
بسم الله الرحمن الرحيم

دانشکده علوم ریاضی
گروه ریاضی محض

**پایان‌نامه کارشناسی ارشد ریاضی گرایش محض**

عنوان:

# دوگان RSA و تحلیل امنیت آن

استاد راهنما:
دکتر محمد غلامی

استاد مشاور:
دکتر مرتضی هیودی

توسط:
سمیه مرادی

اسفند ۹۰

از حمایت علمی پژوهشی و مالی

مرکز تحقیقات مخابرات ایران

کمال تشکر و سپاس را دارم.

**تقدیم به :**

## حضرت ولی عصر (عج)

و

**پدرم،**

که بزرگوارانه با مهر پدری، خستگی‌هایم را زدود و با لطف بی‌حدش مهرورزی را به من آموخت.

**مادرم،**

دریای بی‌کران فداکاری و عشق که وجودم برایش همه رنج بود و وجودش برایم همه مهر و دعایش مرا به قبله‌ی ایمان رهنمون نمود.

**استاد ارجمندم دکتر محمد غلامی**

که از نگاهش صلابت، از رفتارش محبت و از صبرش ایستادگی آموختم.

# تشکر و قدردانی

خداوند منان را شاکرم که بار دیگر در به پایان رساندن برگی دیگر از دفتر زندگی‌ام مرا یاری نمود.

در ابتدا از خانواده‌ی عزیزم بخصوص **پدر و مادرم** تشکر می‌کنم، مهربان فرشتگانی که لحظات ناب جسارت خواستن، عظمت رسیدن و تمام تجربه‌های یکتا و زیبای زندگیم، مدیون حضور سبز آن‌هاست. آغاز به تحصیل در دانشگاه شهرکرد همزمان شد با مقطعی از زندگی‌ام که آمیخته با غم و شادی و خوف و رجاء بود. آفتابی سوزان می‌سوزاند و در عین حال سایه‌هایی دلپذیر از دوستی‌های پاک و بی‌آلایش مرا به خود می‌خواند. شرجی شیون نفس می‌برید و لیکن نسیم مهربانی هم می‌وزید. قصه کوتاه می‌کنم که این جهان از پیشینیان به امثال من رسید و بر من نیز نخواهد ماند. پس در غم‌ها صبر کردم. در عتاب این روزگار کسی دست مرا گرفت، استادی که ازو درس‌های بسیار آموختم: **جناب آقای دکتر محمد غلامی**. تدبیر، آرامش روان و آزادگی، خصلت مدام او بود. آنچه که در این پژوهش به‌دست آورده‌ام بی‌مدد ایشان ممکن نبود. صمیمانه‌ترین مراتب سپاس خود را به ایشان تقدیم نموده و از اکنون تا همیشه خود را سپاسگزار همراهی‌های بی‌دریغ ایشان می‌دانم.

از **جناب آقای دکتر مرتضی هیودی** به عنوان استاد مشاور که با نظرات و رهنمودهای ارزشمندشان مرا یاری نمودند سپاسگزارم.

از داوران گرامی **جناب آقای دکتر علیرضا نقی‌پور** و **سرکار خانم دکتر ندا آهنجیده** که زحمت بازخوانی و داوری این پایان نامه را بر عهده گرفتند کمال تشکر را دارم.

در دوران تحصیل در این مقطع محضر استادی را درک کردم که آموزگاری، همراهی، همدلی را در هم آمیخته بود: سرکار خانم دکتر نها افتخاری را به پاس این ویژگی‌ها ستایش می‌کنم. اگر راهنمایی‌های ایشان در ابتدای این مقطع نبود شاید هرگز به این‌جا نمی‌رسیدم.

در پایان از دوستان و همکلاسی‌های عزیزم بخصوص خانم سکینه نظرپور که در این مدت مرا صمیمانه همراهی کردند، سپاسگزارم و از خداوند متعال موفقیت روز افزون آنان را خواهانم.

