به نام خدا

دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

پیاده‌سازی سریع سخت‌افزاری ضرب نقطه‌ای در امضای دیجیتال مبتنی بر خم بیضوی

پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر-معماری

محمد علی فرمهینی فراهانی

استادان راهنما

دکتر کیارش بازرگان، دکتر مهدی برنجکوب

۱۳۸۹

دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

پایان‌نامه‌ی کارشناسی ارشد رشته‌ی مهندسی کامپیوتر-معماری کامپیوتر **محمد علی فرمهینی فراهانی**

تحت عنوان

پیاده‌سازی سریع سخت‌افزاری ضرب نقطه‌ای در امضای دیجیتال مبتنی بر خم بیضوی

در تاریخ ۸۹/۴/۲۹ توسط کمیته‌ی تخصصی زیر مورد بررسی و تصویب نهایی قرار گرفت.

۱- استاد راهنمای پایان‌نامه — دکتر کیارش بازرگان

۲- استاد راهنمای پایان‌نامه — دکتر مهدی برنجکوب

۳- استاد مشاور پایان‌نامه — دکتر پژمان خدیوی

۴- سرپرست تحصیلات تکمیلی دانشکده — دکتر سید محمود مدرس هاشمی

بر خود لازم می‌دانم کـه از توجـه، راهنمـایی و تشـویق دوسـتان سپاسـگزاری کنم مخصوصاً آقایان احسان اعرابی، فواد فرنیا، عیسی اقبال و حسین رحمتی.

کلیه‌ی حقوق مادی مترتب بر نتایج مطالعات، ابتکارات و نوآوری‌های ناشی از تحقیق موضوع این پایان‌نامه (رساله) متعلق به دانشگاه صنعتی اصفهان است.

تقدیم به:

پدر و مادر عزیزم به خاطر تمام زحمات و فداکاریشان

فهرست مطالب

عنوان **صفحه**

چکیده

این تحقیق برآن است تا یک راه مناسب برای پیاده‌سازی سریع سخت‌افزاری ضرب نقطه‌ای در امضای دیجیتال مبتنی بر خم‌های بیضوی ارائه نماید. در هر سه بخش تولید کلید، تولید امضا و وارسی امضا، تنها چالش محاسباتی عملیات رمزنگاری خم‌های بیضوی، ضرب نقطه‌ای بر روی خم بیضوی در گستره میدان‌های متناهی می‌باشد. از این رو این پایان‌نامه به ارائه راهکارهایی به منظور بهینه سازی ضرب نقطه‌ای می‌پردازد که خود از دو قسمت جمع و دوبرابر کردن نقطه‌ای تشکیل شده است. برای انجام دو عمل جمع و دوبرابر کردن نقطه‌ای، با توجه به اینکه بعضی عملیات ریاضی در میدان‌های متناهی دودویی سریعتر قابل پیاده‌سازی بوده است، این میدان‌ها انتخاب شده‌اند. در این میدان‌ها نیاز به اعمال جمع، مجذور، کاهش، ضرب و معکوس گیری می‌باشد. با عنایت به اینکه عمل معکوس گیری زمانگیرترین عمل ریاضی در میان اعمال ذکر شده می‌باشد، مطابق روال متعارف بر آن شدیم تا به نحوی آن را با اعمال دیگر جایگزین کنیم که این مهم با تغییر مختصات به مختصات تصویری امکانپذیر است. در این تحقیق از مدل مختصات تصویری لوپز-دهاب استفاده می‌شود، زیرا در ازای برطرف کردن نیاز به عمل معکوس‌گیری، این روش کمترین تعداد ضرب چندجمله‌ای را به سیستم تحمیل می‌کند. بنابراین دیگر گلوگاه سیستم ضرب چندجمله‌ای می‌باشد که با ارائه راه‌حل‌های پیشنهادی سعی می‌شود بدون مصرف زیاد فضا، سرعت افزایش یابد. شایان ذکر است که پیاده‌سازی‌های این تحقیق روی تراشه‌ی FPGA، مدل Virtex2 xc2v2000 سنتز شده است. در این تحقیق میدان متناهی دودویی از مرتبه ۱۶۳ برگزیده شده است. بر اساس این انتخاب عملیات کاهش بهینه و از $O(1)$ ارائه شده است. معماری پیشنهادی برای مجذورگیری نیز از مرتبه زمانی $O(1)$ می‌باشد و در ضمن عمل کاهش که در ادامه مجذورگیری مورد نیاز است را نیز مرتفع کرده است. عمل جمع نیز یکی از اعمال پرکاربرد بوده که آن نیز از مرتبه زمانی $O(1)$ ارائه شده است. در نهایت مهمترین واحد عملیاتی یعنی ضرب چندجمله‌ای با عنایت به محدودیت فضایی، از مرتبه زمانی $O(n)$ طراحی شده و در نهایت خود واحد، نتیجه کاهش یافته را ارائه می‌نماید. در ادامه‌ی استفاده از این معماری‌ها و همچنین استفاده از مختصات تصویری و نیز کاستن تعداد یک‌های کلید خصوصی به وسیله روش NAF معماری پیشنهادی ما عمل ضرب نقطه‌ای را تقریبا در ۶۵ میکروثانیه انجام خواهد داد.

