الگوریتم جدید برای رمزنگاری متن، مقاوم در برابر حمله بر اساس فرکانس حروف

یعقوب خراسانی[۱] , میثم بیات[۲]

۱-دکتری تخصصی گروه مخابرات دانشگاه شهید ستاری

۲-دانشیار گروه مخابرات دانشگاه شهید ستاری

چکیده

امروزه امنیت اطلاعات در کانال های ارتباطی از اهمیت فراوانی برخوردار ا ست و هرچه حسا سیت اطلاعات بالاتر با شد، امنیت نیز به همان نسبت اهمیت بالاتر پیدا خواهد کرد. از دیرباز تا کنون الگوریتم های مختلف رمزنگاری، برای تامین امنیت ارتباط مطرح شدند و سازمان های مختلف بر اساس میزان حساسیت اطلاعات، از الگوریتم های مختلف رمزنگاری اســتفاده می‌کنند. اطلاعات را می توان به انواع مختلف دســته بندی کرد. اطلاعات متنی یکی از متنوع ترین، نوع های اطلاعات است که در صورت وجود طبقه بندی اهمیت آن نیز بیشتر می شود. در این مقاله بر اساس الفبای ۲۸ کارکتری روش جدیدی برای رمزنگاری ارائه می‌گردد که دارای امنیت و ســرعت بالا و مقاوم در برابر حمله بر اســاس فرکانس حروف ا ست. نتایج آزمای شگاهی ن شان‌دهنده مقاومت ب سیار بالای این الگوریتم در مقابل حمله جامع به کلید ا ست. نیاز حمله کننده به حافظه ب سیار زیاد که عملا غیر قابل د سترس ا ست، علت دیگری برا ستحکام این الگوریتم می‌با شد. با توجه به الگوریتم تولید کلید در این روش، می توان اطمینان حاصل کرد که این الگوریتم در مقابل حمله در میانه راه (Meet in the middle) نیز بسیار مقاوم است.

کلمات کلیدی: اطلاعات، رمزنگاری، حمله جامع به کلید، حمله در میانه راه، حمله بر اساس فرکانس حروف

A new algorithm for text encryption, resistant to letter frequency attacks

Yaghoub Khorasani[1], Mayasam Bayat[2]

1-Phd Department of Electrical Engineering, Shahid Sattari University of Aeronautical Engineering, Tehran, Iran

2-Associate Professor of communication Engineering,Shahid Sattari Aeronautical University of Science and technology

Abstract

Today, the security of information in communication channels is of great importance, and the higher the classification of information, the higher the importance of security. From a long time ago, various encryption algorithms were proposed to ensure communication security, and different organizations use different encryption algorithms based on the sensitivity of the information. Information can be classified into different types, textual information is one of the most diverse types of information, which becomes more important if there is a classification. In this article, based on the 28-character alphabet, a new encryption method is presented, which has high security and speed, and is resistant to attacks based on the frequency of letters. Laboratory results show a very high resistance of this method against a comprehensive attack. The attacker's need for a lot of memory, which is practically inaccessible, that is another reason for the robustness of this algorithm. Given the key generation algorithm in this method, it can be ensured that this algorithm is also very resistant to attack in the middle.

Keywords: information, cryptography, comprehensive attack, attack in the middle Attack based on letter frequency

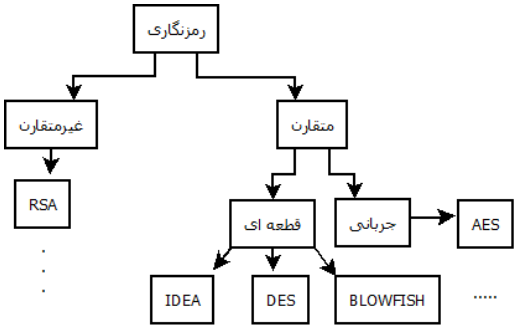
ایمیل نویسنده مسئول: **yaghoubkhorasani@gmail.com**

۱ـ مقدمه

رمزنگاری یکی مباحث اساسی مخابرات به شمار می رود. رمزنگاری مدرن را می‌توان به دو گروه رمزنگاری متقارن (symmetric cipher)و رمزنگاری نامتقارن(asymmetric cipher) تقسیم کرد. در رمزنگاری متقارن معمولا از یک کلید و یا مشتقات آن در رمزگذاری و رمزگشایی استفاده می شود. این در حالی است که در رمزنگاری نامتقارن کلیدهای متفاوتی در رمزگشایی و رمزنگاری مورد استفاده می گردد[۱-۴].