یا رب از ابر هدایت برسان بارانی

پیشتر زانکه چو گردی زمیان برخیزم

سمیه مرادی

اسفند ماه ۱۳۹۰

# چکیده

در این پایان نامه ابتدا به بررسی سیستم رمزی RSA و گونه‌های سریع آن می‌پردازیم. سپس گونه‌های جدیدی از RSA را ارائه می‌دهیم که الگوریتم تولید کلید آن‌ها دو جفت کلید RSAی متمایز با نماهای عمومی و خصوصی یکسان تولید می‌کند. این خانواده از گونه‌های RSA که دوگان RSA نامیده می‌شوند، می‌توانند در طرح‌هایی که نیاز به استفاده از دو سیستم RSAی متمایز باشد با برتری کاهش حافظه‌ی مورد نیاز برای ذخیره‌ی کلیدها استفاده شوند. دو کاربرد دوگان RSA، امضاهای کور و صحت/محرمانگی را بررسی می‌کنیم. هم‌چنین به بررسی امنیت دوگان RSA می‌پردازیم. کران‌های امنیتی در دوگان RSA با نمای عمومی کوچک، دوگان RSA با نمای خصوصی کوچک و دوگان RSAی متعادل تعمیم‌یافته نسبت به RSAی اصلی افزایش می‌یابند.

## کلمات کلیدی

رمزنگاری، رمزگذاری، پایه‌ی کاهش‌یافته‌ی مشبکه، الگوریتم LLL، RSAی متعادل، RSA، دوقلوی RSA

# فهرست مطالب

# فهرست نمادها

| | |
|---|---|
| مجموعه‌ی اعداد صحیح | $\mathbb{Z}$ |
| بی نهایت | $\infty$ |
| به ازای هر | $\forall$ |
| وجود دارد | $\exists$ |
| مجموع | $\sum$ |
| ماکزیمم | $\max$ |
| نرم | $\|.\|$ |
| دترمینان | $\det$ |
| نمای خصوصی | $d$ |
| نمای عمومی | $e$ |
| مشبکه‌ی $L$ | $L$ |
| نماد اُ بزرگ | $O$ |
| پیمانه‌ی RSA | $N$ |
| ضرب داخلی | $\langle . \ , \ . \rangle$ |
| قضیه‌ی باقی‌مانده‌ی چینی | CRT |
| سیستم رمزی RSA | RSA |
| متن رمزی $C$ | $C$ |
| متن ساده‌ی $M$ | $M$ |
| فضای تولید شده توسط $\{v_1, \dots, v_n\}$ | $\text{span}\{v_1, \dots, v_n\}$ |
| جابه‌جا کردن $x$ و $y$ | swap(x,y) |
| کوچک‌ترین عدد صحیح بزرگ‌تر از $x$ | $\lceil x \rceil$ |

# مقدمه

هدف از ارائه‌ی این پایان نامه معرفی سیستم‌های رمزنگاری است که حافظه‌ی مورد نیاز برای ذخیره‌ی کلیدها را کاهش می‌دهند. این پایان نامه در چهار فصل تدوین شده است که بیشتر مطالب آن بر گرفته از مقالات [۳]، [۱۱] و [۱۶] می‌باشد.

فصل اول، پیش نیاز فصل‌های دیگر است که در آن ابتدا تاریخچه‌ای از رمزنگاری را بیان می‌کنیم. سپس به بیان تعاریف و قضایای مقدماتی می‌پردازیم. بیشتر مطالب مورد نیاز در رمزنگاری از نظریه‌ی اعداد بهره می‌گیرد.

سیستم رمزی RSA یکی از سیستم‌های کلید عمومی یا رمز نامتقارن می‌باشد. این سیستم در سال ۱۹۷۷ توسط ریوست[۱] ، شامیر[۲] و آدلمن[۳] معرفی شد که شامل پیمانه‌ی $N = pq$، نمای عمومی $e$ و نمای خصوصی $d$ می‌باشد. در فصل دوم، این سیستم و گونه‌های سریع آن را معرفی می‌کنیم، یعنی نمونه‌هایی از RSA که سرعت رمزگشایی در آن‌ها نسبت به RSAی اصلی بالاتر است. هر نمونه شامل سه الگوریتم تولید کلید، رمزگذاری و رمزگشایی می‌باشد. برای مقایسه‌ی این نمونه‌ها با یکدیگر زمان اجرای رمزگشایی آن‌ها را بررسی می‌کنیم. یکی از مهم‌ترین نمونه‌های RSA، RSAی متعادل است که در آن رمزگشایی با استفاده از قضیه‌ی باقی‌مانده‌ی چینی انجام می‌شود. این نمونه اولین بار در سال ۱۹۹۰ توسط وینر[۴] معرفی شد.

