مقایسه الگوریتم های ریاضی و کلیدهای رمزنگاری با رویکرد انتظامی

سمیه حدادی[1] ، دکتر طاهر لطفی[2]

چکیده

در این پژوهش با روش تحقیق مقایسه ای (قیاسی) فرض کردیم a و b دو عدد مثبت باشند به طوری که $a>b$ باشد. در روش الگوریتم اقلیدسی برای یافتن بزرگترین عامل مشترک بین دو عدد a و b که با نماد $gcd(a,b)$ و یا به طور خلاصه به صورت (a,b) نمایش می دهند. الگوریتم را به این صورت بیان کردیم : ابتدا انتخاب می کنیم $r_0=a$ و $r_1=b$ داریم.

با اثبات قضیه های مختلف و در تحقیق انجام شده و بررسی و مقایسه الگوریتم های رمزنگاری، الگوریتم اقلیدسی و قضیه چینی و قضیه لاگرانژ مشخص شد الگوریتم اقلیدسی روش مناسب رمزنگاری اطلاعات برای مراکز نظامی و انتظامی می باشد. نتایج این تحقیق می تواند در طراحی الگوریتم های کدگذاری اطلاعات و داده های محرمانه و اسناد انتظامی کاربرد داشته باشد.

واژگان کلیدی: *الگوریتم رمزنگاری، کلید ریاضی، امنیت انتظامی داده ها*

[1] دانشجوی کارشناسی ارشد ریاضی کاربردی، دانشگاه آزاد اسلامی، واحد همدان somayeh.hadadi@gmail.com
[2] استادیار گروه ریاضی دانشگاه آزاد اسلامی، واحد همدان

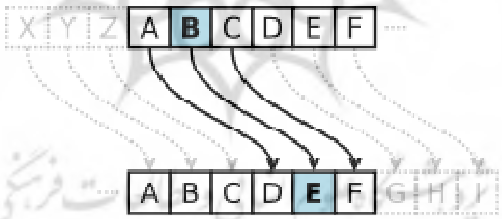
مقدمه

رمزنگاری یا Cryptography دانشی است که به بررسی و شناخت اصول و روش‌های انتقال یا ذخیره اطلاعات به صورت امن می‌پردازد. رمزنگاری دانش تغییر دادن متن پیام یا اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم رمز است، به صورتی که تنها شخصی که از کلید و الگوریتم مطلع است قادر به استخراج اطلاعات اصلی از اطلاعات رمز شده باشد. دانش رمزنگاری بر پایه مقدمات بسیاری از قبیل تئوری اطلاعات، نظریه اعداد و آمار بنا شده است و امروزه به طور خاص در علم مخابرات و مراکز نظامی و انتظامی مورد بررسی و استفاده قرار می‌گیرد. معادل رمزنگاری در زبان انگلیسی کلمه Cryptography است، که برگرفته از لغات یونانی kryptos به مفهوم «محرمانه» و graphien به معنای «نوشتن» است. در رمزنگاری محتویات یک متن به صورت حرف به حرف و در بعضی موارد بیت به بیت تغییر داده می‌شود و هدف تغییر محتوای متن است نه تغییر ساختار زبان شناختی آن. در مقابل کدگذاری تبدیلی است که کلمه‌ای را با یک کلمه یا نماد دیگر جایگزین می‌کند و ساختار زبان‌شناختی متن را تغییر می‌دهد. ریشه واژه Cryptography برگرفته از یونانی به معنای «محرمانه نوشتن متون» است. رمزنگاری پیشینه طولانی و درخشان دارد که به هزاران سال قبل برمی گردد. متخصصین رمزنگاری بین رمز و کد تمایز قائل می‌شوند. رمز عبارتست از تبدیل کاراکتر به کاراکتر یا بیت به بیت بدون آن که به محتویات زبان شناختی آن پیام توجه شود. در طرف مقابل، کد تبدیلی است که کلمه‌ای را با یک کلمه یا علامت دیگر جایگزین می‌کند. امروزه از کدها استفاده چندانی نمی‌شود اگر چه استفاده از آن پیشینه طولانی و پرسابقه‌ای دارد. موفق ترین کدهایی که تاکنون نوشته شده توسط ارتش ایالات متحده ابداع شده اند و در خلال جنگ جهانی دوم در اقیانوس آرام بکار گرفته شد. امروزه با توجه به اهمیت

