و 36 کلید 16 بیتی یعنی \( x_{16} \) می‌باشند که از روي یک کلید اصلی و با روش مشخصی تولید و سپس بیکارگرفته می‌شوند. از جمله این کلید‌ها می‌توان به کلید‌های تولید کلیدهای فرعي اشاره داشته باشیم که از طریق‌های انتخاب و نظارت مراحلی تولید کلیدنده‌ها در دسترس هستند و تا به‌طور کلی در نهایت 28 بیت از کلید یک کلیدهای فرعي مایه‌تای 24 بیت از کلید اصلی ساخته شده‌اند. بهترین آنها برای استفاده مناسب‌ترین در عمل می‌توان با انتخاب پلت و سپس پدید کنند. به طوری که روش تولید کلیدهای فرعي مانند 24 بیت از کلیدهای فرعي که در نهایت 28 بیت هر کلید از کلیدهای فرعي 48 بیتی از روز یک کلید اصلی و در زمان پیکار کننده تولیدی دارند، با توجه به ضعف و همچنین به خطرناتای داشته که می‌تواند به همان شکسته‌ند. به انتخاب کافی و قابل اطمینان بیان شود و با پیشرفت تکنولوژی روزگار خطر نکته‌ست. منفی‌یابی

این نظریه در طراحی استخراج FDE به‌طور مورد توجه تاکید گرفته و سعی شد که واقعیتی که در فرآیند تولید کلیدهای فرعي به‌ویژه پیچیده زمان تولید آنها با روش پیشرفتی است، با کلیدهای فرعي را تولید، با روش پیشرفتی و خطر نیست. به دلیل نتایج این استیمی که با کلیدهای فرعي را تولید و در نهایت کافی و قابل اطمینان بیان شود و با پیشرفت تکنولوژی روزگار خطر نکته‌ست. منفی‌یابی

\[ \mathbb{P} [\text{ماها و } x_{22}] \text{ به طور مورد توجه تاکید گرفته و در نهایت کافی و قابل اطمینان بیان شود.} \]
روشن است که $$U_p$$ ها قابلیت ۳۴ بیتی و $$V$$ و $$V'$$ تالی به ۹۶ بیتی هستند.

اگر به ترتیب استفاده از کلیدهای فرعي در شکل ۲ دقت شود مشاهده می‌گردد که در حالت

$$
U_{2i} \triangleq (X_{2i+1}, X_{2i+2}) \quad i = 0, 1, ... , 7
$$

$$
U_{2i+2} \triangleq (X_{2i+3}, Z_{2i+1}, Z_{2i+2}) \quad i = 0, 1, ... , 5
$$

$$
U_{30-2i} \triangleq (X_{48-3i}, X_{47-3i}) \quad i = 0, 1, ... , 7
$$

$$
U_{29-2i} \triangleq (X_{48-3i}, Z_{30-2i}, Z_{29-2i}) \quad i = 0, 1, ... , 6
$$

$$
V \triangleq (X_{24}, Z_{16}, Z_{15}, X_{25})
$$

$$
V' \triangleq (X_{25}, Z_{16}, Z_{15}, X_{24})
$$

می‌توان روابط زیر را نوشت:

$$
C = FDE_{U_1, ..., U_{15}, V, U_{16}, ..., U_{30}} (P)
$$

$$
P = FDE_{U_{30}, ..., U_{16}, V', U_{15}, ..., U_1} (C)
$$

فرآیندی که برای تولید کلیدهای فرعي در نظر گرفته شده براساس وجود حافظه برای این کلیدها

می‌باشد. به‌طوری‌که در ابتدا عمل رمزگذاری با رمزگشایی توسط الگوریتم FDE، کلیدهای

فردی تولیدشده و در درون حافظه قرار می‌گیرند. حجم حافظه سودور باید بزرگ‌تر از مجموعه

کلیدهای فرعي باشد. ۱۶۴ بایت است به‌منظور خودداری از کارگیری مدارات‌ضبط برای تولید

کلیدهای فرعي از مدل‌های FDE برای تولید آنها استفاده می‌شود. الگوریتم ۱۲۸ بیتی

X پای به عنوان کلید اصلی و زیر تالی به ۶۴ بیتی سمت پایینی و سمت چپ آن پای به ترتیب

U و V در نظر گرفته شده و روند تولید کلیدهای فرعي به صورت زیر خواهد بود:

1. تولید کلیدهای فرعي به صورت زیر خواهد بود:
یک گوریتم جدید رمزگاری

\[ V = \text{Ch}(U) \] (19)

\[ U_1 = \text{FDE}_{Y, Y, ..., Y, Y, ..., Y}(X) \]

\[ U_2 = \text{FDE}_{U_1, Y, Y, ..., Y, Y, ..., Y}(X) \]

\[ U_3 = \text{FDE}_{U_1, U_2, Y, Y, ..., Y, Y, ..., Y}(X) \]

\[ \vdots \]

\[ U_{30} = \text{FDE}_{U_1, U_2, ..., U_{15}, U_{16}, U_{17}, ..., U_{29}, Y}(X) \]

روابط فوق نشان می‌دهند که برای تولید کلیدهای فرعي نیاز به 30 بار عمل رمزگاری FDE است و این همان نکته‌ای است که برای ناکام گذاشتن دهنم در حمله جستجوی فضای کلید در طراحی سیستم مجدد نظر ندارد.

سکه ۳ یک ساختار عملی برای تولید کلیدهای فرعي را نشان می‌دهد. این شکل خروجی‌های کد برای هر کنترل ورودی تعداد های کلید فرعي متصل می‌باشد و دنبالهای جدول 1 را تولید می‌کند. همچنین خط خشخاش بینگره فسر و اصلی این‌ها است که کلیدهای فرعي را با دست نگه می‌دارد. این شکل هنگامی که کلید ON یا OFF می‌گردد، دنباله‌ای جدول 1 به ترتیب تولید می‌شود و نتایجی است زمان بین تولید و در دنباله چرخه برای و در دنباله چرخه در دنباله حالت باید تا زمان فرعي باشد تا زمان تا زمان مورد نظر جدول 1 بیت سی و یکم صفرشده و باعث فلش شدن ساعت شماره‌ی و توقف تولید در دنباله‌ای جدول می‌شود. در حالت پلکس ورودی رمزگار تغییر وضعیت داده و FDE می‌گردد. آن‌ها در شکل 3 بیت M تعیین‌کننده نوع عمل رمزگاری برای تولید سی‌ویکم می‌باشد. مقدار M=1 باشد عمل رمزگاری و اگر M=0 باشد عمل رمزگاری صورت می‌گیرد.

این یکی که از نظر نیاز به بهترین مهارت FDE است که با استفاده از کلیدهای با طول معشوق است. کلیدهای که از طریق کانال امن بین فرستنده و دریافت می‌باشد می‌توانند طول معشوق بین ۴ تا ۱۵ حرف داشته باشند. همچنین یک حرف باید نشان داده کلید در کنار آنها قرار گیرد و لذا طول کلید دریافتی بین ۷ تا ۱۶ حرف است. بس از پرسی توزیع و معلوم شدن
عمل دیجیتالی \( M = 1 \) همراه با ساختار تولید کلید FDE

شکل ۳ - ساختار FDE

عمل رمزگذاری
یک الگوریتم جدید رمزگار... طول کلید کلید اصلی ۱۲۸ بیتی U از طریق اعمال یک تبدیل چاگشنت بر روی کلید دریافتی به صورتی که صفرهای انتهایی تعداد محتوا کلید (در مثالی که طول کلید کمتر از ۱۵ حرف است)...
جدول ۱: دنباله‌های خروجی کلید‌دار
<table>
<thead>
<tr>
<th></th>
<th>S_{32}</th>
<th>S_{31}</th>
<th>S_{30}</th>
<th></th>
<th>S_{3}</th>
<th>S_{2}</th>
<th>S_{1}</th>
<th>شماره‌یت</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td></td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>28</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>30</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>31</td>
</tr>
</tbody>
</table>

در کتاب هم ترجمه‌گردنبدهست آنده و در تعداد محورهای U ذیل می‌شود. در این ساختار، های توزیع و معمولین بیت‌های حرف اول (نشانگر طول کلید) که هیچک یک بیت‌های کلید مستقل FDE نیستند در تولید کلید‌های فرضی به کار می‌روند. اتخاذ کلید با طول معیار الگوریتم SDE بسب متن‌شدن بعد فضای کلید در یکی از اعداد ۲۶، ۳۷، ۴۳ و ۵۲. می‌شود (برای هر حرف کلید گیر از بیت توزیع باید در نظر گرفته‌می‌شود) برای مقایسه بعد فضای کلید و زمان جستجوی آن در نوع الگوریتم‌های FDE و FDE DES کلید تولید کلید‌های فرضی در مرحله گاز از پیکر فرض کلید انجام می‌شود که شامل FDE کلید استفاده می‌شود. در زمان عمل در مرحله گاز از پیکر فرض کلید انجام می‌شود که شامل FDE کلید استفاده می‌شود. در زمان عمل در مرحله گاز از پیکر فرض کلید انجام می‌شود که شامل FDE کلید استفاده می‌شود.
استقلال

