ارزیابی کارایی الگوریتم‌های رمزنگاری متقارن

معصومه بیت عبدالله، محمد اسماعیل دوست*، عامر کعبی

دانشکده مهندسی دریا، دانشگاه علوم و فنون دریایی خرمشهر، ایران

تاریخ دریافت: ۱۳۹۳/۲/۳۰ تاریخ پذیرش: ۱۳۹۴/۸/۹
شناسه دیجیتال (DOI) : 10.22113/jmst.2016.40455

چکیده

با گسترش فناوری، نیاز به امنیت داده‌ها و اطلاعات بر روی بستر مخابراتی ضروری می‌باشد. یکی از موارد پراهمیت جهت برقراری امنیت اطلاعات، محیط های دریایی شامل ارتباطات مابین کشتی‌ها و همچنین ارتباط کشتی‌ها با ایستگاه های زمینی می باشد. جهت حفظ محرمانگی اطلاعات، الگوریتم های رمزنگاری متقارن مانند DES، 3DES، IDEA، RC6، Serpent و AES توسط محققان ارائه شده اند. گزارشات مختلفی توسط محققان جهت مقایسه کارایی این الگوریتم ها ارائه شده است. علی رغم بررسی های متنوع انجام شده، همچنان فقدان گزارشی جامع که از تمامی مناظر این الگوریتم ها را مورد مقایسه قرار دهد، احساس می‌شود. در این مقاله مقایسه و بررسی جامعی از منظر معماری، انعطاف پذیری، امنیت و سرعت اجرا انجام گرفته است. براساس نتایج بدست آمده با توجه به کاربرد بتوان بر اساس انعطاف پذیری، سطح امنیت مورد نظر و یا سرعت اجرا نسبت به انتخاب الگوریتم اقدام نمود. نتایج پیاده سازی و مقایسات نشان دهنده برتری الگوریتم رمزنگاری AES در امنیت و RC6 در سرعت اجرا می‌باشد.

کلمات کلیدی: رمزنگاری، امنیت، مخابرات، رمزنگاری کلید متقارن، مخابرات دریایی

* نویسنده مسئول، پست الکترونیک: m_doust@kmsu.ac.ir

۱. مقدمه

استفاده از رمزنگاری به عنوان یک ضرورت برای حفاظت اطلاعات خصوصی در برابر دسترسی های غیر مجاز در تجارت و سیاست و مسائل نظامی می-باشد. به طور کلی امروزه جهت حفظ محرمانگی اطلاعات، الگوریتم های رمزنگاری مورد استفاده قرار می گیرد. امروزه رمزنگاری و تحلیل رمز به عنوان یک علم مستقل شناخته شده و به عنوان یک وسیله علمی برای ارسال اطلاعات محرمانه روی بسترهای شبکه‌های و مخابرات مورد استفاده قرار می‌گیرد (Ebrahim et al., 2013). با توجه به مرز دریایی ایران در شمال و جنوب کشور، استفاده از الگوریتم مناسب رمزنگاری بر اساس کاربرد مورد نظر در ارتباطات دریایی بسیار ضروری می باشد.

رمزنگاری که به طور عمده به دو بخش رمزنگاری متقارن یا رمزنگاری با کلید خصوصی و رمزنگاری نامتقارن یا رمزنگاری با کلید عمومی صورت می‌گیرد. هدف الگوریتم‌های رمزنگاری ایجاد یک ارتباط سری از طریق سیستم‌های مخابراتی و شبکه‌های کامپیوتری، مباحث مربوط به محرمانگی و احراز هویت را تحت فرض‌های مشخص، به درستی اثبات نماید. در رمزنگاری متقارن، فرایند رمزنگاری و رمزگشایی با یک کلید صورت می‌گیرد. الگوریتم‌های مختلفی در این زمینه ارائه شده‌اند که از مهم‌ترین این الگوریتم‌ها می‌توان الگوریتم-DES (FIPS Pub.46. 1977)، 3DES (Chouinard, J, Y. 2002)، Serpent ، IDEA (Lai. X. et al, 1990) AES (Deamen. J. ،(Anderson. R. et al., 1998) RC6 (Rivest. R. L. et al., 1998) ،et al., 1999) ارائه شده‌اند. در گذشته ارزیابی کارایی الگوریتم‌های رمزنگاری از منظرهای مختلف مانند امنیت و سرعت و یا سایر پارامترهای مورد بحث صورت گرفته است از جمله در (Singh. N. and Raina. J. 2011) یک مقایسه تجزیه و تحلیل بین RC4 و AES برای استفاده بهتر ارائه دادند. که در این مقاله برای پیدا کردن عملکرد مقایسه بین رمزهای بلوکی AES و رمز جریان RC4 تلاش شده است. براساس تجزیه و تحلیل و نتیجه این مقاله به این نتیجه رسیدند که الگوریتمی برای استفاده بهتر است که براساس معیارهای مختلف عملکرد خوبی داشته باشد. معیارهای مختلف عبارتند از: زمان رمزنگاری و رمزگشایی، توان، زمان پردازش CPU، حافظه مصرفی.

