دوازدهمین کنفرانس بین‌المللی انجمن کامپیوتر ایران
دانشگاه شهید بهشتی، دانشکده مهندسی برق و کامپیوتر ،تهران، ایران، ۱ تا ۳ اسفند ۱۳۸۵

اریگامی و الگوریتم‌های رمزنگاری

مهدیه گرائیلو* سمیه تیمارچی† کیوان ناوی‡ مهسا گرائیلو§

چکیده

اریگامی یا هنر تا کردن کاغذ که در قدیم تنها به عنوان یک سرگرمی استفاده می‌شد، امروزه در بسیاری از کاربردهای عملی از جمله ستاره شناسی، ایجاد لنزهایی با حساسیت بالا، خم کردن فلزات، شبیه سازی سیستم‌های نوری و ... مورد استفاده قرار می‌گیرد. در این مقاله ما نشان خواهیم داد که مدل‌های اریگامی قابلیت این را دارند که به عنوان یک روش رمزنگاری مورد استفاده قرار گیرند که از مشخصه‌های مهم این روش، غیر خطی بودن، داشتن فضای کلید بسیار بزرگ و قابلیت پیاده‌سازی موازی می‌باشد. این روش جزو روش‌های رمزنگاری متقارن است بطوری که کلید، مستقل از متن رمز و متن ساده می‌باشد.

کلمات کلیدی

اریگامی، رمزنگاری، رمزگشایی، کلید عمومی، کلید خصوصی، رمزنگاری متقارن، رمز قطعه‌ای، رمز دنباله‌ای.

Origami and Encryption Algorithms

Mahdieh Grailoo Somayeh Timarchi Keivan Navi Mahsa Grailoo

Abstract

Origami, the art of folding paper, is only used for entertainment in the past. But nowadays, it is used in practical application such as deep-space astronomy, lens with highly sensitivity, bending-sheet metal processing, and simulation of optic systems. In this paper, it is presented that origami models can also be used in cryptography. Its important specifications are, being nonlinearity, having large key space, parallel implementation, symmetric cryptosystem that the key is independent of plaintext and ciphertext.

Keywords

Origami, encryption, decryption, public key, private key, symmetric cryptosystem, block cipher, stream cipher.

* دانشجوی کارشناسی ارشد معماری کامپیوتر دانشگاه شهید بهشتی، دانشکده برق و کامپیوتر، m_grailoo@std.sbu.ac.ir
† دانشجوی کارشناسی ارشد معماری کامپیوتر دانشگاه شهید بهشتی، دانشکده برق و کامپیوتر، s_timarchi@sbu.ac.ir
‡ عضو هیأت علمی دانشگاه شهید بهشتی، دانشکده برق و کامپیوتر، navi@sbu.ac.ir
§ دانشجوی کارشناسی نرم‌افزار کامپیوتر دانشگاه فردوسی مشهد، دانشکده کامپیوتر، ma_gr42@stu.um.ac.ir

۱- مقدمه

اریگامی یا «هنر تا کردن کاغذ»، شامل مدل‌های تا کردن کاغذ می‌باشد. در سه دهه اخیر، راه‌های توسعه زیادی برای طراحی مدل‌های اریگامی ایجاد شده است. به دنبال توسعه این مدل‌ها، از تکنیک‌های اریگامی در بسته‌بندی، گرافیک، طراحی و کاربردهای بسیار عملی‌تر و مفیدتر از جمله ساخت لنزها در تلسکوپ فضایی، ایجاد خمیدگی در فلزات و اپتیگامی و ... استفاده می‌شود [۳و۴].

در این مقاله استفاده از اریگامی در رمزنگاری فایل‌ها که آن را Cryptogami (رمزنگاری مبتنی بر مدل‌های اریگامی) نامیده‌ایم، پیشنهاد می‌شود. چندین روش Cryptogami در این مقاله ارائه شده است. در این روش‌ها با اعمال مدل‌های اریگامی به عنوان کلید خصوصی، فایل مورد نظر رمز می‌شود.