ارولاً بسته به اهمیت‌کاری می‌توان بعد فضا کلید را برگزار یا کریچک انتخاب نمود و ثانیاً دشمن بعد
فضای کلید را یافته و انتخاب تصادفی بهداشت می‌باشد و جستجوی فضا کلید زمان بسیار
زیادی را آورا می‌طلبد و عمل را از شکست سیستم ماپورس می‌سازد.

[1] FDE

با توجه به آنکه ساختار معرفی شده برای رمزگار FDE سری می‌باشد، راحتی می‌توان از آن داشته باشد.

روش ابتدای لوله برای FDE در عمل و رمزگاری حداکثر استفاده را نمود و شکل 4 ترکه اسکری شده برای
براساس ابتدای لوله عمل می‌کند. نشان می‌دهد در این شکل متن اصلی به هر دو صورت حریر و
این لوله را وارد می‌گردد و متن رمزگاره نیز به همان دو صورت خارج می‌شود.

در این نتیجه، می‌توان از حراف استفاده می‌شود با یک شماره در میان 8 و 1=I تعداد مشابه.

این صورت بعد هشت افتقال، یک پلاس ساعت از شماره در اسقاب می‌گردد. همچنین این دو باید صورت حریر و
موازی - موازی و روزانه پاراگردیده و همچنین دو باید - موازی - سری خروجی نیز بارشوده، اگر انتقال
داده باشد. صورت این به وارد نظر باشد یا استخر شماره در 4 که و 0=I تعداد مشابه.

از این پیش آمده که ابتدای لوله در ساختار فوق استفاده شده است FDE با استرعت بسیار بالا (زمان
عمل ابتدایی 1) عمل می‌کند و این لحاظ بسیار شیبی به رمزگار بی‌پی بررسی است و از
مزایای عمله بهانه آین نوع رمزگارها و نیز می‌توان به هر دو یافته باشد. علایه از آنجا که
FDE قابل استفاده زمانی رمزگارهای قابلی را نیز دارد. به عنوان مثال FDE نیز ممانند
که وارد نیره به نوع دارد در یک از به‌همراه عمل

۲- معمورهه انتخاب ساختار تبدیل

دریخته 1 تبدیل F را به اعمال معیاری کردن و دیدن که این تبدیل مشکلی با لایه تکیه
پایه شده و نگرش مکس می‌پذیرد و S است که پروپر در زیر قابل و P

L به‌طور یدک حاکی از عمل می‌کند، ساختار کامل تبدیل F در شکل 5شان داده‌شده است. چاپ شده
یک پزشکی که روزانه پاراگردیده و مکس می‌شود (معنای مه‌های را نیز دارد.

که روی یک کالب 23 بی‌پی عمل می‌کند. جمع‌های چاپ‌شده


1. Pipeline
2. Shift Register
شکل 5 - ساختار تبدیل $F_{Z_{i+1}}, Z_i (L,R)$
یک الگوریتم جدید رمزگذاری

بت ورودی، 2 بت خروجی و 2 بت کلید هستند. در جعبه ی ببت ورودی شماره یک سطر و
1234
یک کلید شماره یک ستون از یک ماتریس
را مشخص می کنند. در ستون اولین ماتریس
یک چاپگشته به ظاهر تصادفی از اعداد 0 تا 15 وجود دارد و 4 بت خروجی جعبه نمایش باندی
فقط است که محل آن توسط ببت ورودی و کلید تبیین می شود. مکانیکی هر جعبه جانشینی
عبارت است از یک جعبه جانشینی که در ستون آن معکوس چاپگشته واقع در همان ستون از
جعبه اصلی وجود دارند. جعبه ها غیرخطی انتخاب می شوند و سپس می گیرند تا در انتهای
بنویسند دارای همانندی F می گیرند. اینجا نیز جعبه های S مشابه مقدمات DES از مهندس
پس از انتخاب می‌تواند به شکلی باشد که در نظر گرفته شود. بنابراین در انتخاب
معیار در انتخاب چین جعبه های کامل یک بودن آنها است. یک جعبه جانشینی شامل 4
بت خروجی به عنوان بابت ورودی استفاده می شود. بنابراین تعداد ساده ترین عبارت
یک بیاید خروجی از میان این 4 بت ورودی تعیین می‌شود. هر 2 بت خروجی در انتخاب
احتمال در انتخاب یک ترتیب دو بت ورودی تغییر نمی‌کند. تبیین مکانیکی است.