الگوریتم های رمزنگاری را می توان به دو دسته اصلی تقسیم کرد.۱-رمز های قطعه ای(Block cipher) ۲-رمزهای جریانی(stream cipher).

اغلب رمزهای قطعه ای مبتنی بر ساختار فایستل هستند و قطعات ورودی را در چند مرحله، ساده و پردازش می کنند که به هر مرحله یک دور میگوند و معمولا در هر دور اعمال ساده ای همچون جایگشت و جایگزینی استفاده می گردد[۵]



تصویر۱-انواع الگوریتم های رمزنگاری

ایده جایگزینی و جانشینی در رمزنگاری در سال ۱۹۴۹ توسط شانون مطرح گشت که بر اساس آن جدول s box برای جانشینی و جدول p box برای جایگزینی ارائه شد.

یکی از معروف ترین الگوریتم های رمزنگاری متقارن الگوریتم DES است. این الگوریتم مبتنی بر ساختار فایستل است و در سال ۱۹۷۶ توسط شرکت IMB تحت عنوان استاندارد رمزنگاری داده(Data Encryption Standard) تصویب گردید. این الگوریتم در سال ۱۹۹۸ پس از ۲۳ ساعت به وسیله حمله جامع به کلید شکسته شد[۵-۷]

از معایب DES می توان به طول کوتاه کلید و box sهای مرموز نام برد.پس از DES الگوریتم های 3DES,2DES مطرح گردید که به ترتیب دارای ضعف در مقابل حمله در میانه راه و پیچیدگی پیاده سازی بودند[۸, ۹]

در سال ۲۰۰۰ ریندال (RIJNDAEL) الگوریتم جدیدی را به عنوان استاندارد پیشرفته رمزنگاری داده (AES) ارائه داد. این الگوریتم با طول کلید ۱۲۸،۱۹۲ و ۲۵۶ بیتی ،با طول داده ۱۲۸ بیتی و در دورهای ۱۰،۱۴ و ۱۴ دوری معرفی گردید. این الگوریتم بر خلاف الگوریتم DES مبتنی بر ساختار فایستل نمی باشد. این الگوریتم دارای استحکام بسیار بالایی است و تا کنون هیچ حمله موفقی برای این الگوریتم ارائه نشده است[۱۰-۱۲]

در این مقاله روشی ارائه می گردد که متن را به صورت قطعه ای دریافت می‌کند و در دستخ الگوریتم های رمز های قطعه ای (Block cipher) قرار دارد. این الگوریتم برای الفباهای ۲۸ عضویی مناسب است (الفبای لاتین). این الگوریتم از طبقه های مختلف تشکیل شده و در هر طبقه امنیت داده نسبت به طبقه قبل بیشنر می‌شود.

در بخش ۲، روش پیشنهادی مطرح می گردد. بخش ۳، نتایج آزمایشگاهی مطرح می شود و نهایتا در بخش آخر به نتیجه گیری پرداخته می‌شود.

۲ـ روش پیشنهادی

متن یکی از انواع متداول اطلاعات است که برای تامین امنیت آن الگوربتم های رمزنگاری متعددی ارائه شده است[۱۳-۱۶]. قبل ارائه روش پیشنهادی فرض شود که پیام ورودی متنی به زبان انگلیسی است که حروف الفبای آن شامل۲۶ حرف است و با اضافه کردن علامت فاصله، نقطه و یک کارکتر دیگر مثل ویرگول، الفبا مورد نظر شامل ۲۹ حرف می شود و می توان هر یک از حروف الفبا به عددی بین ۰ الی ۲۸ نگاشت کرد. متن ورودی به قطعاتی حداقل ۱۴ کاراکتری تقسیم می‌شود.