در این مقاله، بعد از مقدمه کوتاهی از رمزنگاری و کاربردهای اریگامی در بخش ۲، به ارائه روش‌های پیشنهادی در بخش ۳ می‌پردازیم. پیاده‌سازی نرم‌افزاری و سخت‌افزاری در بخش ۴ و نتیجه‌گیری در بخش ۵ آورده شده است.

۲- مبانی اریگامی و الگوریتم های رمزنگاری

۲-۱- مقدمه‌ای بر رمزنگاری

تکنیک‌ها و روش‌های مختلفی برای انجام رمزنگاری روی داده‌ها جهت جلوگیری از دسترسی غیر مجاز به اطلاعات وجود دارد. رمزنگاری به طور عمده به دو بخش رمزنگاری متقارن یا رمزنگاری با کلید خصوصی و رمزنگاری نامتقارن یا رمزنگاری با کلید عمومی تقسیم می‌شود. در رمزنگاری متقارن از یک کلید برای رمزنگاری و رمزگشایی استفاده می‌شود و یا کلید رمزگشایی به آسانی از روی کلید رمزنگاری بدست می‌آید. بنابراین این نوع سیستم هنگامی که کلیدها می‌توانند به یک روش قابل اعتماد و امن توزیع و ذخیره شوند؛ یا جایی که کلید بین دو سیستمی مبادله می‌شود که قبلا هویت یکدیگر را تایید کرده‌اند مورد استفاده قرار می گیرد.

دررمزنگاری نامتقارن از کلیدهای مختلفی برای رمزنگاری و رمزگشایی استفاده می‌کنند. فرستنده پیام، متن را با کلید عمومی کد می‌کند و گیرنده آن را با کلید اختصاصی خودش رمزگشایی می کند. رمزهای کلید خصوصی بر مبنای نوع عملکرد، چگونگی طراحی و پیاده‌سازی و کاربردهایشان به دو گونه رمزهای دنباله‌ای و رمزهای قطعه‌ای تقسیم می‌شوند [۱و۲].

۲-۲- اریگامی و کاربردهای آن

اریگامی یکی از کاردستی‌های محبوب ژاپنی‌هاست که معنای لغوی این کلمه در ژاپن «تا کردن کاغذ» یا «هنر تا کردن کاغذ» می‌باشد که تمام مدل‌های کاغذ و تا کردن را در بر دارد. هدف این هنر، آفریدن طرح‌های جالب از کاغذ با کمک تاهای هندسی می‌باشد. اصلی‌ترین شکل اریگامی، استفاده از یک کاغذ مربع شکل صاف است که باید مدل مورد نظر را بدون هیچ برشی روی کاغذ مربع، فقط با تا کردن ایجاد نمود؛ البته این محدودیت امروزه ضعیف‌تر شده است.

ایده‌ی ورود تکنیک‌های اریگامی و مفاهیم اساسی، درساخت و ایجاد تلسکوپ فضایی با کیفیت بالا مطرح شد. لنز این تلسکوپ‌ها دارای شیارها و لبه‌های مرزبندی شده و متحدالمرکز هست که روی ورق نازکی از شیشه و سیلیکا و پلاستیک با قابلیت خمیده شدن و تمرکز نور قلم زده شده است. این لنزها می توانند به صورت یک بسته، تا شوند تا حجم کمی را در یک وسیله پرتاب‌کننده به فضا اشغال کنند. همچنین استقرار این لنزها در فضا آسان است زیرا هم نازک هستند و هم پوسته صافی هستند که نیاز به پشتیبان بزرگ و سنگین (موتورها) ندارند [۳] .