گسترش توان دفاعی و امنیتی و از جمله آنها رمزنگاری در سیستم انتظامی و دفاعی کشور، این مسئله از اهمیت ویژه ای برخوردار که از چه شیوه ای می توان استفاده نمود تا امکان رمزگشایی را به حداقل ممکن کاهش داده و امنیت حفاظت اطلاعات را در علوم نظامی و انتظامی بالا ببریم.

بیان مساله

در بررسی نخستین استفاده کنندگان از تکنیک‌های رمزنگاری به سزار (امپراتور روم) و نیز الکندی که یک دانشمند مسلمان است برمی‌خوریم، که البته روش‌های خیلی ابتدایی رمزنگاری را ابداع و استفاده کرده‌اند. به عنوان مثال، با جابجا کردن حروف الفبا در تمام متن به اندازه مشخص آن را رمز می‌کردند و تنها کسی که از تعداد جابجا شدن حروف مطلع بود می‌توانست متن اصلی را استخراج کند.



شکل شماره ۱ : نمونه‌ای از روش رمزگذاری، رمز سزار که بر اساس جابجایی حروف الفبا می باشد.

اصول شش گانه کرکهف

آگوست کرکهف شهرت خود را از پژوهش های زبان شناسی و کتاب هایی که در این خصوص و زبان ولاپوک نوشته بود بدست آورد. او در سال ۱۸۸۳ دو مقاله با عنوان «رمزنگاری نظامی»

منتشر کرد. در این دو مقاله شش اصل اساسی وجود داشت که اصل دوم آن به عنوان یکی از قوانین رمزنگاری هنوز هم مورد استفاده دانشمندان در رمزنگاری پیشرفته است:

- سیستم رمزنگاری باید نه به لحاظ تئوری و در عمل غیر قابل شکست باشد.
- سیستم رمز نگاری باید هیچ نکته پنهان و محرمانه‌ای نداشته باشد. بلکه تنها چیزی که سری است کلید رمز است.
- کلید رمز باید به گونه ای قابل انتخاب باشد که اولاً بتوان به راحتی آن را عوض کرد و ثانیا بتوان آن را به خاطر سپرد و نیازی به یادداشت کردن کلید رمز نباشد.
- متون رمز نگاری باید از طریق خطوط شبکه های ارتباطی قابل انتقال باشند.
- دستگاه رمزنگاری یا اسناد رمز شده باید توسط یک نفر قابل حمل و نقل باشد.
- سیستم رمزنگاری باید به سهولت قابل راه اندازی باشد.

رمزنگاری پیشرفته

با پدید آمدن رایانه‌ها و افزایش قدرت محاسباتی آنها، دانش رمزنگاری وارد حوزه علوم رایانه گردید و این پدیده، موجب پیدایش سه تغییر مهم در مسائل رمزنگاری شد:

۱- وجود قدرت محاسباتی بالا این امکان را پدید آورد که روش‌های پیچیده تر و مؤثرتری برای رمزنگاری به وجود آید.

۲- روش‌های رمزنگاری که تا قبل از آن اصولا برای رمز کردن پیام به کار می‌رفتند، کاربردهای جدید و متعددی پیدا کردند.

۳- تا قبل از آن، رمزنگاری عمدتاً بر روی اطلاعات متنی و با استفاده از حروف الفبا انجام می‌گرفت، اما ورود رایانه باعث شد که رمزنگاری بر روی انواع اطلاعات و بر مبنای بیت های دیجیتال انجام شود.