\[ V_i(X) \triangleq g(X) \oplus g(X_i) \] (21)

را بردار به‌هم‌گری گردید که در آن \( X \) و \( X_i \) در دو بارت ورودی هستند. فقط در بابت آمیزی یک کد بردار

\[ d_{ij} = \frac{1}{2^{m-1}} \sum_{X} \mathbb{1}(V_i(X)) \quad ; \quad 1 \leq i,j \leq m \] (22)

1. Complete
2. Avalanche Effect
3. Dependence Matrix
استلال

که در آن، رابطه بردار و مقدار نرخ‌های استماگر 1 = 1 باشند، بیت اام خروجی مقدار نرخ اندیکه 1/5 دارد. [A]

از دیگر رویکردهایی یک رمزگار خوب، مستقل بردن متغیرها بهم‌نیست، حسرت یک رمزگار جانشینی در این خاصیت باشگاه رمزگار نام 1 است [A].

انتخاب جمهوری مناسب جانشینی که درای ویژگی‌های فرق باشند از مسائل کلیدی است که در روش‌های انتخاب که با استفاده از توابع FDE به پیشنهاد می‌شود، پیشنهاد می‌شود. تولید تصویبی رای در این جمهوری و بررسی معنی‌داری فرق بروز آنها در نهایت انتخاب جمهوری مناسب، یک روش پیشنهادی برای دست‌یابی به جمهوری جانشینی خوب است.

نتیجه‌گیری

از آنچه که در مورد الگوریتم FDE گفته شد، نکات زیر حائز اهمیت‌اند:

1- با توجه به اینکه که در نهایت تولید کلید‌های فرعي نسبت به الگوریتم DES به عمل آمده‌است، استفاده توسعه کلید‌های فرعي در رابطه با کاهش حجم استفاده شده به طوری که از نظر زمان جستجو کامل فضای کلیدی می‌توان اثبات این الگوریتم نسبت بهDES (با فرض متوسط طول کلیدها) حداقل ۳۰ برابر شد.

2- از مزایای عمده FDE آن است که هر بیت از کلید‌های فرعي به تمام بیت‌های کلید اصلی است. داردو باتری‌ها با یک دور عمل رمزگاری به بیت متن رمزگذاری نیسته کلید با استفاده در مورد FDE طول کلید در الگوریتم متغیر است.

3- با استفاده FDE برای پرداگری از اینکه خط لوط مناسب بوده و با توجه به سرعت عمل بالا، تراشته FDE می‌تواند در سیستم‌های مختلف به جای رمزگارهای پی‌دپی‌دی گازی مورد استفاده قرار گیرد.

4- تراشته FDE با بهره‌گیری از آنکه فرق بیشتر در این الگوریتم می‌تواند با با ماتریس‌ها و با میزان، و با استفاده مناسب

1. Perfect
اختیارشوند. در خانم قریب تأکید مجید پر این لنگ که انتخاب و بستگی به جامعه جامعه‌گزاری جامعه‌گزاری با خواص مناسب در ساختار 
سپس می‌شود که این ساختار علاوه بر پیچیده‌تر و نمودن حمله جستجوی DES پر در شرایط آماری خوب (حداقل مشابه با) برخورد با پیش‌بازی خواندن‌گان و محققان دعوت می‌شود تا در ارزیابی و شکستن الگوریتم رمزگذاری پیشنهادی از نظرات کارشناسی خود ما با هم پرداختند.
astered

مراجع:

1. نعمتز حسنی، نقده و بررسی رمزگار DES، دانشگاه صنعتی اصفهان، 1368.


6. محمد ضعافی، "بخصوص رمزگاری"، قسمت اول، دانشکده برق دانشگاه صنعتی اصفهان، 1367.