در فصل سوم، سیستم رمزی دوگان RSA را معرفی کرده و گفته می‌شود که این سیستم از دو سیستم رمزی متمایز RSA با نمای عمومی و خصوصی یکسان و دو پیمانه‌ی متفاوت تشکیل می‌شود. این سیستم به دلیل داشتن نماهای عمومی و خصوصی یکسان حافظه‌ی مورد نیاز برای ذخیره‌ی کلیدها را

---

[۱] Rivest

[۲] Shamir

[۳] Adleman

[۴] Wiener

کاهش می‌دهد. این نمونه از RSA توسط سان[۵]، وو،[۶] تینگ[۷] و هینک[۸] در سال ۲۰۰۶ معرفی شد. هم‌چنین در این فصل دو کاربرد مهم آن را بیان می‌کنیم. دوگان RSA شامل سه نوع دوگان RSA با نمای عمومی کوچک یا طرح ۱، دوگان RSA با نمای خصوصی کوچک یا طرح ۲ و دوگان RSAی متعادل تعمیم‌یافته یا طرح ۳ می‌باشد.

در فصل چهارم، امنیت این سیستم را بررسی می‌کنیم، یعنی نشان می‌دهیم که نماهای عمومی و خصوصی باید در چه شرایطی صدق کنند تا دوگان RSA امن باشد. برای بررسی امنیت این سه طرح از دو ابزار ریاضی، کسرهای مسلسل و مشبکه استفاده می‌کنیم. در پایان مقایسه‌ی مختصری بین سه نوع سیستم رمزی دوگان RSA، دوقلوی RSA و (۲× RSA) انجام می‌دهیم.

---

[۵] Sun

[۶] Wu

[۷] Ting

[۸] Hinek

# فصل ۱

# مفاهیم و قضایای مقدماتی

## ۱.۱ تاریخچه

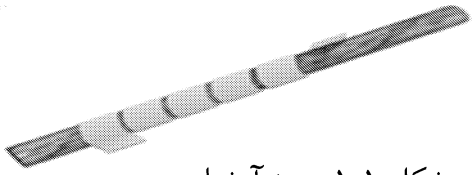
رمزنگاری از دو کلمه‌ی یونانی به مفهوم‌های محرمانه و نوشتن گرفته شده است. رمزنگاری عبارت است از یک نظام یا الگوی ریاضی – منطقی که بر اساس آن اطلاعات و مفاهیم آشکار و قابل فهم برای همگان، طبق روالی برگشت پذیر به اطلاعاتی نامفهوم و گنگ تبدیل می‌شود. این اطلاعات نامفهوم و گنگ توسط کسی که روال معکوس و پارامترهای لازم را می‌داند قابل برگشت و بهره برداری است.

رمزنگاری [۲۱] پیشینه‌ی تاریخی ۵۵۰۰ ساله دارد. ۳۵۰۰ سال قبل از میلاد با ابداع خط میخی توسط سومری‌ها که کسی تا قرن نوزدهم میلادی از مضمون آن چیزی نمی‌دانست دانشمندان زبان‌های باستانی موفق به رمزگشایی آن شدند. در همین دوران نیز خط هیروگلیف در مصر ابداع شد که دشوارتر از خط میخی بود.

اولین رگه‌های رمزنگاری متون به آثاری کشف شده از حدود ۱۹۰۰ سال قبل از میلاد بر می‌گردد، یعنی حدود ۱۶۰۰ سال پس از ابداع رسم الخط هیروگلیف. در پاپیروس‌های کشف شده از این دوران به نظر می‌رسد که از رسم الخط نامتعارف هیروگلیف (یعنی نظم نامتعارف در نوشتار) برای مخفی نگاه

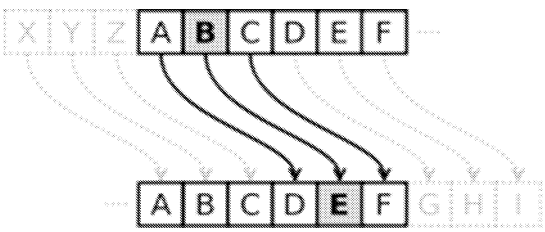
داشتن مضمون نوشته از بیگانگان و دشمنان، بهره گرفته شده است. در بین النهرین نیز از رمزنگاری برای مخفی نگه داشتن فرمول ساخت ظروف سفالی استفاده می‌شد.

