Specialized Scientific Quarterly Journal of

Arman Process (APJ)

Investigating the applicable security encryption algorithms

M. Nemati [*,1] ***, N. Fareghzadeh*** [2]

[1] *Department of Computer Science, Khodabandeh Branch, Islamic Azad University, Zanjan, Iran*
[2] *Department of Computer Science, Khodabandeh Branch, Islamic Azad University, Zanjan, Iran*

ABSTRACT

KEYWORDS:
Cryptography
Network Security
Encryption
Algorithm
Public Key

Corresponding author
m.nemati@gmail.com

Submitted: 2021-09-08
Accepted: 2021-11-26

Recently, the distributed internet applications under the scalable networks are growing rapidly, so the need to protect and secure such applications has also increased. Encryption algorithms are vital in today's cyber world, where there is always the risk of unauthorized access to all types of data. The most sensitive and vulnerable data is financial and payment system data, which can compromise personal identification information or customer payment card details and other personal information. Cryptographic algorithms are critical to protecting this information and reducing the risks that business face in conducting payment transactions. In fact, cryptographic algorithms play a major role in the information security of systems and the production of digital signatures. Existing digital signatures are often based on cryptographic algorithms and lead to the recognition of electronic information so that the identity of the author of the document and the comprehensiveness of its information can be reviewed and controlled. In this article, in addition to defining and classifying common cryptographic algorithms, we try to make a comparison on power and effectiveness of applicable algorithms in this area. This review and comparison can lead to improved functions and improved approaches to using these algorithms.

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
14	0	2

فصلنامه تخصصی

آرمان پردازش

بررسی و مقایسه الگوریتم های رمزنگاری امنیتی کاربردی

مریم نعمتی*[۱]، نفیسه فارغ زاده[۲]

۱ گروه کامپیوتر، دانشکده برق و کامپیوتر، واحد خدابنده، دانشگاه آزاد اسلامی، زنجان، ایران

۲ گروه کامپیوتر، دانشکده برق و کامپیوتر، واحد خدابنده، دانشگاه آزاد اسلامی، زنجان، ایران

چکیده

امروزه اینترنت و برنامه های کاربردی تحت شبکه به سرعت در حال رشد هستند، از این‌رو نیاز به محافظت و تامین امنیت چنین برنامه هایی نیز افزایش یافته است. الگوریتم‌های رمزنگاری در دنیای سایبر امروزی که همیشه خطر دسترسی غیرمجاز به همه نوع داده وجود دارد، امری حیاتی محسوب می‌شوند. حساس‌ترین و آسیب‌پذیرترین داده، داده‌های سیستم مالی و پرداختی است که می‌تواند اطلاعات شناسایی شخصی یا مشخصات کارت پرداخت مشتریان و سایر اطلاعات شخصی را در معرض خطر قرار دهد. الگوریتم‌های رمزنگاری برای محافظت از این اطلاعات و کاهش خطراتی که مشاغل در انجام معاملات پرداخت با آن روبرو هستند، بسیار مهم است. درواقع، الگوریتمهای رمزنگاری نقش اصلی را در امنیت اطلاعات سیستمها و تولید امضای دیجیتال بازی می کنند. امضاهای دیجیتال موجود غالبا مبتنی بر الگوریتمهای رمزنگاری بوده و باعث به رسمیت شناسی اطلاعات الکترونیکی شده به طوریکه هویت پدیدآورنده سند و جامعیت اطلاعات آن، قابل بازبینی و کنترل میباشد. در این مقاله کوشش می کنیم علاوه بر تعریف و دسته بندی الگوریتمهای رمزنگاری رایج و مقایسه ای بر روی قدرت و میزان تاثیرگذاری انجام دهیم. این بررسی و مقایسه می تواند منجر به بهبود کارکردها و اصلاح رویکردهای بکارگیری این الگوریتم ها بشود.