تعاریف و اصطلاحات

عناصر مهمی که در رمزنگاری مورد استفاده قرار می‌گیرند به شرح زیر می باشد:

- متن آشکار :

پیام و اطلاعات را در حالت اصلی و قبل از تبدیل شدن به حالت رمز، متن آشکار یا به اختصار پیام می نامند. در این حالت اطلاعات قابل فهم توسط انسان است.

- متن رمز :

به پیام و اطلاعات بعد از درآمدن به حالت رمز، گفته می‌شود. اطلاعات رمز شده توسط انسان قابل فهم نیست.

- رمزگذاری (رمز کردن) :

عملیاتی است که با استفاده از کلید رمز، پیام را به رمز تبدیل می‌کند.

- رمزگشایی (باز کردن رمز) :

عملیاتی است که با استفاده از کلید رمز، پیام رمز شده را به پیام اصلی باز می‌گرداند. از نظر ریاضی، این الگوریتم برعکس الگوریتم رمز کردن است.

- کلید رمز :

اطلاعاتی معمولاً عددی است که به عنوان پارامتر ورودی به الگوریتم رمز داده می‌شود و عملیات رمزگذاری و رمزگشایی با استفاده از آن انجام می‌گیرد. انواع مختلفی از کلیدهای رمز در رمزنگاری تعریف و استفاده می‌شود.

پروتکل رمزنگاری

به طور کلی یک پروتکل رمزنگاری، مجموعه‌ای از قواعد و روابط ریاضی است که چگونگی ترکیب کردن الگوریتم های رمزنگاری و استفاده از آنها به منظور ارائه یک سرویس رمزنگاری در یک کاربرد خاص را فراهم می سازد. معمولاً یک پروتکل رمزنگاری مشخص می کند که : اطلاعات موجود در چه قالبی باید قرار گیرند، چه روشی برای تبدیل اطلاعات به عناصر ریاضی باید اجرا شود، کدامیک از الگوریتم های رمزنگاری و با کدام پارامترها باید مورد استفاده قرار گیرند، روابط ریاضی چگونه به اطلاعات عددی اعمال شوند، چه اطلاعاتی باید بین طرف ارسال کننده و دریافت کننده رد و بدل شود، چه مکانیسم ارتباطی برای انتقال اطلاعات مورد نیاز است. به عنوان مثال می‌توان به پروتکل تبادل کلید دیفی- هلمن برای ایجاد و تبادل کلید رمز مشترک بین دو طرف اشاره نمود.

الگوریتم رمزنگاری

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. اصطلاح الگوریتم رمزنگاری یک مفهوم جامع است و لازم نیست هر الگوریتم از این دسته، به طور مستقیم برای رمزگذاری اطلاعات مورد استفاده قرار گیرد، بلکه صرفاً وجود کاربرد مربوط به رمزنگاری مدنظر

است. در گذشته سازمان ها و شرک هایی که نیاز به رمزگذاری یا سرویس های دیگر رمزنگاری داشتند، الگوریتم رمزنگاری منحصر به فردی را طراحی می نمودند. به مرور زمان مشخص گردید که گاهی ضعف های امنیتی بزرگی در این الگوریتمپ ها وجود دارد که موجب سهولت شکسته شدن رمز می شود. به همین دلیل امروزه رمزنگاری مبتنی بر پنهان نگاه داشتن الگوریتم رمزنگاری منسوخ شده است و در روش های جدید رمزنگاری، فرض بر این است که اطلاعات کامل الگوریتم رمزنگاری منتشر شده است و آنچه پنهان است فقط کلید رمز است. بنابر این تمام امنیت حاصل شده از الگوریتم ها و پروتکل‌های رمزنگاری استاندارد، متکی به امنیت و پنهان ماندن کلید رمز است و جزئیات کامل این الگوریتم‌ها و پروتکل ها برای عموم منتشر می‌گردد. بر مبنای تعریف فوق، توابع و الگوریتم های مورد استفاده در رمزنگاری به دسته های کلی زیر تقسیم می شوند:

- توابع بدون کلید
- توابع درهم ساز
- تبدیل های یک‌طرفه
- توابع مبتنی بر کلید
- الگوریتم های کلید متقارن
- الگوریتم های رمز قالبی
- الگوریتم های رمز دنباله ای
- توابع تصدیق پیام
- الگوریتم های کلید نامتقارن
- الگوریتم های مبتنی بر تجزیه اعداد صحیح

- الگوریتم های مبتنی بر لگاریتم گسسته
- الگوریتم های مبتنی بر منحنی های بیضوی
- الگوریتم های امضای رقومی

الگوریتم های رمزنگاری بسیار متعدد هستند، اما تنها تعداد اندکی از آنها به صورت استاندارد درآمده‌اند.

رمزنگاری کلید متقارن

رمزنگاری کلید متقارن یا تک کلیدی، به آن دسته از الگوریتم ها، پروتکل ها و سیستم‌های رمزنگاری گفته می‌شود که در آن هر دو طرف رد و بدل اطلاعات از یک کلید رمز یکسان برای عملیات رمزگذاری و رمزگشایی استفاده می‌کنند. در این قبیل سیستم ها یا کلیدهای رمزگذاری و رمزگشایی یکسان هستند و یا با رابطه‌ای بسیار ساده از یکدیگر قابل استخراج می‌باشند و رمزگذاری و رمزگشایی اطلاعات نیز دو فرآیند معکوس یکدیگر می‌باشند. واضح است که در این نوع از رمزنگاری، باید یک کلید رمز مشترک بین دو طرف تعریف گردد. چون کلید رمز باید کاملاً محرمانه باقی بماند، برای ایجاد و رد و بدل کلید رمز مشترک باید از کانال امن استفاده نمود یا از روش‌های رمزنگاری نامتقارن استفاده کرد. نیاز به وجود یک کلید رمز به ازای هر دو طرف درگیر در رمزنگاری متقارن، موجب بروز مشکلاتی در مدیریت کلیدهای رمز می‌گردد.

رمزنگاری کلید نامتقارن

رمزنگاری کلید نامتقارن، در ابتدا با هدف حل مشکل انتقال کلید در روش متقارن و در قالب پروتکل تبادل کلید دیفی- هلمن پیشنهاد شد. در این نوع از رمزنگاری، به جای یک کلید مشترک، از یک زوج کلید به نام‌های کلید عمومی و کلید خصوصی استفاده می‌شود. کلید خصوصی تنها در اختیار دارنده آن قرار دارد و امنیت رمزنگاری به محرمانه بودن کلید خصوصی بستگی دارد. کلید عمومی در اختیار کلیه کسانی که با دارنده آن در ارتباط هستند قرار داده می‌شود. به مرور زمان، به غیر از حل مشکل انتقال کلید در روش متقارن، کاربردهای متعددی برای این نوع از رمزنگاری مطرح گردیده است. در سیستم های رمزنگاری نامتقارن، بسته به کاربرد و پروتکل مورد نظر، گاهی از کلید عمومی برای رمزگذاری و از کلید خصوصی برای رمزگشایی استفاده می‌شود و گاهی نیز، بر عکس، کلید خصوصی برای رمزگذاری و کلید عمومی برای رمزگشایی به کار می‌رود. دو کلید عمومی و خصوصی با یکدیگر متفاوت هستند و با استفاده از روابط خاص ریاضی محاسبه می گردند. رابطه ریاضی بین این دو کلید به گونه ای است که کشف کلید خصوصی با در اختیار داشتن کلید عمومی، عملاً ناممکن است.