۴۸۶ سال قبل از میلاد نیز یونانیان باستان با استفاده از نوشتن متن به صورت افقی روی نوار باریکی از پاپیروس یا چرم که به صورت اریب به دور یک چوب نازک و بلند پیچیده می‌شد برای مخفی نگه داشتن نوشته‌ها استفاده می‌کردند و تنها کسی می‌توانست آن را باز خوانی کند که چوبی با ضخامت و بلندی یکسان با چوب کاتب پیام داشته باشد. این روش منسوب به شاعر یونانی قرن هفتم میلادی به نام آرشیلوس می‌باشد. راز این روش تا حدود ۵۰۰ سال مخفی ماند تا سرانجام در ۱۲۰ سال قبل از میلاد برملا شد.



شکل ۱.۱: رمز آرشیلوس

اولین الگوی رمزنگاری ثبت شده در تاریخ، رمز سزار می‌باشد. ژولیوس سزار با ابداع روشی مبتنی بر جانشینی کاراکترها به ارسال پیام رمزنگاری شده برای فرماندهان سپاه خود، رسمیت بخشید، که در آن هر حرف از متن با حرفی که در جدول الفبا به اندازه‌ی $k$ حرف فاصله داشت، جانشین می‌شد. مثلاً با به کار بردن رمز سزار و کلید ۵ روی کلمه‌ی CRYPTOGRAPHY متن رمز HWDUYTLWFUMD حاصل می‌شود. رمز سزار تنها ۲۶ کلید به کار می‌برد. از این‌رو به سادگی می‌توان متن ساده را از روی متن رمز تعیین کرد. منظور از ۲۶ کلید همان اعداد $0, 1, \ldots, 25$ به ترتیب متناظر با حروف الفبای $A, B, \ldots, Z$ می‌باشد.




شکل ۲.۱: رمز سزار

۱۶۲۶ سال پس از میلاد یک روش رمزنگاری به نام رمز کبیر توسط روزینول در دربار لوئی چهاردهم ابداع شد که به جای حروف و اِعراب زبان فرانسه، اعداد جایگزین می‌شدند.

ساموئل مورس در سال ۱۸۴۵ کد مورس را که بیش از یک قرن کاربرد داشت، ابداع کرد. اختراع کد مورس با این هدف صورت گرفت که هر حرف الفبا با دنباله‌ای از علائم الکتریکی (شامل ۵ نماد مختلف) کد شده و بر روی یک رشته سیم واحد ارسال می‌شد. بدیهی است که در سمت گیرنده بایستی کد مورس توسط یک متخصص، بازخوانی و رمزگشایی می‌شد.

آگوست کرکهف به خاطر ۲ مقاله‌ی بسیار مهم که در سال ۱۸۸۳ در ژورنال علوم نظامی منتشر کرد در دنیای رمزنگاری مدرن شأن والایی یافت. اصول شش گانه‌ای که به نام خود او در تاریخ ثبت شده زیربنای روش‌های رمزنگاری مدرن قرار گرفت. اصل دوم آن به عنوان یکی از قوانین رمزنگاری هنوز مورد استفاده‌ی دانشمندان در رمزنگاری پیشرفته است.

این اصول از این قرارند.

۱) سیستم رمزنگاری اگر نه به لحاظ تئوری که در عمل غیر قابل شکست باشد.

۲) سیستم رمزنگاری باید هیچ نکته‌ی پنهان و محرمانه نداشته باشد، بلکه تنها چیزی که باید سری بماند کلید رمز است. (اصل اساسی کرکهف)

۳) کلید رمز باید به گونه‌ای قابل انتخاب باشد که اولاً بتوان به راحتی آن را عوض کرد و ثانیاً بتوان آن را به خاطر سپرد و نیازی به یاداشت کردن کلید رمز نباشد.