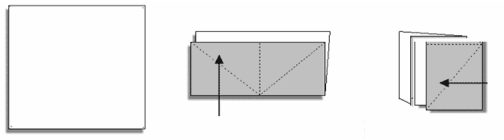
کاربرد دیگر اریگامی در اپتیگامی می‌باشد که در آن با توجه به مدل‌های اریگامی به طراحی سیستم‌های نوری می‌پردازند که در آن ترکیبی از انعکاس‌ها برای همگراسازی و یا واگراسازی وجود دارد [۴].

همچنین زمزمه‌هایی در مورد Ultra-mobile PC وجود دارد که ماکروسافت آن را توسعه داده است. این کامپیوتر یک Tablet PC خیلی سبک با قابلیت touch screen و یک صفحه ″۷ می‌باشد که یک Origami Device تلقی می‌شود.

۳- روش‌های پیشنهادی

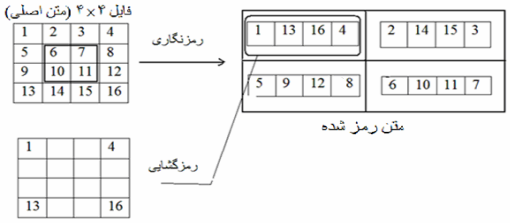
۳-۱- Cryptogami جایگشتی

روش پیشنهادی این مقاله، استفاده از مدل‌های اریگامی در رمزنگاری فایل‌ها می‌باشد. در اینجا یک فایل را به صورت ماتریس $m \times n$ در نظر می‌گیریم که هر خانه ماتریس می‌تواند حاوی w بیت باشد. برای سادگی ارائه روش، فرض می‌کنیم که هر خانه‌ی ماتریس حاوی اطلاعات یک بیتی می‌باشد. به عنوان مثال مدل اریگامی ساده مربع چهار لای شکل (1) را در نظر بگیرید. چنانچه بخواهیم از این مدل در رمزنگاری فایل‌ها استفاده کنیم، ابتدا فایل مورد نظر را باید به ماتریس s×s تبدیل کنیم.



شکل (۱) : مدل اریگامی مربع ۴ لا با ۲ تای بالا و چپ

با توجه به مدل اریگامی «مربع چهار لا» در نهایت فایل به یک ماتریس $s/2 \times s/2$ تبدیل می‌شود که در آن هر خانه ماتریس جدید حاوی اطلاعات ۴ بیتی می‌باشد. مثالی از رمزنگاری و رمزگشایی یک فایل ۴×۴ در شکل (۲) نشان داده شده است.

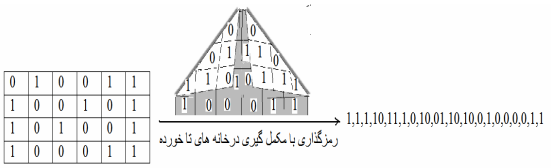


شکل (۲) : روش رمزنگاری با مدل اریگامی شکل (۲)

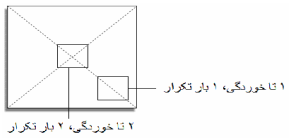
۳-۲- Cryotogami نمایی

با اعمال تغییرات در روش Cryptogami جایگشتی معرفی شده در بخش ۳-۱، می‌توان روش مذکور را از حالت جایگشتی خارج نمود. مثلا یک روش پیشنهادی این است که هر خانه در محل تا خوردگی، مکمل شود. چنانچه در این دستگاه رمزنگاری، از روش مکمل‌گیری بیت‌ها در محل تا خوردگی‌ها استفاده شود، در حمله «فقط با متن رمز» چون حمله کننده و در واقع نفر سوم که متن رمز شده را دریافت می‌کند، از محل بیت‌های مکمل شده اطلاعی ندارد (چون محل تا خوردگی ها را نمی‌داند)، در نتیجه باید در هر مرحله بیت‌هایی را مکمل کرده و تمام جایگشت‌های آن را به دست آورد. چون تعداد i، بیت‌های مکمل شده مشخص نیست، عملا همه حالت‌های ممکن که با N بیت می‌توان ساخت، یعنی 2^N حالت، باید امتحان شود. همانطور که از محاسبات بر می‌آید در یک ایده مکمل گیری ساده، روش مذکور غیر خطی یا نمایی می‌شود شکل (۳).