در مقاله ارائه شده در (Masram. R.et al., 2014) تجزیه و تحلیل و مقایسه‌ی برخی از پیام‌های رمزنگاری با کلید متقارن (RC4، AES ,Blowfish , RC2 , DES , 3DES , Skipjack) را براساس زمان رمزنگاری با تغییرپذیری ویژگیهای گوناگون فایل مانند انواع داده‌های مختلف، حجم داده، تراکم داده و اندازه‌های کلیدی فراهم می‌کند. با توجه به نتایج مشابه نتیجه گیری می‌شود که زمان رمزنگاری به نوع داده وفشردگی داده‌ی فایل بستگی ندارد. این تحقیق نشان داد که رمزنگاری فقط به تعداد بایت‌های موجود در فایل بستگی دارد. همچنین آشکار شد که زمان رمزنگاری و حجم داده با یکدیگر متناسب هستند. حجم داده زمان رمزنگاری را افزایش می‌دهد و برعکس. با افزایش اندازه کلید، زمان رمزنگاری افزایش می‌یابد، اما با افزایش اندازه کلید برای رمز جریانی مانند RC4 زمان رمزنگاری کاهش می‌یابد.

در (Thakur. J. et al., 2011) یک مقایسه از AES RC6, Blowfish, RC2, 3DES, DES, ارائه دادند. آنها برای الگوریتم‌های مختلف تنظیمات مختلف مانند اندازه بلوک داده‌ها ، انواع داده‌های مختلف، قدرت مصرف باتری، اندازه‌های مختلف کلید و در نهایت سرعت رمزنگاری و رمزگشایی استفاده کردند. آنها نتیجه گرفتند که در صورت تغییر در اندازه داده-ی Blowfish و RC6 عملکرد بهتری از دیگر الگوریتم‌ها دارد. حال AES عملکرد بهتری نسبت به RC2 , DES, 3DES دارد. در صورت تغییر اندازه کلید نتیجه گرفته شد که بالاتر بودن اندازه کلید به وضوح منجر به تغییر در باتری و زمان مصرف می-باشد.

در این کار همچنین آزمایشی برای مقایسه عملکرد الگوریتم‌های رمزنگاری مختلف داخل اجرا انجام داده است. چارچوب شبکه آنها نزدیک به نتایج آنهایی که از قبل نشان داده شده است. مقایسه الگوریتم‌های زیر انجام شد: DES, 3DES, RC2, AES نتایج نشان می‌دهد که AES عملکرد بهتری نسبت به سایر الگوریتم های دارد.

در مقاله ارائه شده توسط (Pc. A. et al., 2013)، مقایسه‌ای از الگوریتم رمزنگاری متقارن به نام‌های زیر را نشان داده است : RC2, 3DES, DES, AES, RC6, Blowfish بطوریکه این مقاله بر روی مقایسه الگوریتم‌های رمزنگاری در تنظیمات مختلف برای هر الگوریتم مانند اندازه کلیدهای داده ، انواع مختلف داده‌ها و اندازه آنها، توان مصرف باتری ، اندازه مختلف کلیدها و در نهایت سرعت رمزنگاری و همچنین سرعت رمزگشایی تمرکز دارد. نتایج برتری Blowfish در زمان پردازش، توان مصرفی و خروجی نسبت به دیگر الگوریتم‌ها نشان می‌دهد.

با وجود ارزیابی و بررسی های انجام شده، همچنان خلاء بررسی جامع الگوریتم های رمزنگاری متقارن احساس می شود. از اینرو در این مقاله بررسی جامعی صورت گرفته و ارزیابی کارایی الگوریتم‌های رمزنگاری متقارن از مناظر مختلف مانند معماری، امنیت، انعطاف پذیری، محدودیت و سرعت مورد بررسی و مقایسه قرار می‌گیرد.

این مقاله به صورت زیر سازماندهی شده است. در بخش دوم مواد و روش ها شرح داده شده و در بخش سوم ارزیابی کارایی و نتایج مقایسه الگوریتم‌های رمزنگاری متقارن پرداخته شده و و در نهایت بحث و نتیجه گیری در بخش چهارم آورده است.

۲- مواد و روش ها

معیارهایی که در این مقاله الگوریتم‌های رمزنگاری مورد ارزیابی قرار می‌گیرند در جدول ۱ نشان داده شده است. معیار اول مورد ارزیابی معماری می‌باشد که شامل ساختار و نحوه پیاده الگوریتم در نظر گرفته می‌شود (Ebrahim et al., 2013) و (Anderson. R. et al., 1998). معیار دوم امنیت بوده که قدرت الگوریتم رمزنگاری در مقابل حملات را نشان می‌دهد (Kaur. M, et al., 2014).

جدول۱. معیارهای ارزیابی الگوریتم‌های رمزنگاری

معیار	تعریف
معماری	ساختار و عملیات هایی را که یک الگوریتم توان انجام آنها را دارد، ویژگی‌های آن و اینکه آنها چگونه پیاده سازی می‌شوند را تعریف می‌کند.
امنیت	یک معیار مثبت از قدرت سیستم در مقابل یک حمله این است که هر الگوریتم رمزنگاری دارای این خاصیت متمایز کننده (ساخته شده با ترکیب جانشینی با جابجایی به طور مکرر) باشد. امنیت یک الگوریتم رمزنگاری بستگی به اندازه کلید مورد استفاده برای عمل رمزنگاری دارد: به طور کلی، با طول کلید بیشتر رمزنگاری قوی‌تر است .طول کلید با واحد بیت اندازه گیری می‌شود.
انعطاف پذیری	اینکه آیا الگوریتم قادر به تحمل تغییرات جزئی با توجه به شرایط است را معین می‌کند.
محدودیت (حملات شناخته شده)	معین می‌کند که این الگوریتم چقدر با استفاده از منابع کامپیوتری در دسترس آن خوب کار می‌کند. به علاوه اینکه چقدر در برابر انواع مختلف از حملات آسیب پذیر است.
سرعت	زمان اجرای الگوریتم رمزنگاری را نشان می‌دهد.