واژگان کلیدی:
رمزنگاری
امنیت شبکه
رمزگذاری
الگوریتم
کلید عمومی

[۱] نویسنده مسئول

m.nemati@gmail.com

تعداد جداول	تعداد شکل ها	تعداد مراجع
۲	۰	۱۴

مقدمه

رمزنگاری[1] دانشی است که به بررسی و شناختِ اصول و روش‌های انتقال یا ذخیره اطلاعات به صورت امن می‌پردازد. رمزنگاری استفاده از روش‌های ریاضی، برای برقراری امنیت اطلاعات است. دراصل، رمزنگاری دانش تغییر دادن متن اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم رمز است. به صورتی که تنها شخصی که از کلید و الگوریتم آگاه است می‌تواند اطلاعات اصلی را از اطلاعات رمزگذاری، استخراج کند و شخصی که از آن‌ها آگاهی ندارد نمی‌تواند به اطلاعات دسترسی پیدا کند [1].

دانش رمزنگاری بر پایه اصولی مانند نظریه اطلاعات، نظریه اعداد و آمار بنا شده‌است و امروزه در علوم کامپیوتری مورد بررسی و استفاده قرار می‌گیرد. اساسا رمزنگاری یعنی فرایند تبدیل متن ساده و آشکار به یک متن رمز پنهان جهت امنیت داده در برابر دسترسیهای غیرمجاز. این فرآیند در بخش دیگری که نیاز است متن رمز، رمزگشایی شود به شکل قابل درک (متن ساده) تبدیل میشود. در واقع هدف اصلی از رمزنگاری مراقبت از داده ها در برابر مهاجمان میباشد. الگوریتم رمزنگاری، به هر الگوریتم یا تابع ریاضی گفته می‌شود که به علت دارا بودن خواص مورد نیاز در رمزنگاری، در پروتکل‌های رمزنگاری مورد استفاده قرار گیرد. بر مبنای تعریف بالا، توابع و الگوریتم‌های مورد استفاده در رمزنگاری به دسته‌های کلی زیر تقسیم می‌شوند [2-4]:

- توابع بدون کلید
  - توابع درهم‌ساز
  - تبدیل‌های یک‌طرفه
- توابع مبتنی بر کلید
  - الگوریتم‌های کلید متقارن
    - الگوریتم‌های رمز قالبی
    - الگوریتم‌های رمز دنباله‌ای
    - توابع تصدیق پیام*
  - الگوریتم‌های کلید نامتقارن
    - الگوریتم‌های مبتنی بر تجزیه اعداد صحیح
    - الگوریتم‌های مبتنی بر لگاریتم گسسته
    - الگوریتم‌های مبتنی بر منحنی‌های بیضوی
  - الگوریتم‌های امضای دیجیتال

لازم به ذکر است، اساسا در حوزه فناوری اطلاعات و ارتباطات الگوریتم‌های رمزنگاری بسیار زیاد هستند، اما تنها شمار اندکی از آن‌ها به صورت استاندارد و قابل کاربرد درآمده‌اند، که در این مقاله به الگوریتم های کاربردی تر در حوزه فناوری اطلاعات و ارتباطات می پردازیم.

الگوریتم های رایج رمزگذاری

رمزگذاری شیوه‌ای است که در آن متن اصلی پیام با استفاده از مجموعه ای از عملیات ریاضی معکوس‌پذیر به یک متن بی‌معنا تغییر می‌یابد. به عبارت دیگر رمزگذاری به طور سیستماتیک ترتیب عناصر یک پیغام را تغییر می‌دهد تا برای همه به جز گیرنده قابل فهم باشد. به طور کلی در عمل رمزگذاری دو جزء مهم وجود دارد که عبارتند از : کلید رمز و الگوریتم رمزگذاری که تعریف آنها به قرار زیر است [5, 6]:

کلید رمز و طول آن : کلید رمز کلیدی است که بتوان با استفاده از آن قفل دسترسی به متن اصلی را باز کرد. این کلید یک مقدار عددی است که معمولاً به شکل مبنای شانزده است. کاراکترهای مورد استفاده برای ساخت یک کلید معمولی به صورت دوتایی یا چهارتایی دسته‌بندی می‌شوند که شامل اعداد ۰ تا ۹ و حروف A تا F هستند. یکی از عوامل موثر در استحکام و مقاومت روش رمزگذاری در مقابل مهاجمان، طول کلید رمزاست. هر چه تعداد ترکیب‌های احتمالی یک کلید رمز بیشتر باشد، امکان کشف و لو رفتن آن مشکل‌تر می‌شود و درجه امنیّت آن بالاتر می‌رود. با تمام اینها، چنانچه تحلیل مناسب و زمان کافی در اختیار باشد، هر کلید رمزی صرف‌نظر از تعداد بیت‌های آن قابل کشف است. طول کلید با تعداد بیت‌های آن با توجه به اطلاعاتی که بایستی رمزگذاری گردد، انتخاب می‌شود. به این ترتیب که هر چه اطلاعات و پیام حساس‌تر بوده و نیاز به امنیت بیشتری باشد، تعداد بیت‌های انتخابی بیشتر خواهد بود. الگوریتم رمزگذاری فرآیندی چندمرحله‌ای است که کاربر با استفاده از آن متن اصلی را به رمز تبدیل می‌کند و یا این که متن رمزگذاری شده را به متن اصلی برگرداند. روش های کاربردی و عمومی رمزگذاری که اصولا بر مبنای نحوه استفاده از کلید رمز با یکدیگر تفاوت دارد، به شرح زیر می باشند:

◙ روش رمزگذاری متقارن با کلید خصوصی:

روش رمزگذاری متقارن روشی است که در آن تنها یک کلمه رمز یا کلید ورود به متن اصلی مورد استفاده قرار می‌گیرد. در این روش هر یک از طرفین ارتباط، بایستی یک کلید رمز خصوصی یکسان همانند داشته باشند. در حقیقت متن اصلی با این کلید خصوصی رمزگذاری شده و برای بازیابی متن اصلی و تبدیل آن از حالت رمز (بی‌معنا) به حالت اصلی (معنادار) نیز باید از همان کلید خصوصی استفاده نمود. علت نامگذاری این روش به نام متقارن این است که در هر طرف معامله یک کلید یکسان مورد استفاده قرار گرفته و رمزگذاری

[1] Cryptography

حالت متقارن دارد. ایراد این روش این است که کلید خصوصی باید قبل رمزگذاری پیام‌ها، از یک کانال ارتباطی ایمن بین طرفین مبادله شود. اما حسن این روش سرعت بالای آن است [7]. الگوریتم معروف مورد استفاده در این روش به نام DES یا رمزگذاری استاندارد اطلاعات نامیده می‌شود که در ادامه در مورد آن توضیح داده می‌شود.

■ الگوریتمDES :

یکی از اساسی‌ترین و رایج‌ترین الگوریتم‌های رمزگذاری است که اولین بار در سال ۱۹۷۷ در امریکا برای کاربردهای نظامی به کار گرفته شد. در این الگوریتم از رمزگذاری بلوک به بلوک استفاده می‌شود. به این ترتیب که ابتدا یک کلید رمز به طول ۵۶ بیت ایجاد می‌شود و سپس متن اصلی به بلوک‌ها یا قسمت‌های ۶۴ بیتی تقسیم‌شده و با استفاده از این کلید رمز در یک فرآیند ۱۶ مرحله‌ای به یک رمز ۶۴ بیتی تبدیل می‌شود. بنابراین کل متن به قسمت‌های ۶۴ بیتی رمزدار شده تبدیل می‌شود. این الگوریتم در روش رمزگذاری متقارن با کلید خصوصی مورد استفاده قرار می‌گیرد. ولی دارای معایبی به شرح زیر است:
معایب : کلید رمز در این الگوریتم یکی است، لذا باید همزمان در اختیار دو طرف باشد، همچنین ارسال کلید رمز از یک نفر به نفر دیگر نیز مشکلات خاصّ خود را دارد و ممکن است به دست او نرسد و یا در حین ارسال فرد دیگری به آن دسترسی یافته و آن را تغییر دهد. تغییر کلید رمز را نمی‌توان از طریق الگوریتم شناسایی نمود. به عبارت دیگر این الگوریتم قادر نیست که اصالت پیام را تصدیق و تایید کند [8].