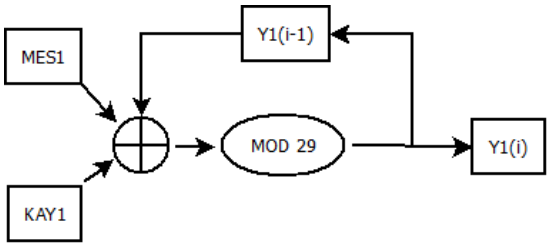
طول کلید نیز همسان با طول یک قطعه از پیام، در نظر گرفته می‌شود.به عنوان مثال اگر یک قطعه از پیام ۱۴ کاراکتر باشد، طول کلید نیز باید ۱۴ کاراکتر باشد. در ادامه، الگوریتم پیشنهادی در ۶ گام به شرح زیر، بیان می گردد.

گام اول: در ابتدا هر کدام از حروف یک بلوک را به عددی بین ۰ و ۲۸ نگاشت می‌شود و بر اساس رابطه زیر اولین قطعه از پیام با اولین قطعه از کلید جمع شده و باقیمانده آن به مد ۲۹ به عنوان اولین قطعه از خروجی مرحله اول (y1) محاسبه می گردد.

$$Y1(1)=mod((kay1+mes1),29) \qquad (1)$$

برای محاسبه قطعه های دیگر خروجی با توجه به تصویر (۲) از رابطه زیر استفاده می شود.

$$Y1(i)=mod((kay1(i)+mes1(i)+Y1(i-1),29) \qquad (2)$$



تصویر۲- فلوچارت گام اول

در تصویر ۲، یک قطعه از پیام با یک قطعه از کلید جمع می شود و حاصل آن بر مد ۲۹ محاسبه می شود و در نهایت به حاصل جمع بلوک ۲ از پیام و کلید، جمع می شود.

گام دوم: در این گام نیاز هست به پیچیدگی الگوربتم افزوده شود. در این گام هر جرف را به معکوس آن جایگزین میکنیم. به عنوان مثال حرف دوم الفبا را با حرف ۲۸ الفبا جایگزین میکنیم. با استفاده از رابطه (۳) خروجی این گام محاسبه می گردد.

$$Y2(i)=Y1(29-i+1) \qquad (3)$$

گام سوم: همانند گام اول، Y3 محاسبه می شود. در پایان این گام به ازای هر تغییر کوچک در پیام و یا کلید، خروجی این گام به طور کامل تغییر میکند.به عبارت دیگر اثر بهمنی در این گام به طور کامل محقق می گردد و الگوریتم پیشنهادی در پایان این گام در مقابل حمله بر اساس فرکانس حروف مقاوم است.

گام چهارم: در این گام بر اساس سلیقه کاربر می توان مقدار عددی هر قطعه را با قطعه دیگر به صورت غیرخطی جایگزین کرد. این گام معادل استفاده از s box در الگوریتم های AES و DES است.به عنوان مثال اگر گارکتر های t, s را به ترتیب به اعداد ۱۵ و ۸ نگاشت شده باشد در این گام می توان اعداد ۲و ۱۷ را جایگرین اعداد ۱۵ و ۸ کرد.

گام پنجم: همانند گام های اول و سوم ، خروجی محاسبه می گردد.