معیار سوم انعطاف پذیری بوده که شامل تغییرات جزئی الگوریتم با توجه به شرایط را معین می‌کند. معیار چهارم محدودیت بوده که نشان دهنده بازدهی

الگوریتم و میزان آسیب پذیر بودن آن در برابر حملات است (Ebrahim et al., 2013)، (Elbaz. L. et al., 2000)، (Rivest. R. L.etal., 1998) در نهایت معیار پنجم سرعت بوده که زمان اجرای الگوریتم رمزنگاری را نشان می‌دهد (Elminaam. D. et al., 2008).

دررمزنگاری متقارن، رمزنگاری و رمزگشایی اطلاعات با کلیدی مشابه صورت می‌گیرد. در این بخش انواع الگوریتم های ارائه شده توسط محققین به اختصار مورد بررسی قرار می‌گیرد. از جمله الگوریتم‌های مورد بررسی در این مقاله عبارتند از AES (Deamen. J., et al., 1999)، DES (FIPS-Pub.46. 1977)، 3DES (Chouinard, J, Y. 2002)، RC6 (Rivest. R. L.et al., 1998)، IDEA (Lai. X et al, 1990) و Serpent (Anderson. R. et al., 1998).

استاندارد رمزنگاری داده‌ها (DES)، طراحی شده توسط IBM بر اساس رمز لوسیفر آنها اولین استاندارد رمزنگاری بود که توسط NIST (موسسه ملی استانداردها و فناوری) منتشر شد (FIPS-Pub.46. 1977). DES در ابتدا به عنوان یک الگوریتم قوی در نظر گرفته شد، اما امروز مقدار زیاد داده‌ها و طول کلید کوتاه DES، استفاده از آن را محدود می‌کند (Ebrahim et al., 2013).

بر اساس معیارهای ارزیابی بررسی شده در بخش قبل، از منظر معماری، DES الگوریتم رمزنگاری متقارن که ساختار آن فیستل (Feistel) است. DES یک رمزنگاری بلوکی است که در آن یک متن ساده ۶۴ بیتی با ۱۶ دور و طول کلید ۵۶ بیتی استفاده می شود. در اصل این کلید ۶۴ بیتی (همان اندازه بلوک) است. اما در هر بایت ۱ بیت به عنوان یک بیت توازن (parity) انتخاب می‌شود که برای مکانیزم رمزنگاری مورد استفاده قرار نمی‌گیرد. ۱۶ دورDES به شانزده کلید ۴۸ بیتی متفاوت نیاز دارد که همگی انها به روش غیر خطی و نسبتا پیچیده از کلید ۵۶ بیتی اصلی، استخراج می‌شوند. از طرفی DES شامل ۸ عدد s-box می‌باشد و از الگوریتم یکسان در رمزگشایی مورد استفاده قرار می گیرد (FIPS-Pub.46. 1977).

در بررسی امنیتی DES باید گفت که قدرت و امنیت DES به طول کلید ۵۶ بیتی آن بستگی دارد، که انتخاب یک کلید خاص بسیار سخت است. علاوه بر این DES یک اثر بهمنی قوی[2] را به نمایش گذاشت، به عنوان مثال یک اصلاح کوچک در متن یا کلید، ممکن است متن رمز را به طرز محسوسی تغییر دهد. در ابتدا DES امن در نظر گرفته شد. اگر چه DES در برابر حملات خطی و دیفرانسیل مختلف مقاومت می‌کند اما در سال ۱۹۹۸ بنیاد مرز الکترونیک (EFF) یک ماشین با هدف خاص برای "رمز گشایی DES" طراحی کرد. در یک نمایش، آن کلید یک پیام رمز شده را در کمتر از یک روز در ترکیب با یک اتحاد از کاربران کامپیوتر در سراسر جهان به دست آورد.

در بررسی محدودیت DES باید گفت که DES در برابر حملات تحلیل رمز خطی بسیار آسیب پذیر است، کلید ضعیف نیز یک مشکل بزرگ DES است. 3DES در نوامبر سال ۱۹۹۸، با تمرکز بر عیوب قابل توجه در DES بدون تغییر ساختار اصلی از این الگوریتم جایگزین شد. 3DES نسخه بسیار پیچیده‌تر از DES بود که دستیابی به سطح بالایی از امنیت با رمزنگاری داده‌ها با سه بار اعمال DES با استفاده از سه کلید مختلف داشت. 3DES هنوز هم برای استفاده توسط سیستم های دولتی آمریکا تایید می-شود، اما توسط استاندارد رمزنگاری پیشرفته (AES) جایگزین شده است (Chouinard, J, Y. 2002).

بر اساس معیار های ارزیابی بررسی شده در بخش قبل، از منظر معماری ، 3DES دقیقا همان چیزی است که نامیده می‌شود، آن سه تکرار از رمزنگاری DES در هر بلوک انجام می‌دهد. از آنجا که آن یک نسخه بهبود یافته از DES است، بر اساس مفهوم ساختار فسیتل(Feistel) است. در 3DES یک متن

[2] Avalanche effect

ساده ۶۴ بیتی با ۴۸ دور و طول کلید ۱۶۸ بیتی جایگردانی(جابجایی) شده به ۱۶ زیر کلید هر یک به طول ۴۸ بیت استفاده می‌شود. از طرفی 3DES شامل ۸ عدد s-box می‌باشد و از الگوریتم یکسان در رمزگشایی مورد استفاده قرار می‌گیرد(FIPS-Pub.46. 1977).