■ الگوریتم DES[1] سه‌گانه:

این الگوریتم یک روش افزایش قدرت رمزگذاری DES می‌باشد که از طریق استفاده از دو یا سه کلید مختلف در فرآیند رمزگذاری و رمزگشایی مورد استفاده قرار می‌گیرد. روش کار در الگوریتم به این ترتیب است که ابتدا متن اصلی به وسیله کلید S1 رمزگذاری می‌شود. این عامل باعث می‌شود که طول کلید رمز از ۵۶ بیت (در DES) به ۱۱۲ بیت افزایش یابد، بنابراین دسترسی و کشف کلید رمز به آسانی امکان پذیر نمی باشد.

■ روش رمزگذاری نامتقارن با کلید عمومی:

در این روش دو طرف دارای دو کلید رمز هستند. یکی رمز عمومی و کلید رمز خصوصی. استفاده از این روش نسبت به روش متقارن ساده‌تر بوده، ولی سرعت آن کمتر است. در این تکنیک کلید عمومی به راحتی از طریق کانال‌های عمومی انتقال اطلاعات، انتقال می‌یابد و کلید خصوصی به صورت محرمانه نزد دو طرف نگهداری می‌شود. روش کار به این صورت است که یک کلید عمومی مورد استفاده قرار می‌گیرد تا پیام به صورت رمز درآید و کلید دیگر (خصوصی) برای رمزگشایی آن استفاده می‌گردد. اگر چه این کلیدهای عمومی و خصوصی از لحاظ ریاضی به هم مربوط می‌باشند، ولی از نظر محاسباتی عملی نیست که از یک کلید، کلید رمز دیگر استخراج گردد. این روش دارای امنیّت بالایی بوده و در هنگامی که حداکثر امنیت مورد نیاز باشد، استفاده می‌شود. از آن‌جایی که کلید عمومی در دسترس همگان قرار دارد، برای حفظ امنیت بایستی کلید خصوصی در فواصل کوتاه زمانی عوض گردد.علت نامگذاری این روش به نام نامتقارن نیز این است که رمزگذاری حالت نامتقارن دارد.الگوریتم مورد استفاده در این روش به نام RSA شناخته می‌شود که در ادامه در مورد آن توضیح داده می‌شود [9].

■ الگوریتمRSA :

سه نفر از محققین دانشگاه MIT در سال 1978 استاندارد ویژه‌ای را برای الگوریتم رمزگذاری تعریف کردند که نام این الگوریتم از حروف اول نام این سه نفر (Ron Rivest, Avi Shamir, Rich Aldeman) گرفته شده است. این الگوریتم در روش رمزگذاری نامتقارن با کلید عمومی بسیار کاربرد دارد و با دو کلید رمز عمومی و خصوصی کار می‌کند. امنیّت این روش بر مبنای اعداد بسیار بزرگ است. اندازه کلید رمز مورد استفاده درRSA، بسیار متغیر است. ولی در حالت عادی طول آن ۵۱۲ بیت می‌باشد. در مواقعی که خطر کشف کلید وجود دارد یا هنگامی که نیاز است تا امنیت کلید طی سال‌های زیادی تامین گردد از کلیدهایی با طول ۱۰۲۴ بیت تا ۲۰۴۸ بیت استفاده می‌شود. الگوریتم RSA یکی از معتبرترین الگوریتم‌ها در رمزگذاری است [10].

■ روش رمزگذاری یک طرفه:

در این روش همان‌طور که از نام آن پیداست، رمزگشایی در طرف دیگر انجام نمی‌گیرد و امکان آن وجود ندارد و تحلیل الگوریتم رمزگذاری و دستیابی به اصل پیام رمز شده تنها در یک طرف امکان‌پذیر است. این روش بطور گسترده مورد استفاده قرار نگرفته است و اولین‌بار برای ذخیره‌کردن اطلاعات نظیر کلمه عبور (Password) در سیستم‌های NT و UNIX و یا اطلاعات شخصی در کارت‌های اعتباری ATM به کار برده شد. یکی دیگر از مثال‌های استفاده از این روش در تعریف امضای دیجیتالی است که در بخش بعدی در مورد آن توضیح داده خواهد شد.