روش پیشنهادی دیگر برای خارج شدن از حالت جایگشتی، این است که تعداد تا خوردگی روی هر خانه از فایل، تعداد تکرار محتویات آن خانه را مشخص نماید شکل (۴).

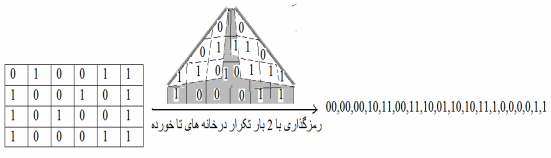


شکل (۳) : رمزنگاری با مدل اریگامی تای موشکی و مکمل گیری در خانه های تا خورده



شکل (۴): رمزنگاری Cryptogami با تکرار به تعداد تا خوردگی در محل تا

می‌توان برای سادگی بدون توجه به تعداد تاخوردگی، خانه‌های مورد نظر در محل تاهای قطری را به تعداد ثابت t، تکرار نمود شکل(۵). اکنون روشی را در نظر می‌گیریم که علاوه بر مکمل‌گیری، تعداد t بار تکرار در خانه‌های با تای قطری را نیز داشته باشیم. در نتیجه نفر سوم در حمله «فقط با متن رمز» چون کلید و در نتیجه تعداد تکرار را نمی‌داند؛ باید همه حالات یک بار تکرار ، دو بار تکرار و ..



شکل (۵) : رمزنگاری با مدل اریگامی تای موشکی و ۲ بار تکرار در خانه‌های تا خورده

را در نظر بگیرد. برای محاسبه کل حالات، ابتدا فرض می‌کنیم یکی از بیت‌های متن رمز شده ناشی از تکرار است و باید حذف شود در این حالت $N-1$ بیت باقی می‌ماند که با توجه به توضیح مورد قبل، 2^{N-1} حالت باید امتحان شود. سپس فرض می‌کنیم دو تا از بیت‌های متن رمز شده ناشی از تکرار است و باید حذف شود؛ در این حالت $N-2$ بیت باقی می‌ماند که تعداد حالات آن 2^{N-2} می‌شود و ... در نهایت داریم:

$$2^N + 2^{N-1} + 2^{N-2} + 2^{N-3} + \ldots = \sum_{t=0}^{L} 2^{N-t} = 2^{N+1}$$

با توجه به انواع مدل‌های اریگامی معرفی شده، مشاهده می‌شود که در این مدل‌ها لزوما نباید فایل به صورت ماتریس مربعی باشد و می‌توان آنها را به ابعاد $m \times n$ در نظرگرفت که در صورت مشخص نبودن m و n، تعداد حالات درحمله «فقط با متن رمز» برای محاسبه متن اصلی از روی متن رمز شده، افزایش می‌یابد. روش پیشنهادی دیگر برای افزایش تعداد حالات، تقسیم فایل متن اصلی به تعداد B بلاک (که B می‌تواند مستقل یا وابسته به طول بافر باشد) و رمز کردن هر بلاک بطور جداگانه با مدل‌های اریگامی می‌باشد. در صورت بلاک-بندی یک فایل به طول N و رمز کردن هر بلاک بطور جداگانه با مدل اریگامی و مساوی در نظر گرفتن طول بلاک‌ها، تعداد بلاک‌ها می‌تواند با پارامتر B ارسال شود. برای محاسبه همه‌ی حالات شامل حالت یک بلوکه و دو بلوکه و ... خواهیم داشت :

$$2^N + 2\times 2^{N/2} + 3\times 2^{N/3} + 4\times 2^{N/4} + \ldots = \sum_{b=0}^{N} b\times 2^{N/b}$$

در نتیجه در این دستگاه رمزنگاری، کلید از یک مدل اریگامی و یک ۵ تایی (n,m,i,t,B) به‌عنوان جزء ثانویه کلید، تشکیل شده است.