در بررسی امنیت 3DES باید گفت که 3DES یک نسخه بهبود یافته از DES است. 3DES از یک کلید با طول بزرگتر (به عنوان مثال ۱۶۸ بیت) نسبت به DES برای رمزنگاری استفاده می‌کند. عملیات‌های DES (رمزنگاری-رمزگشایی- رمزنگاری) ۳ بار در 3DES با ۲ تا ۳ کلید مختلف، ارائه "۱۱۲ بیت از امنیت"، اجتناب از به اصطلاح حمله ملاقات در میانه انجام می‌شوند. 3DES سطح بالایی از امنیت را در مقایسه با DES ارائه می‌دهد و هنوز هم توسط دولت ایالات متحده استفاده می‌شود (Ebrahim et al., 2013).

در بررسی محدودیت 3DES باید گفت که 3DES در معرض حملات دیفرانسیل و مرتبط با کلید است . همچنین به تنوع خاصی از حمله ملاقات در میانه حساس است.

الگوریتم IDEA در سال ۱۹۹۰ ارائه شده و نسبتا سریع و امن می باشد. این الگوریتم در برابر هر دو تجزیه و تحلیل دیفرانسیل و خطی مقاوم است. IDEA به عنوان یک رمزنگاری بلوکی امن ارائه شده و در مالکیت عمومی در دهه‌های گذشته در نظر گرفته می شود (Lai. X et al., 1990).

بر اساس معیارهای ارزیابی بررسی شده در بخش قبل، از منظر معماری، IDEA الگوریتم رمزنگاری متقارن بر اساس مفهوم ساختار تعویض-جایگشت است. این الگوریتم یک رمزنگاری بلوکی است که در آن یک متن ساده ۶۴ بیتی با ۸ دور و طول کلید ۱۲۸ بیتی جایگردانی شده به ۵۲ زیر کلید هر یک به طول ۱۲۸ بیت استفاده می‌شود. از طرفی IDEA شامل s-box نمی‌باشد و از الگوریتم یکسان در رمزگشایی مورد استفاده قرار می گیرد .

در بررسی امنیت IDEA باید گفت که IDEA دارای مقاومت قوی در برابر حملات دیفرانسیل تحت فرضیه معین است. IDEA از عملیات گروه متعدد برای افزایش قدرت خود در برابر حملات آشنا استفاده می-کند. IDEA با طول کلید ۱۲۸ بیتی یک الگوریتم امنیتی قوی است. هیچ نقطه ضعفی مربوط به حملات خطی یا جبری در مورد IDEA گزارش نشده است. بهترین حمله، که برای همه کلیدها اعمال می-شود و می‌تواند IDEA را بشکند به ۶ دور کاهش یافته است (Ebrahim et al., 2013).

در بررسی محدودیت IDEA باید گفت که تعدادی حساسیت در مورد دسته‌های مختلف کلیدهای ضعیف و نسخه دورهای حداقل در IDEA مشاهده شدند. IDEA همچنین در معرض حمله برخورد قرار دارد. IDEA شامل ۸ دور است که در آن ۳ دور اول به نظر می‌رسد بسیار در برابر حملات کلید مانند حملات برنامه-کلید و حملات زمان بندی دیفرانسیل مرتبط با کلید قرار گرفته‌اند[12].

Rijndael توسعه یافته توسط Rijmen و Daemen ، استاندارد رمزنگاری پیشرفته ایالات متحده در اکتبر سال ۲۰۰۰ اعلام شده توسط موسسه ملی استانداردها و فناوری شد. Rijndael با استفاده از طول کلید متغیر، رمز بسیار سریع و جمع و جور است. ساختار متقارن و موازی آن انعطاف پذیری زیادی را برای افرادی که آن را پیاده سازی می‌کنند، با مقاومت موثر در برابر حملات رمز کردنی، فراهم می‌کند. AES می‌تواند به خوبی با طیف گسترده‌ای از پردازنده‌های مدرن مانند پنتیوم، RISC و پردازنده-های موازی سازگار شود. به طور کلی، AES نام استاندارد است، و Rijndael الگوریتمی است که توصیف شده، اگرچه در عمل این الگوریتم به عنوان "AES" شناخته می‌شود (Ebrahim et al., 2013).

بر اساس معیارهای ارزیابی بررسی شده در بخش قبل، از منظر معماری، AES نیز الگوریتم کلید متقارن بر اساس مفهوم میدان‌های گالوا (Galios Field) است. AES یک رمزنگاری بلوکی است که در

آن یک متن ساده ۱۲۸ بیتی با دور متغیر ۱۰، ۱۲، یا ۱۴ (برای کلید ۱۲۸ بیتی ۱۰ دور، برای کلید ۱۹۲ بیتی ۱۲ دور و برای کلید ۲۵۶ بیتی ۱۴ دور دارد) و طول کلید متغیر ۱۲۸، ۱۹۲، ۲۵۶ بیتی جایگردانی شده به ۱۰ زیر کلید به ترتیب هر یک به طول ۱۲۸، ۱۹۲، طول ۲۵۶ بیت استفاده می‌شود. از طرفی AES شامل یک s-box می‌باشد و الگوریتم از یکسان در رمزگشایی مورد استفاده قرار می‌گیرد. در بررسی امنیت AES باید گفت امنیت AES به طول کلید متغیر آن که می‌تواند تا ۲۵۶ بیت برای ایجاد مقاومت در برابر حملات خاص آینده (حملات برخورد و الگوریتم های محاسبات کوانتومی بالقوه) باشد، بستگی دارد. حملات عمومی که در برابر ویرایش‌های دور متمرکز از AES آشکار شدند حمله مربع، حمله مربع بهبود یافته، حمله دیفرانسیل غیر ممکن و حمله برنامه کلید معکوس شده هستند، اما هیچ یک از این حملات عملا ممکن نبود.