■ الگوریتمSHA :

این روش شامل الگوریتمی است که گیرنده را از تغییر و تحریف پیام مطمئن می‌کند. در بعضی از موارد استفاده‌کنندگان اطلاعات علاوه بر پنهان‌ماندن پیام (رمزنگاری)، مایلند که اطلاعات طی

[1] Data encryption standard

فرآیند ارسال تحریف نشوند. لذا برای اینکه گیرنده از عدم دستکاری اطلاعات در حین ارسال اطمینان حاصل نماید، با استفاده از این الگوریتم خلاصه‌ای از متن اصلی فراهم شده و به همراه آن ضمیمه می‌گردد. البته خلاصه مذکور ابتدا درهم سازی شده و سپس رمزگذاری می‌شود و در حقیقت چکیده رمزگذاری شده به پیام اصلی ضمیمه می‌گردد. گیرنده نیز پس از دریافت پیام، چکیده را رمزگشایی و آن را با اصل پیام تطبیق می‌دهند. لازم به ذکر است، با پیشرفت کاربرد الگوریتمهای رمزگذاری روش ها و الگوریتم های جدیدتری نیز پیشنهاد شده اند ولی در این مقاله ما به رایج ترین این الگوریتم ها در کاربردهای فناور محور، حوزه تجارت الکترونیک و خدمات مرتبط پرداختیم.

قدرت امنیتی الگوریتم های رمزگذاری رایج

الگوریتم‌های به کار رفته در کاربردهای رمزنگاری بسته به نوع الگوریتم و طول کلید دارای قدرت‌های امنیتی متفاوت هستند. دو الگوریتم دارای قدرت امنیتی برابر هستند اگر میزان عملیات مورد نیاز برای شکستن الگوریتم‌ها یا میزان عملیات مورد نیاز برای به دست آوردن کلید برای آن‌ها برابر باشد .قدرت امنیتی الگوریتم‌ها به طور معمول بر حسب میزان عملیات مورد نیاز برای شکستن یک الگوریتم رمز متقارن که بهترین حمله برای آن حمله جستجوی کامل فضای کلید است، بیان می‌شود. به عنوان مثال هنگامی که گفته می‌شود قدرت امنیتی یک الگوریتم (رمز متقارن، رمز نامتقارن، امضای دیجیتال، MAC، تابع چکیده ساز، پروتکل امنیتی، مولد عدد تصادفی یا n بیت است، این به این معناست که عملیات مورد نیاز برای شکستن الگوریتم معادل است با عملیات مورد نیاز برای شکستن یک الگوریتم رمز متقارن با کلید n بیتی که بهترین حمله به آن، حمله جستجوی کامل فضای کلید است. مقادیری که در ادامه برای قدرت امنیتی الگوریتم‌های مختلف بیان می‌شود، با توجه به پیشرفت‌های کنونی، مشخص شده‌اند. طبیعی است که اگر به عنوان نمونه در روش فاکتورگیری اعداد بزرگ پیشرفت‌های چشمگیری به دست آیند، مقادیری که برای قدرت امنیتی رمز و امضای دیجیتال RSA ذکر شده‌اند، به نسبت پیشرفت حاصل شده، کاهش می‌یابند. جدول ۱ قدرت امنیتی الگوریتم‌های رمز متقارن استاندارد AES (Rijndael با طول قالب ۱۲۸ بیت) با کلیدهای ۱۲۸، ۱۹۲ و ۲۵۶ بیت، 2TDEA (TDESدو کلیدی) و 3TDEA (TDESسه کلیدی) و الگوریتم‌های رمز نامتقارن RSA(و دیگر الگوریتم‌های مبتنی بر لگاریتم گسسته در میدان محدود نظیر DSA و دیفی-هلمن) را بیان می‌دارد. الگوریتم‌های رمز متقارن مذکور در جدول ۱ استاندارد و رایج و کاربردی می باشند [7, 10, 11].