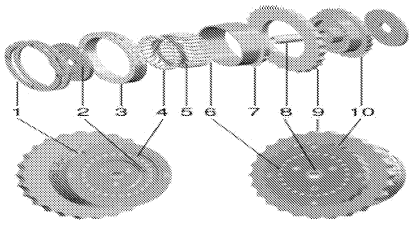
۴) متون رمزنگاری باید از طریق خطوط تلگراف قابل مخابره باشند.

۵) دستگاه رمزنگاری یا اسناد رمز شده باید توسط یک نفر قابل حمل و نقل باشد.

۶) سیستم رمزنگاری باید به سهولت قابل راه‌اندازی باشد.

در سال ۱۹۱۸ آرتورشربیورس دستگاهی به نام ماشین انیگما برای رمزنگاری اسناد محرمانه عرضه کرد که بر اساس چرخش یک سری روتور هم محور و یک سری اتصالات الکتریکی ساخته شده بود. بر روی روتورها حروف $A$ تا $Z$ حک شده بودند و هر روتور به ۲۶ اتصال الکتریکی مجهز بود. به ازای هر حرف که بر روی این ماشین تایپ می‌شد، حرفی در خروجی چاپ می‌شد که به موقعیت فعلی

روتور و وضعیت کنونی اتصالات وابسته بود.




شکل ۳.۱: ماشین انیگما

در سال ۱۹۴۹ کلود شانون با انتشار مقاله‌ی خود [۲۱] به مفهوم اتحاد رابطه‌ی مقدار حداقل اطلاعات رمز نشده‌ای را که می‌توان از معادل رمز شده‌ی آن استخراج کرد (با فرض دسترسی نفوذگر به منابع بی‌پایان مثل زمان و امکانات) پیشنهاد کرد. او با پایه گذاری تئوری اطلاعات کمک بزرگی به علم سایبرنتیک کرد که دانش رمزنگاری از آن بهره‌ی بی‌کران برد. رساله‌ی کارشناسی ارشد شانون بهترین پروژه‌ی قرن شناخته شده است.

سرویس اطلاعاتی انگلستان به رهبری جیمز الیس، کلیفورد کوک، مالکوم ویلیامسون، روش رمزنگاری کلید عمومی را ابداع ولی آن را مخفی نگاه داشتند. به همین دلیل نام آن‌ها در سایه نام ریوست، شامیر و آدلمن مخفی ماند، چرا که این سه نفر در دانشگاه MIT همین روش را به ثبت رسانده و به طور فراگیر اعلام کردند.

در سال ۱۹۷۱ هارست فیستل سیستم رمزنگاری متقارن خود، لوسیفر را در IBM ابداع و تکمیل کرد که بعدها پایه‌ی روش رمزنگاری DES شد. با معرفی تحقیقات فیستل درIBM، دامنه‌ی تحقیقات رمزنگاری به دانشگاه‌ها و مراکز تحقیقات غیر نظامی کشیده شد و توانست جای خود را به عنوان شاخه‌ای از دانش، در اذهان باز کند، چرا که تا قبل از این زمان، به دلیل اتصال آن با مراکز جاسوسی و اطلاعاتی، تحقیقات رمزنگاری با هاله‌ای از بدبینی مواجه بود. در سال ۱۹۷۷ ریوست، شامیر و آدلمن یک سیستم رمزنگاری با کلید عمومی را ابداع کردند که در آن فقط از مفهوم‌های مقدماتی نظریه اعداد استفاده می‌شود. این سیستم رمزنگاری RSA نامیده می‌شود که از نخستین حرف نام‌های خانوادگی ابداع کنندگان الگوریتم آن گرفته شده است. در سال‌های بعد نمونه‌هایی از RSA ساخته شد،

مثلاً در سال ۱۹۸۲ سیستم رمزی $\mathrm{RSA} - \mathrm{CRT}$ توسط کویز کواتر[۱] و کیوور[۲] ارائه شد و در سال ۱۹۹۷ سیستم رمزی RSA با پیمانه‌ای به شکل $\prod_{i=1}^{r} p_i$ توسط کالینس[۳] ارائه شد. هم‌چنین انواع دیگر RSA به منظور کاهش حافظه‌ی مورد نیاز برای ذخیره‌ی کلید ابداع شدند. مثلاً در سال ۲۰۰۵ نوعی از RSA به نام دوقلوی RSA توسط ویگر[۴] و لنسترا[۵] معرفی شد. در سال ۲۰۰۶ سان، وو، تینگ و هینک گونه‌ای از RSA به نام دوگان RSA را معرفی کردند.