در بررسی محدودیت AES باید گفت که AES نقطه ضعف جدی ندارد؛ اگرچه مشاهده شده که یک مشخصه ریاضی (و نه یک حمله) از رمز ممکن است در برابر یک حمله آسیب پذیر باشد. علاوه بر این در AES پیاده سازی رمز معکوس بر روی یک کارت هوشمند نسبت به خود رمز نامناسب است (Deamen. J., et al, 1999).

RC6 مشتق شده از RC5، طراحی شده توسط رونالد ریوست، مت راب شاو، ری سیدنی، و یکین لیزا یین یک الگوریتم کلید متقارن است. به پروژه‌های NESSIE و CRYPTREC ارائه شد. این الگوریتم توسط امنیت RSA به ثبت رسید. RC6 عملکرد خوبی از نظر امنیت و سازگاری ارائه می‌دهد (Ebrahim et al., 2013).

بر اساس معیارهای ارزیابی بررسی شده در بخش قبل، از منظر معماری ، RC6 یک الگوریتم کلید خصوصی ساختار یافته فسیتل (Feistel) است که در آن یک متن ساده ۱۲۸ بیتی با ۲۰ دور و طول کلید متغیر ۱۲۸، ۱۹۲، و ۲۵۶ بیتی استفاده می‌شود. از آنجا که RC6 بر روی اصل RC کار می‌کند، می‌توانید طیف گسترده‌ای از طول کلمه، طول کلید و تعداد دور را حمایت کند، RC6 شامل s-box نیست و از الگوریتم یکسان در رمزگشایی مورد استفاده قرار می-گیرد.

دربررسی امنیت RC6 باید گفت که امنیت RC6 در سری‌های کاملا تصادفی از بیت‌های خروجی آن با ۱۵ دور یا کمتر، اجرا بر روی بلوک‌های ورودی ۱۲۸ بیتی نهفته است، که یک پارامتر به منظور ایجاد یک الگوریتم رمزنگاری مقاوم در برابر حملات این است که خروجی آن سری‌های کاملا تصادفی از بیت را دنبال کند. یک حمله رمز گشایی خطی می‌تواند برای ۱۶ دور RC6 راه اندازی شود، اما نیاز به ۲ ^ ۱۱۹ متن ساده شناخته شده دارد، که این امکان حمله را غیر ممکن می‌سازد. الگوریتم RC6 همچنین در برابر حملات دیفرانسیل قوی می‌باشد، که با بیش از ۱۲ دور صورت گرفته‌اند (Rivest. R. L.et al., 1998).

دربررسی محدودیت RC6 باید گفت که در RC6، برای یک دسته تک از کلیدهای ضعیف، مشاهده می-شود که خودگردانی کامل تا بالای ۱۷ دور از الگوریتم به دست نمی‌آید. هیچ محدودیت دیگری مشخص نشد (Rivest. R. L.etal., 1998).

Serpent طراحی شده توسط «راس اندرسون»، «الی بیهام»، و «لارس نادسن» است. Serpent در مالکیت عمومی قرار دارد و هنوز ثبت نشده است. بر اساس معیارهای ارزیابی بررسی شده در بخش قبل، از منظر معماری، Serpent یک الگوریتم کلید متقارن است که بر اساس ساختار شبکه تعویض-جایگشت است. در این الگوریتم یک متن ساده ۱۲۸ بیتی با ۳۲ دور و طول کلید متغیر ۱۲۸، ۱۹۲، و ۲۵۶ بیتی استفاده می‌شود. از طرفی Serpent شامل ۸ عدد s-box می-باشد و از الگوریتم یکسان در رمزگشایی مورد استفاده قرار می‌گیرد. در بررسی امنیت Serpent باید گفت که Serpent مبتنی بر روش‌های امنیتی، دارای یک حاشیه امنیتی بزرگتر است. به گفته نویسنده Serpent ، ۱۶ دور Serpent کاملا در برابر همه انواع حملات

شناخته شده مناسب است، اما به عنوان جبران زیان در برابر کشفیات آینده در رمز گشایی آن به ۳۲ دور افزایش یافته است. به منظور جلوگیری از حمله برخورد Serpent معمولا به منظور تغییر کلیدها به خوبی قبل از اینکه ۲۶۴ بلوک رمزگذاری شده‌اند با احتیاط رفتار می‌کند. Serpent با حداقل پتانسیل آن (فقط تعداد نیمی از دور ها) هنوز به اندازه 3DES با ۳ کلید، امن است(Anderson. R. et al., 1998). در بررسی محدودیت Serpent باید گفت که هیچ محدودیتی در Serpent پیدا نشد. با این حال ۳۲ دور Serpent را کمی کندتر و پیچیده برای پیاده سازی بر روی بلوک‌های کوچک می‌سازد.