جدول ۱. قدرت امنیتی الگوریتم‌های رمز متقارن و نامتقارن

RSA	(DSA، دیفی-هلمن و ...)	الگوریتم‌های رمز متقارن	قدرت امنیتی بر حسب بیت
پیمانه ۱۰۲۴ بیتی	پیمانه ۱۰۲۴ بیتی	TDEA۲	۸۰
پیمانه ۲۰۴۸ بیتی	پیمانه ۲۰۴۸ بیتی	TDEA۳	۱۱۲
پیمانه ۳۰۷۲ بیتی	پیمانه ۳۰۷۲ بیتی	AES-128	۱۲۸
پیمانه ۷۶۸۰ بیتی	پیمانه ۷۶۸۰ بیتی	AES-192	۱۹۲
پیمانه ۱۵۳۶۰ بیتی	پیمانه ۱۵۳۶۰ بیتی	AES-256	۲۵۶

برای توابع چکیده‌ساز قدرت امنیتی چکیده‌ساز با توجه به کاربردی که چکیده‌ساز را به کار می‌برد، تعیین می‌گردد. بنابراین بسته به قدرت امنیتی مورد نیاز کاربرد، باید تابع چکیده‌ساز با قدرت امنیتی مناسب استفاده شود. برای مثال در امضای دیجیتال با توجه به قدرت امنیتی مورد نیاز کاربرد باید اندازه پیمانه و تابع چکیده‌ساز متناسب به کار گرفته شود. اگر برای امنیت ۱۱۲ بیتی از امضای دیجیتال RSA با پیمانه ۲۰۴۸ بیتی استفاده شود، ولی چکیده‌ساز به کار گرفته شده در امضا دارای امنیت ۸۰ بیت باشد، امنیت امضا نیز بیشتر از ۸۰ بیت نخواهد بود. جدول ۲ قدرت امنیت خانواده توابع چکیده‌ساز SHA را در کاربردهای مختلف نشان می‌دهد. توابع چکیده‌ساز مذکور در جدول ۲ استاندارد بوده و عموما استفاده از توابع چکیده‌ساز دیگر مرسوم نیست.

جدول ۲. قدرت امنیتی توابع چکیده‌ساز در کاربردهای مختلف

الگوریتم	تابع استخراج کلید و مولد عدد تصادفی	HMAC	امضای دیجیتال و تابع چکیده ساز
SHA-1	۱۶۰	۱۶۰	۸۰
SHA-224	۲۲۴	۲۲۴	۱۱۲
SHA-256	۲۵۶	۲۵۶	۱۲۸
SHA-384	۳۸۴	۳۸۴	۱۹۲
SHA-512	۵۱۲	۵۱۲	۲۵۶

به عنوان جمع‌بندی امنیت تابع چکیده‌ساز هنگامی که در امضای دیجیتال به کار رود یا خود به صورت مجزا استفاده شود، در حالت ایده آل نصف طول خروجی است. امنیت تابع چکیده‌ساز هنگامی که در HMAC، مولد عدد تصادفی یا تابع استخراج کلید به کار رود، در حالت ایده‌آل برابر طول خروجی آن می‌باشد. به عنوان نمونه به منظور داشتن امضای دیجیتال RSA با امنیت ۱۱۲۲ بیتی طول پیمانه RSA حداقل باید ۲۰۴۸ بیتی و چکیده‌ساز مورد استفاده در آن نیز باید دارای امنیت حداقل ۱۱۲ بیت باشد [12]. برای مثال SHA-224 برای این کاربرد مناسب است، ولی SHA-1 برای امضای دیجیتال با امنیت ۱۱۲۲ بیت دارای امنیت کافی نیست.