## ۲.۱ مفاهیم مقدماتی

**تعریف ۱.۲.۱.**[۲۲] سیستم رمزی که کلیدهای رمزگذاری $e$ و رمزگشای $d$ متمایز بوده و محاسبه‌ی $d$ از روی $e$ سخت باشد را سیستم کلید عمومی یا رمز نامتقارن گویند.

در چنین سیستم‌هایی کلید رمزگذار $e$ را می‌توان به صورت همگانی اعلام نمود. اگر باب بخواهد یک پیغام رمزشده دریافت کند کلید رمزگذاری را به همگان اعلام نموده و کلید رمزگشای متناظر با آن یعنی $d$ را مخفی نگاه می‌دارد. هر کسی می‌تواند $e$ را به کار ببرد و متن رمز شده برای باب بفرستد. از این رو، $e$ را یک کلید عمومی می‌نامند. ولی تنها باب قادر به گشودن پیام‌ها می‌باشد و از این جهت $d$ یک کلید خصوصی نامیده می‌شود.

در سیستم‌های کلید عمومی هیچ نیازی به مبادله‌ی کلید بین افراد نیست. کلیدهای رمزگذاری در کتاب‌های راهنمای عمومی درج می‌شوند. اگر چه هر کسی می‌تواند این راهنما را بخواند، ولی این راهنما باید از نوشتن‌های غیر مجاز محافظت گردد. اگر حمله کننده، قادر به جایگزینی کلید عمومی آلیس با کلید خودش باشد، آن‌گاه می‌تواند پیام‌های ارسال شده برای آلیس را باز کند.

**اعداد تصادفی:** [۲۲] فرض کنیم یک مولد بیت تصادفی داریم که با توزیع یکنواختی بیت‌های

---

[۱] Quisquater

[۲] Couvreur

[۳] Collins

[۴] Weger

[۵] Lenstra

تصادفی تولید می‌کند. توضیح می‌دهیم که یک چنین وسیله‌ای چگونه اعداد تصادفی تولید می‌کند.

می‌خواهیم اعداد تصادفی با توزیع یکنواخت از مجموعه‌ی $\{۰, ۱, \dots, m\}$ که $m \in \mathbb{N}$ تولید کنیم. قرار می‌دهیم $n = \text{size } m = \lfloor \log\ m \rfloor + ۱$. سپس $n$ بیت تصادفی $b_n \dots, b_۲, b_۱$ را تولید می‌کنیم. اگر عدد $a = \sum_{i=۱}^{n} b_i ۲^{n-i}$ بزرگ‌تر از $m$ باشد، آن‌گاه این عدد را فراموش کرده و به روشی مشابه عدد دیگری تولید می‌کنیم، در غیر این صورت $a$ یک عدد تصادفی است. اگر بخواهیم اعداد $n$ – بیتی $(n \in \mathbb{N})$ تصادفی با توزیع یکنواخت تولید کنیم، آن‌گاه $n - ۱$ بیت تصادفی $b_n, \dots, b_۳, b_۲$ را تولید کرده و با فرض $b_۱ = ۱$ قرار می‌دهیم $a = \sum_{i=۱}^{n} b_i ۲^{n-i}$.

**اعداد اول تصادفی:** در بسیاری از سیستم‌های رمزنگاری با کلید عمومی، اعداد اول تصادفی به طول معین مورد نیاز هستند. ساخت چنین اعدادی را توضیح می‌دهیم.

می‌خواهیم عدد اول تصادفی به طول $k$ تولید کنیم. یک عدد $k$ بیتی تصادفی فرد طبق آن‌چه در بالا گفتیم تولید می‌کنیم. برای این منظور، اولین و آخرین بیت $n$ را برابر ۱ می‌گیریم. بقیه‌ی بیت‌ها به صورت تصادفی با توزیع احتمال یکنواخت انتخاب می‌شوند. سپس اول بودن آن را امتحان می‌کنیم.