۳- نتایج

در این بخش نتایج مقایسه کارایی الگوریتم های رمزنگاری متقارن مورد بررسی قرار می گیرد. در جدول ۲ الگوریتم‌های رمزنگاری متقارن براساس ساختار الگوریتم و طول پیام، طول متن رمز شده، اندازه کلید، تعداد S_box، تعداد دور مقایسه شده‌اند (Ebrahim et al., 2013) و (Verma. P., et al., 2015). نتایج مقایسات ارائه شده نشان دهنده کارایی بالاتر الگوریتم رمزنگاری AES نسبت به سایر الگوریتم‌های رمزنگاری متقارن می‌باشد.

جدول ۲. مقایسه معماری الگوریتم های متقارن

	طراحی شده توسط	سال	ساختار الگوریتم	طول پیام/ متن رمز شده	طول کلید	s_box	تعداد دور
DES	IBM	۱۹۷۵	Feistel	۶۴ بیت	۵۶	۸	۱۶
3DES	IBM	۱۹۹۸	Feistel	۶۴ بیت	۱۱۲ یا ۱۲۸	۸	۴۸
IDEA	James Massey	۱۹۹۰	Substitution Permutation	۶۴ بیت	۱۲۸	____	۸
Serpent	Anderson,Lers Kundsen	۲۰۰۰	Substitution Permutation	۱۲۸ بیت	۱۲۸، ۱۹۲، ۲۵۶	۸	۳۲
AES	Joan Daemen,Incent Rijmen	۲۰۰۰	Galios Field	۱۲۸ بیت	۱۲۸، ۱۹۲، ۲۵۶	۱	۱۰، ۱۲، ۱۴
RC6	Ron Rivest,Mat Robshaw	۲۰۰۰	Feistel	۱۲۸ بیت	۱۲۸، ۱۹۲، ۲۵۶	____	۲۰

جدول ۳. مقایسه امنیت

	AES	RC6	3DES	DES
امنیت	ایمن	آسیب پذیر	نا مناسب	اثبات شده نامناسب است

جدول۴ .خلاصه ای از انعطاف پذیری الگوریتم های متقارن

الگوریتم ها	انعطاف پذیری	تغییرات	توضیحات
DES	خیر	ندارد	ساختار DES هیچ گونه تغییرات را پشتیبانی نمی‌کند.
3DEA	بله	168	ساختار 3DES مانند DES است، آن هیچ گونه تغییرات را پشتیبانی نمی-کند، اما از آنجا که آن DES را 3 بار تکرار می‌کند بنابراین طول کلید به ۱۶۸ بیت گسترش می‌یابد.
IDEA	خیر	ندارد	ساختار IDEA هیچ گونه تغییرات را پشتیبانی نمی‌کند.
AES	بله	۱۲۸، ۱۹۲، ۲۵۶	ساختار AES قابل افزایش تا چند برابر ۶۴ بیت بود، با طول زیر کلید یکسان با طول کلید
RC6	بله	۱۲۸-۲۰۴۸	RC6 دارای طول کلید متغیر است و می تواند تا ۲۰۴۸ بیت گسترش یابد با این حال طول کلید باید مضربی از ۳۲ بیت باشد.
Serpent	بله	۲۵۶	کلیدهای Serpent همیشه به ۲۵۶ بیت لایه‌گذاری می شوند. لایه متشکل از

یک بیت "۱" دنبال شده با بیت های "۰"است.

در جدول ۳ الگوریتم‌های رمزنگاری DES, 3DES, RC6, AES از لحاظ امنیت با هم مقایسه شده‌اند. همانطور که دیده می‌شود AES بهترین امنیت را در مقایسه با سایر الگوریتم‌ها داراست. در جدول۴ الگوریتم‌های مختلف بر اساس انعطاف پذیری خود یعنی توانایی یک الگوریتم برای پذیرش تغییرات با توجه به الزامات مورد تجزیه و تحلیل قرار می‌گیرند.

جدول ۵. زمان گرفته شده برای رمزنگاری هر الگوریتم (میلی‌ثانیه)

اندازه ورودی (کیلو بایت)	AES	RC6	3DES	DES
۴۹	۵۶	۴۱	۵۴	۲۹
۵۹	۳۸	۲۴	۴۸	۳۳
۱۰۰	۹۰	۶۰	۸۱	۴۹
۲۴۷	۱۱۲	۷۷	۱۱۱	۴۷
۳۲۱	۱۶۴	۱۰۹	۱۶۷	۸۲
۶۴۹	۲۱۰	۱۲۳	۲۲۶	۱۴۴
۸۹۹	۲۵۸	۱۶۲	۲۹۹	۲۴۹
۹۶۳	۲۰۸	۱۲۵	۲۸۳	۲۵۰
۵۳۴۵,۲۸	۱۲۳۷	۶۹۵	۱۴۶۶	۱۲۹۶
۷۳۱۰,۳۳۶	۱۳۳۶	۷۵۶	۱۷۸۶	۱۶۹۵