نتیجه گیری

همانطور که در مقاله حاضر بحث شد، سیستم های رمزنگاری در حال حاضر به دو حوزه مطالعاتی مهم شامل رمزنگاری متقارن و نامتقارن تقسیم می‌شوند. بحثهای زیادی شده که کدام یک از الگوریتم‌های بررسی شده در مقاله حاضر بهترند، اما درواقع جواب مشخصی برای این سوال وجود ندارد. البته براساس بررسی های انجام شده محققان به این نتیجه رسیدند که طول پیغامی که با الگوریتم‌های متقارن میتواند رمزنگاری شود از الگوریتم‌های نامتقارن کمتر است. همچنین با تحقیق به این نتیجه رسیدند که الگوریتم‌های متقارن الگوریتم‌های بهینه تری هستند. اما وقتی که بحث امنیت پیش می آید الگوریتم‌های نامتقارن کارایی بیشتری دارند. به طور خلاصه می‌توان گفت که الگوریتم‌های متقارن دارای سرعت بالاتر و الگوریتم‌های نامتقارن دارای امنیت بهتری هستند. در ضمن گاهی از سیستم ترکیبی از هر دو الگوریتم استفاده می‌کنند که به این الگوریتم‌ها الگوریتم های ترکیبی گفته می‌شود. اما اگر به طور دقیق تر به این دو نگاه کنیم آنگاه متوجه خواهیم شد که الگوریتم‌های نامتقارن و الگوریتم‌های کلید متقارن دارای دو ماهیت کاملاً متفاوت هستند و کاربردهای متفاوتی دارند به طور مثال در رمزنگاریهای ساده که حجم داده‌ها بسیار زیاد است از الگوریتم متقارن استفاده می‌شود، زیرا داده‌ها با سرعت بالاتری رمزنگاری و رمزگشایی می‌شوند. اما در پروتکل هایی که در اینترنت استفاده می‌شود، برای رمز نگری کلید هایی که نیاز به مدیریت دارند از الگوریتم‌های نامتقارن استفاده می‌شود.

مراجع

[1] Lima, M. N., dos Santos, A. L., & Pujolle, G. (2009). A survey of survivability in mobile ad hoc networks. Communications Surveys & Tutorials, IEEE, 11(1), 66–77.

[2] Jamali, S. B. S. (2015). A survey over black hole attack detection in mobile ad hoc network. International Journal of Computer Science and Network Security (IJCSNS), 15, 44.

[3] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. Wireless Networks, 20, 2481–2501.

[4] Yan, Z., Zhang, P., & Vasilakos, A. V. (2015). A security and trust framework for virtualized networks and software-defined networking. Security and Communication Networks, 8(13). doi:10.1002/sec.1243.

[5] Ioannis, K., Dimitriou, T., & Freiling, F. C. (2007). Towards intrusion detection in wireless sensor networks. In Proceedings of the 13th European wireless conference.

[6] Khemariya, N., & Khuntetha, A. (2013). An efficient algorithm for detection of blackhole attack in AODV based MANETs. International Journal of Computer Applications, 66(18), 18–24

[7] Tsai, C., Lai, C., & Vasilakos, V. (2014). Future internet of things: Open issues and challenges. ACM/Springer Wireless Networks,. doi:10.1007/s11276-014-0731-0.

[8] Wan, J., Yan, H., Suo, H., & Li, F. (2011). Advances in cyber-physical systems research. KSII Transactions on Internet and Information Systems, 5(11), 1891–1908.

[9] Montenegro, G., & Castelluccia, C. (2004). Crypto-based identifiers (CBIDs): Concepts and applications. ACM Transactions on Information and System Security, 7(1), 97–127.

[10] Xu, X. H. (2013). Study on security problems and key technologies of the internet of things. In Proceedings of the IEEE international conference on computing and information sciences (ICCIS) (pp. 407–410).

[11] Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: a review. In Proceedings of the IEEE international conference on computer science and electronics engineering (ICCSEE), (vol. 3, pp. 648–651).

[12] Liu, B., Chen, H., Wang, H. T., & Fu, Y. (2012). Security analysis and security model research on IoT. Computer & Digital Engineering, 40(11), 21–24.

[13] Yang, G., Xu, J., Chen, W., Qi, Z. H., & Wang, H. Y. (2010). Security characteristic and technology in the internet of things. Journal of Nanjing University of Posts and Telecommunications (Natural science), 4, 20–29.

[14] Malan, D. J., Welsh, M., & Smith, M. D. (2004). A public-key infrastructure for key distribution in tinyOS based on elliptic curve cryptography. In Proceedings of the IEEE international conference on sensor and ad hoc communications and networks SECON04 (pp. 71–80).