**تعریف ۲.۲.۱.** اعداد اول $p$ و $q$ در RSA را متعادل گویند، هرگاه تقریباً هم‌اندازه باشند. به ویژه اگر در رابطه‌ی $\frac{۱}{۲} < \frac{p}{q} < ۲$ صدق کنند.

**تعریف ۳.۲.۱.** (اُ بزرگ $O$): فرض کنیم $f$ و $g$ دو تابع با دامنه‌ی اعداد صحیح مثبت باشند، گفته می‌شود $f = O(g)$ هرگاه

$$\exists\, c \in \mathbb{R}, n_۰ \in \mathbb{N} \qquad |f(n)| < c|g(n)| \qquad \forall\, n > n_۰.$$

**هزینه‌ی جمع، ضرب و تقسیم با باقی‌مانده:** در بسیاری از زمینه‌های رمزنگاری اعداد صحیح با دقت بالا جمع، ضرب و تقسیم می‌شوند. برای تخمین زمان اجرای چنین کاربردهایی باید مدت انجام چنین عملیاتی را مطالعه کنیم. بدین منظور مدل محاسباتی در نظر گرفته شده باید حتی‌الامکان شبیه به کامپیوترهای واقعی باشد. فرض کنیم $a$ و $b$ دو عدد صحیح مثبت با بسط دوتایی به ترتیب به طول $m$ و $n$ باشند و جمع دو رقم دوتایی در مدت زمان $O(۱)$ صورت پذیرد. در این صورت

کل عمل جمع در مدت زمان $\mathrm{O}(\max\{m,n\})$ انجام می‌شود. به روش مشابه تفریق $b-a$ در مدت زمان $\mathrm{O}(\max\{m,n\})$ محاسبه می‌شود. برای عمل ضرب نیز از روش ابتدائی استفاده می‌کنیم، مثلاً $a=۱۰۱۰۱$ و $b=۱۰۱$ را به این صورت ضرب می‌کنیم که عدد $b$ را از راست به چپ در نظر می‌گیریم. به ازای هر ۱ در $b$، عدد $a$ را به شکلی می‌نویسیم که رقم سمت راست آن در موقعیت ۱ در نظر گرفته از $b$ قرار گیرد. سپس این $a$ به نتیجه‌ی قبلی اضافه می‌شود. نتیجه برابر ۱۱۰۱۰۰۱ خواهد بود. چنین عمل جمعی در مدت زمان $O(m)$ صورت گرفته و تعداد جمع‌های مورد نیاز برابر $O(n)$ است. از این‌رو محاسبه در مدت زمان $O(mn)$ صورت می‌پذیرد.

در حالت کلی اگر $a$ و $b$ اعداد صحیح باشند داریم

۱) جمع $a$ و $b$ نیاز به مدت زمان $\mathrm{O}(\max\{\text{size } a,\text{size } b\})$ دارد.

۲) ضرب نمودن $a$ و $b$ در زمان $\mathrm{O}((\text{size } a)(\text{size } b))$ انجام می‌شود.

۳) تقسیم با باقی‌مانده $a$ به وسیله‌ی $b$ در زمان $\mathrm{O}((\text{size } b)(\text{size } q))$ انجام می‌شود که $q$ خارج قسمت است.

برای پیمانه‌ی $k$ – بیتی $n$، $0 \le m_1, m_2 \le n-1$ و عدد صحیح مثبت $c$ جدول ۱.۱ را داریم.

| عملیات مورد نظر | زمان اجرایی |
|---|---|
| $(m_1+m_2) \pmod n$ | $O(k)$ |
| $(m_1-m_2) \pmod n$ | $O(k)$ |
| $(m_1 m_2) \pmod n$ | $O(k^2)$ |
| $(m_1)^{-1} \pmod n$ | $O(k^3)$ |
| $(m_1)^c \pmod n$ | $O((\log c)\times k^2)$ |

جدول ۱.۱: زمان اجرایی

**زمان چندجمله‌ای:** [۲۲] در تجزیه و تحلیل یک الگوریتم رمزنگاری، باید نشان داد که آن الگوریتم دارای کارایی مؤثری بوده و در عین حال شکستن آن سخت است. فرض کنیم که $z_1, z_2, \ldots, z_n$ ورودی یک الگوریتم باشند. گفته می‌شود که زمان اجرای الگوریتم به صورت