مقایسه رمزنگاری کلید متقارن و کلید نامتقارن

اصولاً رمزنگاری کلید متقارن و کلید نامتقارن دارای دو ماهیت متفاوت هستند و کاربردهای متفاوتی نیز دارند. بنابر این مقایسه این دو نوع رمزنگاری بدون توجه به کاربرد و سیستم مورد نظر کار دقیقی نخواهد بود. اما اگر معیار مقایسه، به طور خاص، حجم و زمان محاسبات مورد نیاز باشد، باید گفت که با در نظر گرفتن مقیاس امنیتی معادل، الگوریتم‌های رمزنگاری متقارن خیلی سریع‌تر از الگوریتم‌های رمزنگاری نامتقارن می‌باشند.

الگوریتم اقلیدسی

فرض کنید a و b دو عدد مثبت باشند به طوری که $a>b$. الگوریتم اقلیدسی روشی است برای یافتن بزرگترین عامل مشترک بین دو عدد a و b که با نماد $gcd(a,b)$ و یا به طور خلاصه به صورت (a,b) نمایش می دهند. همچنین روشی برای یافتن معکوس یک عدد در هنگ عدد دیگر در صورت وجود می باشد. الگوریتم به صورت زیر بیان می شود :

ابتدا انتخاب می کنیم $r_0=a$ و $r_1=b$ داریم .

$r_0=q_1r_1+r_2 \qquad 0<r_2<r_1$

$r_1=q_2r_2+r_3 \qquad 0<r_3<r_2$

$r_{m-2}=q_{m-1}r_{m-1}+r_m \qquad 0<r_m<r_{m-1}$

$r_{m-1}=q_mr_m+0$

ثابت می کنیم :

$(a,b)=(r_0,r_1)=(r_1,r_2)=(r_2,r_3)=\dots(r_{m-1},r_m)$

برای این منظور ملاحظه می کنیم :

$(r_{m-1},r_m)=(q_mr_m,r_m)=r_m$

$(r_{m-2},r_{m-1})=(q_{m-1}r_{m-1}+r_m,q_mr_m)=(q_{m-1}q_mr_m+r_m,\ q_mr_m)\ )=(\ r_m(q_{m-1}q_m+r+1),q_mr_m)=r_m$

به همین ترتیب با ادامه این روش نتیجه حاصل می شود.

بدیهی است در صورتی که در الگوریتم مذکور $r_m=1$ باشد آنگاه a و b نسبت به هم اول بوده لذا معکوس b در هنگ a وجود دارد.

اکنون در تلاش محاسبه معکوس b در هنگ a هستیم، بر اساس دو دنباله متناهی r_i , q_i که از الگوریتم اقلیدسی حاصل می شود .

تعریف می کنیم :

$$t_j=\begin{cases} ۰ & \text{اگر } j=۰ \\ ۱ & \text{اگر } j=۱ \\ t_{j-2}-q_{j-1}t_{j-1} & \text{اگر } j\geq ۲ \end{cases}$$

و

$$s_j=\begin{cases} ۱ & \text{اگر } j=۰ \\ ۰ & \text{اگر } j=۱ \\ s_{j-2}-q_{j-1}s_{j-1} & \text{اگر } j\geq ۲ \end{cases}$$

قضیه :

برای $0\leq j\leq m$ داریم :

$$s_jr_0+r_j=t_jr_1=s_ja+t_jb$$

برهان : برای $j=0$ داریم :

$$r_0=s_0r_0+t_0r_1=r_0+0r_1=r_0$$

و برای $j=1$ نیز داریم :

$$r_1=s_1r_0+t_1r_1=0r_0+r_1=r_1$$

اکنون فرض کنید $i\geq ۲$ وحکم برای i-2 , i-1 برقرار باشد. ثابت می کنیم حکم برای i نیز صادق است. بنابر فرض استقرار داریم :

$r_{i-1}=s_{i-1}r_0+t_{i-1}r_1 \quad , \quad r_{i-2}=s_{i-2}r_0+t_{i-2}r_1$

در فرضیه مورد بررسی پرسش تحقیق عبارت است از : آیا عدد ۲۸ در هنگ ۷۵ معکوس دارد؟ در صورت وجود آن را به دست آورید.