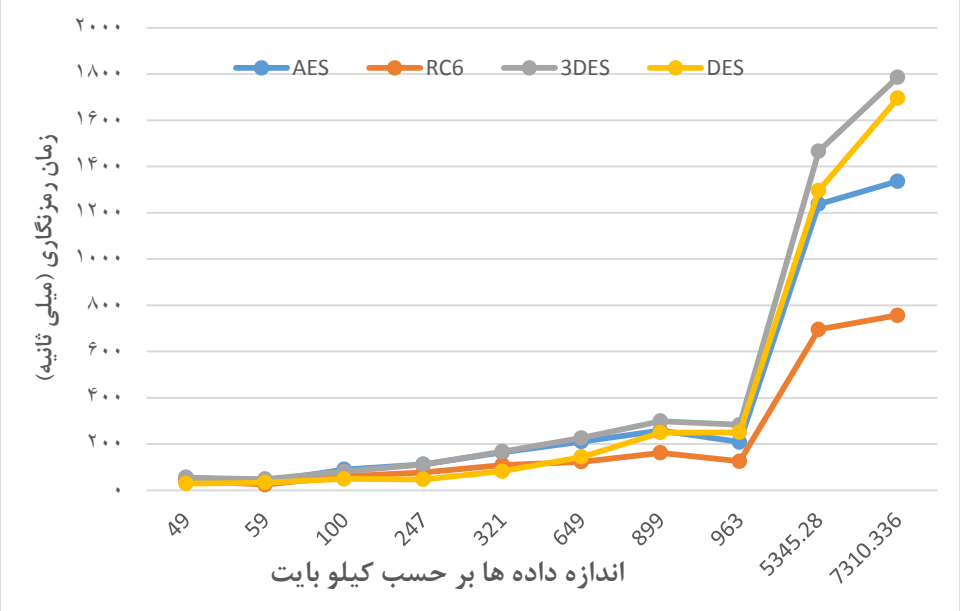
جدول ۶. زمان گرفته شده برای رمزگشایی هر الگوریتم (میلی‌ثانیه)

اندازه ورودی (کیلو بایت)	AES	RC6	3DES	DES
۴۹	۶۳	۳۵	۵۳	۵۰
۵۹	۵۸	۲۸	۵۱	۴۲
۱۰۰	۶۰	۵۸	۵۷	۵۷
۲۴۷	۷۶	۶۶	۷۷	۷۲
۳۲۱	۱۴۹	۱۰۰	۸۷	۷۴
۶۴۹	۱۴۲	۱۱۹	۱۴۷	۱۲۰
۸۹۹	۱۷۱	۱۵۰	۱۷۱	۱۵۲
۹۶۳	۱۶۴	۱۱۶	۱۷۷	۱۵۷
۵۳۴۵,۲۸	۶۵۵	۶۸۴	۸۳۵	۷۸۳
۷۳۱۰,۳۳۶	۸۸۲	۷۵۴	۱۱۰۱	۹۵۳

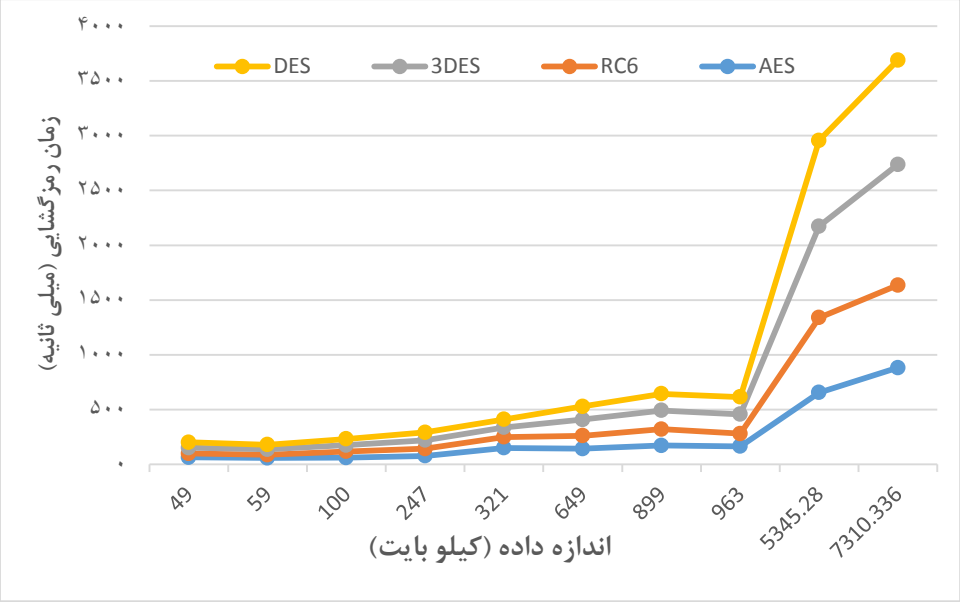
معیار ارزیابی کارایی بعد، سرعت اجرای الگوریتم‌های رمزنگاری می‌باشد. جهت انجام مقایسه سرعت اجرای الگوریتم‌ها از گزارش ارائه شده در (Elminaam. D. et al., 2008) استفاده شده است. با توجه به اینکه زمان رمزنگاری و رمزگشایی به تعداد بایت‌ها در فایل بستگی دارد، با تغییر تعداد بایت‌ها سرعت رمزنگاری و رمزگشایی تغییر می‌کند. به همین منظور ورودی با اندازه‌های متفاوت بر حسب کیلو بایت به الگوریتم‌ها داده شده است. جداول ۵ و ۶ به ترتیب زمان اجرای الگوریتم‌های رمزنگاری و رمزگشایی را بر جسب میلی ثانیه نشان می‌دهد.