۳-۳- اریگامی و قالب‌بندی

در بسیاری از روش‌های قطعه‌ای یا قالبی معمولا از طول قالب‌های یکسان و به صورت پشت سر هم استفاده می‌شود که این قالب بندی به شیوه متداول را، نوعی پیش پردازش روی متن اصلی، برای اعمال توابع رمزنگاری به حساب می‌آوریم. حال اگر روشی بکار برده شود که نوعی قالب‌بندی انجام دهد که قالب‌ها لزوما دارای طول یکسان نباشد و علاوه بر آن در انتخاب قالب، محدودیت انتخاب پشت سر هم بیت‌ها به عنوان یک قالب، وجود نداشته باشد، این پیش پردازش می‌تواند باعث افزایش پیچیدگی روش رمزنگاری شود. در این روش مدل‌های

اریگامی قالب‌هایی را ایجاد می‌کنند که با توجه به شکل، بیت‌های هر قالب از نقاط مختلف فایل انتخاب می‌شود و طول قالب‌ها در یک فایل لزوما مساوی نیستند (شکل (۶)).

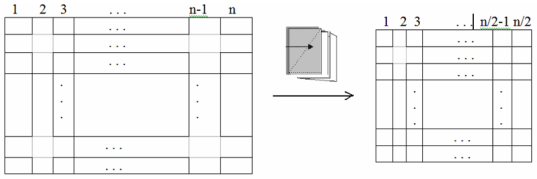
شکل (۶) : ایجاد قالب هایی با طول مختلف با مدل های اریگامی

در این صورت می‌توان در هر روش رمزنگاری متقارن یا نامتقارن که در آن به نوعی از قالب‌بندی یا بلوک‌بندی استفاده می‌شود، از مدل-های اریگامی به عنوان پیش پردازش استفاده نمود.

۴- پیاده‌سازی سخت‌افزاری و نرم‌افزاری

۴-۱- پیاده‌سازی نرم‌افزاری

در حالت کلی می‌توان فایل را به صورت $n \times n$ در نظر گرفت که در این حالت پیاده‌سازی نرم‌افزاری برای اعمال مدل اریگامی شکل (۱) به صورت شکل (۷) می‌شود. که در آن p فایل متن اصلی و C فایل رمز شده است بطوریکه هر خانه C شامل ۴ خانه از p می‌باشد.




```
For ( i=1  to  n/2 )
  For (j=1 to n/2 )
     {        C[ i,j ] ← P[ i,j ]   ,
              P[ n-i+1,j ]      ,
              P[ n-i+1,n-j+1 ] ,
              P[ i,n-j+1 ]      ;        }
```

شکل (۷) : پیاده‌سازی نرم‌افزاری رمزنگاری با مدل اریگامی شکل (۱)

۴-۲- پیاده‌سازی سخت‌افزاری

چنانچه C ماتریس متن رمز شده، P ماتریس متن اصلی، AC آدرس خانه‌های C و AP آدرس خانه‌های P باشد؛ روش Cryptogami شامل انتقال‌های w بیتی $C[AC] \leftarrow P[AP]$ می‌باشد.