جواب: ابتدا الگوریتم اقلیدسی را اعمال می کنیم تا ملاحظه شود r_m چه عددی حاصل می شود. اگر $r_m=1$ شود آنگاه ۲۸ در هنگ ۷۵ معکوس دارد و لذا t_m را بایستی به دست آورد، داریم :

$r_i=r_{i-2}-q_{i-1}r_{i-1}$

$s_i=s_{i-2}-q_{i-1}s_{i-1}$

$t_i=t_{i-2}-q_{i-1}t_{i-1}$

جدول شماره ۱ : آزمایش الگوریتم اقلیدسی

i	r_i	q_i	s_i	t_i
۰	$r_0=a=75$	-	۱	۰
۱	$r_1=b=28$	[۷۵/۸۰] = ۲	۰	۱
۲	$r_2=75-2*28=19$	[۲۸/۱۹] = ۱	۱-۲*۰=۱	۱-۲*۰=-۲
۳	$r_3=28-1*19=9$	[۱۹/۹] = ۲	۰-۱*۱=-۱	۱-۱*-۲=۳
٤	$r_4=19-2*9=1$	[۹/۱] = ۹	۳	-۸

ملاحظه می کنیم که $r_4=1$ لذا معکوس وجود دارد و طبق قضیه t_m معکوس b در هنگ a است. که در اینجا ۶۷ $tm= -8$

قضیه با قیمانده چینی (Chinese remainder theorem)

فرض کنیم $m_1,m_2,\ldots,m_r$ اعداد صحیح مثبت باشند. به طوری که دو به دو نسبت به هم اول باشند. فرض کنیم $a_1,a_2,\ldots,a_r$ نیز اعداد صحیح دلخواه باشند.

آن گاه دستگاه $X \equiv a_i \ , 1 \leq i \leq r$ فقط و فقط یک جواب در هنگ $M= m_1,m_2,\ldots,m_r$ دارد که برابر است با :

$$X=\sum_{i=1} a_i.M_i.y_i.$$

که در آن

$$y_i=M_i \mod m_i \ , \ M_i=\frac{M}{mi}$$

برهان : ثابت می کنیم تابع

$$\aleph: Z_M \rightarrow z_{m1} * z_{m2} * \ldots * z_{mr}$$

با ضابطه

$$\aleph(x)=(x \bmod m_1 \ , x \bmod m_2 \ ,\ldots,x \bmod m_r)$$

یک به یک و برو است. (برو بودن $\aleph$ تضمین می کند که برای هر $a_1,a_2,\ldots,a_r$ دستگاه دارای جواب است. یک به یک بودن تضمین می کند که جواب یکتاست).

اثبات برو بودن تابع $\aleph$

فرض کنید $(a_1,a_2,\ldots,a_r) \in z_{m1} * z_{m2} * \ldots z_{mr}$ دلخواه باشد. چون $M=m_1*m_2*\ldots*m_r$ و mi_r ها دو به دو نسبت به هم اول فرض شده اند لذا $M_i=M \mid m_i$ نسبت به m_i اول است در نتیجه معکوس M_i در هنگ m_i وجود دارد اگر آن را y_i بنامیم ادعا می کنیم :

$X=\sum_{i=1} a_i M_i y_i$ عضوی است که $\aleph(x)=(a_1 \dots a_r)$

برای این منظور ملاحظه می کنیم :

$$a_i M_i y_i \equiv_{m_i} a$$

و همواره برای $j \neq i$ داریم :

$$a_i M_i y_i \equiv_{m_i} 0$$

لذا $\aleph(x)=(a1,\dots,ar)$.