گام ششم: بر اساس رابطه زیر، پیام رمز شده از باقیمانده مجموع کلید این گام با خروجی گام قبل به مد ۲۹ محاسبه می گردد و بر اساس نگاشت اولیه به متن تبدیل می شود.

$$\text{Cipher Text}=\text{mod}((\text{kay}(i)+Y5),29) \qquad (4)$$

۲-۱- الگوریتم تولید کلید

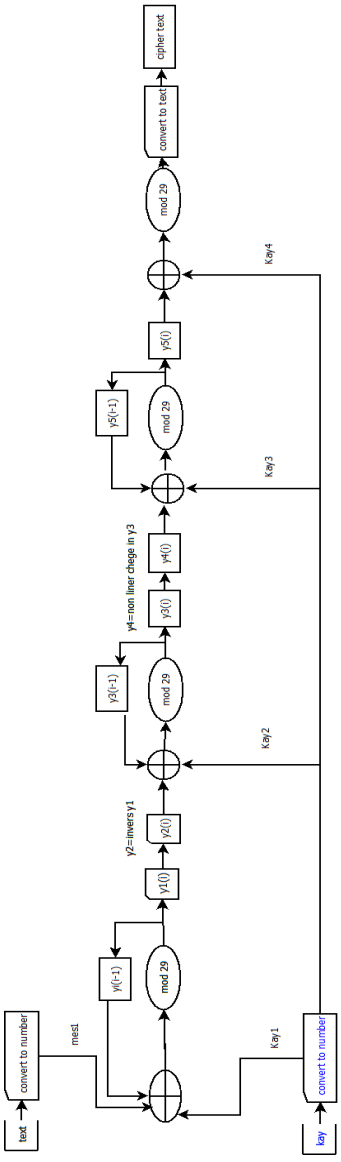
برای تولید کلید گام ۲ به بعد از روابط زیر استفاده می شود

$$\text{Kay2}=\text{mod}((\text{kay1}+\text{kay1}^*),29) \qquad (5)$$

$$\text{Kay1}^*(i)=\text{kay1}(26-i+1) \qquad (6)$$

الگوریتم فوق باعث می شود که در صورت در دسترس بودن کلید در گام های آخر برای حمله کننده، امکان دسترسی به کلیدهای گام های قبل وجود نداشته باشد.

تصویر (۳)، فلوچارت الگوریتم پیشنهادی را به طور کامل نشان می دهد.



تصویر ۳- فلوچارت الگوریتم پیشنهادی

۳ـ نتایج آزمایشگاهی

حمله جامع یکی از معروفترین حملات در رمزنگاری است .در سال۱۹۹۸ با استفاده از این حمله الگوریتم DES که تا آن زمان به عنوان استاندارد رمزنگاری داده به شمار می آمد، شکسته شود. در این حمله با پیش بینی تمام کلیدهای ممکن، متن اولیه آشکار می گردد. هر چند پیاده سازی این حمله نیازمند فضای ذخیره سازی زیاد و زمان طولانی است، اما توانست الگوریتم DES را در ۲۳ ساعت بشکند.

با توجه به این که در الگوریتم پیشنهادی طول کلید ۱۴ قطعه در نظر گرفته شده است و هر قطعه دارای ۲۹ حالت مختلف می باشد، حمله جامع به کلید شامل ۲۹۱۴ حالت مختلف است که با فرض اینکه در هر نانو ثانیه یک رمز مورد آزمایش واقع گردد، به زمانی معادل با $4 * 10^{21}$ سال نیاز می باشد.

همچنین با فرض اینکه برای آزمایش هر کلید ۱۲۸ بیت فضا مورد نیاز باشد برای آزمایش تمام کلیدهای ممکن نیاز به $2^7 * 29^{26}$بیت حافظه است که در عمل فراهم کردن آن غیر ممکن است.

با فرض اینکه سیستمی وجود داشته باشد که الگوریتم DES را در یک ثانیه شکست دهد، این سیستم در ۲۷۵۶ سال امکان شکست الگوریتم پیشنهادی را دارد.

در این الگوربتم به طور متوسط مدت زمان لازم برای رمزگذاری با استفاده از یک رایانه خانگی برای پیامی به طول ۲۶ قطعه،۳ میکرو ثانیه است.که با توجه به تعداد کم دورها و محاسبات ساده این الگوریتم، پیش بینی می شود که در مقایسه با بسیاری از الگوریتم ها زمان کمتری برای رمزگذاری و رمزگشایی دارد و هچنین با توجه به اینکه در هر گام از اعمال غیر خطی همچون همنهشتی استفاده شده است،انتظار می رود در مقابل حمله تفاضلی نیز بسیار مقاوم باشد.