۴- بحث و نتیجه گیری

بسترهای انتقال اطلاعات بر اساس کاربرد و توان پردازنده‌های مورد استفاده، نیاز به سطوح مختلفی از امنیت، سرعت و انعطاف پذیری الگوریتم رمزنگاری مورد استفاده جهت حفظ محرمانگی اطلاعات را دارند. این مسئله در محیط‌های دریایی نظیر ارتباطات مابین کشتی‌ها و همچنین ارتباط کشتی نیز برقرار می‌باشد. بر اساس کاربرد در مواردی سرعت اجرای الگوریتم بر امنیت آن برتری داشته و در مواردی امنیت بالا از ضروری‌ترین پارامترها می‌باشد. جهت سهولت در ارزیابی شکل های ۱ و ۲ به ترتیب سرعت رمزنگاری و رمزگشایی الگوریتم‌ها را نشان می‌دهد. همانطور که دیده می‌شود سرعت رمزنگاری و رمزگشایی الگوریتم RC6 بهترین عملکرد را داراست. عملکرد AES در مقایسه با RC6 کمی کندتر است، اما بهترین امنیت را دربرابر حملات دارد. 3DES با اینکه امنیت بیشتری نسبت به DES دارد ولی سرعت رمزنگاری و رمزگشایی پایین‌تری دارد.



شکل ۱. مقایسه زمان رمزنگاری الگوریتم‌ها



شکل ۲. مقایسه زمان رمزگشایی الگوریتم‌ها

از طرفی دیگر بر اساس نتایج ارائه شده در بخش قبل، بالاترین سطح امنیت مربوط به الگوریتم رمزنگاری AES می باشد. وجود الگوریتمی منعطف که موازنه‌ای مابین امنیت و سرعت برقرار کند و براساس نیاز افزایش سطح امنیتی آن با کاهش سرعت اجرا میسر باشد، مطلوب این گونه کاربردها می‌باشد. الگوریتم‌های رمزنگاری DES، 3DES، IDEA، RC6، Serpent و AES ذکر شده بر اساس پارمترهای معماری، انعطاف پذیری، سرعت و امنیت الگوریتم‌ها ارزیابی و مورد مقایسه قرار گرفته‌اند. بر اساس نتایج پیاده سازی و مقایسات، بر اساس سطح امنیت و سرعت مورد نیاز هر کاربرد، می‌توان از الگوریتم رمزنگاری مناسب را انتخاب نمود.

منابع

Anderson. R., Biham. E. and Knudsen. L. 1998. Serpent: A Proposal For The Advanced Encryption Standard. AES algorithm submission.

Chouinard, J, Y. 2002. Design of Secure Computer Systems CSI4138/CFG4394 Notes on the Data Standard (DES).

Deamen. J. and Rijmen. V. 1999. AES Proposal: Rijedeal. AES Algorithm submission.

Ebrahim, M., Khan, S. and Bin Khalid, U. 2013. Symmetric Algorithm Survey: A Comparative Analysis, International of Computer Applications:12-19.

Elbaz. L, and Bar-El. H. 2000. Strength Assessment of Encryption Algorithms. Advanced Embedded Security.

Elminaam. D, Abdul Kader. H, Ha, Zdhoud. M. 2008. Performance Evaluation of Symmetric Encryption Algorithm. IJCSNS: 280-286.

FIPS-Pub.46. 1977. Data Encryption Standard. National Bureau of Standards, U.S. Department of Commerce, Washington D.C.

Kaur. M, and Kaur. S. 2014. Survey of Various Encryption Techniques for Audio Data. IJARCSSE:1314-1317.

Lai. X. and Massey. J. 1990. A proposal for a new block encryption standard'', In Proceedings of the EUROCRYPT 90 Conference:389- 404.

Masram. R., Shahare. V., Abraham. J., Moona. R. 2014. Analysis and Comparison of Symmetric Key Cryptographic Algorithm Based on Various File Features'', IJNSA: 43-52.

Pc. A., Devassy. A., C George. S, and Devassy. A. 2013. Survey of Symmetric Cryptographic Algorithms. IOSR-JECE:65-75.

Rivest. R. L., Robshaw. M. J. B., Sidny. R. and YIN. Y.L. 1998. The $RC6^{TM}$ Block Cipher: 1-21.

Singh. N. and Raina. J. 2011. Comparative Analysis of AES and RC4 Algorithms for Better Utilization. International Journal of Computer Trends and Technology:178-181.

Thakur. J, and Kumar. N. 2011. DES, AES and Blofish: Symmetric Key Cryptographic Algorithms Simulation Based Performance Analysis. International Journal of Emerging Technology and Advanced Engineering: 6-12.

Verma. P, Shekhar. J, Preey, Asthana. A. 2015. A Survey for Performance Analysis Various Cryptography Technique Digital Contents. IJCSMC:522 - 531.

Performance Evaluation of Symmetric Key Cryptography Algorithms

Masome Beit Abdollah, Mohammad Esmaeildoust‡, Amer Kaabi

Faculty of Marine Engineering, Khorramshahr University of Marine Science and Technology, Iran

(DOI): 10.22113/jmst.2016.40455

Abstract

With growth of technology, the needs for data and information security over communication channels are necessary. Providing information security in marine environment includes communication between ships and also ships with ground station are one of the most important issues in information security. In order to provide Confidentiality, symmetric key cryptography algorithms such DES, 3DES, IDEA, RC6, Serpent and AES are presented by researchers. Different reports in literature are presented by researchers in order to compare the performance of these algorithms. Despite various considerations, the needs for deep comparison of these algorithms are needed. Therefore in this paper, deep consideration and comparison in the points of architecture, flexibility, security and speed of these algorithms are done. Based on the achieved results, the appropriate algorithm can be employed based on required flexibility, speed or desired levels of security. The result of implementation and comparison shows the advantages of AES algorithm in provided security and RC6 in speed of execution.

List of tables and figures

‡ Corresponding Author Email: m_doust@kmsu.ac.ir