چون تعداد اعضای Z_m با تعداد اعضای $z_{m1} * z_{m2} * \dots * z_{mr}$ برابر است پس نتیجه می شود که $\aleph$ یک به یک نیز هست.

مثال تحقیق

فرض کنیم : $m_3=13$, $m_2=11$, $m_1=7$, $r=3$

آنگاه $M=m_1*m_2*m_3=1001$

داریم $M_3=77$, $M_2=91$, $M_1=\frac{M}{m_1}=\frac{۱۰۰۱}{۱۱}=۱۴۳$

و نیز $y_3=12$, $y_2=4$, $y_1=5$

آنگاه $\aleph^{-1} : Z_7*Z_{11}*Z_{13} \rightarrow Z_{1001}$

با ضابطه $\aleph^{-1}(a_1,a_2,a_3)=\sum_{i=1}^{r} M_i y_i a_i=715a_1+364a_2+924a_3 \bmod ۱۰۰۱$

اکنون اگر $a_1=5$ و $a_2=3$ و $a_3=10$ انتخاب کنیم آنگاه :

$$\aleph^{-1}(5,3,10)=715*5+346*3+924*10 \bmod 1001=894 \bmod 1001=894$$

لذا $894\equiv ۵$ و $894\equiv ۳$ و $894\equiv ۱۰$

نتیجه گیری

با توجه به نتایج به دست آمده و مقایسه الگوریتم های مختلف رمزنگاری و ضریب امنیت آنها، پیشنهاد می گردد مراکز انتظامی و پلیسی جهت کاربرد الگوریتم مناسب رمزنگاری با علم اعداد، الگوریتم اقلیدسی را مورد استفاده قرار دهند. در روش الگوریتم اقلیدسی برای یافتن بزرگترین عامل مشترک بین دو عدد a و b که با نماد gcd(a,b) و یا به طور خلاصه به صورت (a,b) نمایش می دهند. الگوریتم را به این صورت بیان کردیم : ابتدا انتخاب می کنیم $r_0=a$ و $r_1=b$ داریم. امنیت رمزنگاری بر اساس پنهان ماندن کلید است نه الگوریتم مورد استفاده. در حقیقت، با فرض اینکه الگوریتم از قدرت کافی برخوردار است تنها روش درک متن اصلی برای یک استراق سمع کننده، کشف کلید است. در بیشتر حملات، حمله کننده تمام کلیدهای ممکن را تولید و روی متن رمز شده اعمال می‌کند تا در نهایت یکی از آنها نتیجه درستی دهد. تمام الگوریتم های رمزنگاری در برابر این نوع حمله آسیب پذیر هستند، اما با استفاده از کلیدهای طولانی تر، می توان کار را برای حمله کننده مشکل تر کرد. با اثبات قضیه های مختلف و در تحقیق انجام شده و بررسی و مقایسه الگوریتم های رمزنگاری، الگوریتم اقلیدسی و قضیه چینی و قضیه لاگرانژ مشخص شد الگوریتم اقلیدسی روش مناسب رمزنگاری اطلاعات برای مراکز نظامی و انتظامی می باشد.

فهرست منابع

- باقری، محمد (۱۳۸۳). رمزنگاری با کلید عمومی، دانشگاه امام حسین (ع).

- ذاکر الحسینی، علی. امنیت داده ها، انتشارات نص.

- رمضانیان، رحیم و همکاران، آشنایی با نظریه اطلاع، رمز نگاری و کدگذاری، دانشگاه فردوسی مشهد، طرح پژوهشی قطب.

- Vera Pless (1982), Introduction to the Theory of Error, Correcting Codes, John Wiley & Sons, Inc, ISBN: 08684-471-003

- Elwyn R. Berlekamp (1984), Algebraic Coding Theory ,Aegean Park Press) revised edition, ISBN: 8-063-89412-0

- Randy Yates ,A Coding Theory Tutorial.