یکی از حملات متدوال در الگوریتم های رمزنگاری متن، حمله بر اساس فرکانس حروف است.بر اساس نتایج آزمایشگاهی الگوریتم پیشنهادی در مقابل حمله بر اساس فرکانس حروف کاملا مقاوم است زیرا در اسن الگوریتم نتیجه خروجی بر اساس پایگاه حروف است. به عنوان مثال یک حرف یکسان اگر در دو جای یک بلوک استفاده شده باشد، در خروجی هر کدام داری مقدار متفاوتی هستند. جدول ۱ نتایج مقایسه الگوریتم پیشنهادی با الگوریتم DES و الگوریتم مطرح شده در رفرنس [۱۶] را نشان می‌دهد.

جدول ۱- مقایسه الگوریتم پیشنهادی با برخی از الگوریتم های رمز نگاری

	حمله کلید جامع	حمله به فرکانس حروف	حمله در میانه راه
DES	مقاوم نیست	مقاوم است	مقاوم نیست
الگوریتم پیشنهادی	مقاوم است	مقاوم است	مقاوم است
الگوریتم مطرح شده [۱۶]	مقاوم است	عدم احراز امنیت	مقاوم است

٤ـ نتیجه گیری

در این مقاله الگوریتم جدیدی برای رمزنگاری متن، مناسب برای الفبای ۲۹ کارکتری ارائه گردید که دارای کارایی،استحکام و سرعت زبادی در رمزنگاری می باشد. این الگوریتم در مقابل حملات متعدد ارزیابی گردید و در مقابل ایا حملات مقاومت مناسبی را ار خود نشان داد.مدت زمان لازم برای حمله جامع به کلید این الگوریتم حدود ۴*۱۰۲۱ سال می باشد که ۲۷۷۵۵ برابر زمان لازم برای حمله جامع در الگوریتم DES است. سرعت مناسب،محاسبات ساده و الگوریتم تولید کلید از دیگر مزایای این روش است. انتظار می رود از مقایسه کارایی این الگوریتم با بسیاری از الگوریتم های رمز نگاری دیگر،نتایج مناسبی حاصل گردد.

٥ـ مراجع

[۱] D. S. A. Minaam, H. M. Abdual-Kader, and M. M. Hadhoud, "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types," Int. J. Netw. Secur., vol. 11, no. 2, pp. 78-87, 2010.

[۲] J. Liu, H. Zhang, J. Jia, H .Wang, S. Mao, and W. Wu, "Cryptanalysis of an asymmetric cipher protocol using a matrix decomposition problem," Science China Information Sciencs, vol. 59, no. 5, pp. 1-11, 2016.

[۳] E. Sakalauskas and A. Mihalkovich,

"Improved asymmetric cipher based on matrix power function resistant to linear algebra attack," Informatica, vol. 28, no. 3, pp. 517-524, 2017.

[۴] Y. Zhang, D. Xiao, W. Wen, and K.-W. Wong, "On the security of symmetric ciphers based on DNA coding," Information Sciences, vol. 289, pp. 254.۲۰۱۴ ,۲۶۱–

[۵] J. Thakur and N. Kumar, "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis," International journal of emerging technology and advanced engineering, vol. 1, no. 2, pp. 6-12, 2011.

[۶] J. J. Amador and R. W. Green, "Symmetric-key block cipher for image and text cryptography," International Journal of Imaging Systems and Technology, vol. 15, no. 3, pp. 178-188, 2005.

[۷] P. Patil, P. Narayankar, D. Narayan, and S. M. Meena, "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish," Procedia Computer Science, vol. 78, pp. 617-624, 2016.

[۸] M. Taghipour, A. Moghadam, N. Moghadam, and B. Shekardasht, "Implementation of Software-Efficient DES Algorithm," Advances in Networks, vol. 3, no. 1, pp. 7-22, 2015.

[۹] T. Nie and T. Zhang, "A study of DES and Blowfish encryption algorithm," in Tencon 2009-