$AC_{1,1}$	$AP_{1,1}$	$AP_{n,1}$	$AP_{n,n}$	$AP_{1,n}$
$AC_{1,2}$	$AP_{1,2}$	$AP_{n,2}$	$AP_{n,n-1}$	$AP_{1,n-1}$
.	.			.
.	.			.
.	.			.
$AC_{n/2,n/2}$	$AP_{n/2,n/2}$	$AP_{n/2+1,n/2}$	$AP_{n/2+1,n/2+1}$	$AP_{n/2,n/2+1}$

شکل (۸): Lookup table برای پیاده‌سازی سخت افزاری شکل (۱)

پیاده‌سازی سخت‌افزاری برای رمزنگاری فایل p شامل مدار تولید آدرس‌های AP و AC است زیرا بسته به مدل اریگامی بکار رفته در انتقال‌های w بیتی، AP و AC تغییر می‌کنند. برای بالا بردن سرعت می‌توان از Lookup table با مساحت $n \times n \times a$ استفاده کرد (a طول آدرس می‌باشد). Lookup table اریگامی شکل (۱) به صورت شکل (۸) می‌باشد. در ضمن این روش‌ها را می‌توان به صورت موازی نیز پیاده‌سازی نمود؛ زیرا خانه‌هایی که در اثر تا خوردگی روی هم قرار می‌گیرند را می‌توان مستقل از هم و به صورت موازی در خانه‌های متناظرشان در متن رمز شده قرار داد.

۵- مقایسه و نتیجه گیری

این روش دارای فضای کلید بسیار بزرگ است که در آن امنیت این روش مستقل از طول کلید است. یعنی افزایش یا کاهش طول کلید، امنیت آن را افزایش یا کاهش نمی‌دهد. همچنین کلید کاملا مستقل از متن ساده و متن رمز می‌باشد. تابع رمزنگاری یک به یک است زیرا به ازای اعمال مدل اریگامی خاص (کلید) روی متن اصلی، فقط یک متن رمز شده به دست می‌آید و با اعمال آن مدل اریگامی خاص (کلید) روی همان متن رمز شده، فقط یک متن ساده متناظر با متن اصلی به دست می‌آید. در این روش با تغییر رمزنگاری تاهای قطری مثلا استفاده از هر روش دیگر روی تاهای قطری اعم از مکمل‌گیری، روش رمزنگاری سزار و ... می توان آن را از حالت جایگشتی و در نتیجه خطی بودن خارج نمود. در مقایسه با روش‌های جایگشتی، خطی آفینی، DES و ... نمایی بودن این روش از مزایای آن به شمار می‌آید.

چنانچه روش‌های مذکور به عنوان سیستم رمزنگاری مستقل بکار رود جزء سیستم‌های متقارن به شمار می‌آیند زیرا کلید رمزنگاری و رمزگشایی به آسانی از روی هم بدست می‌آیند. این روش‌ها قابل پیاده‌سازی به صورت موازی می‌باشند. به علت تشابه این روش با روش‌های قالبی و نیز دارا بودن مزیت طول قالب متغیر و قالب‌گیری از خانه‌های مختلف متن اصلی، می‌توان مزایای روش‌های قالبی را به این روش افزود. با توجه به اینکه رمزهای قطعه‌ای از جمله پرکاربردترین رمزهای کلید خصوصی هستند و به علت قابلیت‌های فراوان که در اجرای سریعتر و برقراری امنیت و ایجاد مقاومت در برابر انواع حملات «متن انتخاب شده» و سایر انواع حمله های رمزنگاری دارند، یکی از بهترین گزینه‌ها در ایجاد اهداف طرح‌های رمزنگاری می‌باشند [۲].

مراجع :

[1] A. Menezes, P. Van Orschot, and S.Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
[2] Johannes A. Buchmann, "*INTRODUCTION TO CRYPTOGRAPHY*",ACM Press,2000
[3] Lawrence Livermore National Laboratory, "A Giant Leap for Space Telescope", S&TR March 2003 Foldable Optic.
[4] Jon H. Myer, " Optigami—A Tool for Optical System Design", Applied Optics, vol. 8, no. 2, p. 260, 1969.Mats Hagberg and Robert J. Lang, US Patent 6, 542, 529, Folded-Cavity, Broad Area Laser Source, April 1, 2003.