کلمات کلیدی: ۱- امضای دیجیتال ۲-پیاده‌سازی سخت‌افزاری ۳-بهینه‌سازی الگوریتم ۴-ضرب نقطه‌ای ۵-میدان‌های متناهی

فصل اول
مقدمه

مقدمه

رمزنگاری کلید عمومی در سال ۱۹۷۶ به وسیله ویتفیلد دیفی[۱] و مارتین هلمن[۲] معرفی شد و در سال بعد از آن اولین ارائه کاربردی آن توسط ران ریوست، آدی شامیر و لن آدلمن پیشنهاد شد که امروزه به نام رمزنگای RSA[۳] مشهور است. در این مدل رمزنگاری امنیت بر اساس سختی مسئله فاکتورگیری اعداد صحیح استوار است.

رمزنگاری خم بیضوی[۴] در سال ۱۹۸۵ به وسیله نیل کوبلیتز[۵] و ویکتور میلر[۶] اختراع شد. رمزنگاری خم بیضوی نیز مانند RSA بر مبنای کلید عمومی بوده و کارایی شبیه به RSA دارد ولی امنیت آن همانگونه که از اسم او بر می‌آید بر اساس سختی مسئله لگاریتم گسسته خم بیضوی[۷] می‌باشد. تاکنون بهترین الگوریتمی که جهت شکست مسئله لگاریتم گسسته خم بیضوی به کار گرفته شده است از پیچیدگی زمانی کاملا نمایی برخوردار بوده در صورتی که برای شکست مسئله فاکتورگیری اعداد صحیح الگوریتمی با پیچیدگی زمانی زیرنمایی قابل استفاده

---

[1] Whitfield Diffie
[2] Martin Hellman
[3] Rivest, Shamir, Adleman
[4] Elliptic Curve Cryptography (ECC)
[5] Neal Koblitz
[6] Victor Miller
[7] Elliptic Curve Discrete Logarithm Problem (ECDLP)

می‌باشد. این امر بدین معناست که جهت حصول سطح مطلوب از امنیت به طور محسوسی کلید رمزنگاری خم بیضوی نسبت به مدل RSA کوچکتر خواهد بود. مثلا به طور عمومی پذیرفته شده است که یک کلید ۱۶۰ بیتی خم بیضوی به اندازه یک کلید ۱۰۲۴ بیتی RSA امنیت ایجاد می کند. طول کلید کوچکتر می‌تواند روی سرعت، توان مصرفی، پهنای باند و حافظه مورد نیاز تاثیر به سزایی داشته باشد.

هدف پایان‌نامه

با توجه به استفاده روز افزون از برنامه‌های کاربردی که احتیاج به احراز اصالت دارند، نیاز به سیستم‌های کارا جهت احراز اصالت بیشتر از پیش احساس می‌شود. به همین منظور نیاز به الگوریتم‌هایی داریم که عمل امضای دیجیتال را بتوانند با سرعت بالا انجام دهند. از این رو طبق آنچه در بخش قبل به آن اشاره شد، می‌توان سطح مشخصی از امنیت را به وسیله کلیدی با طول کوتاهتر در امضای دیجیتال مبتنی بر خم‌های بیضوی نسبت به مدل-های مرسوم آن یعنی RSA و DSA [1] تامین کرد. حال اگر بخواهیم تعداد زیادی از جلسات امن را در آن واحد داشته باشیم، نیاز به پیاده‌سازی سخت‌افزاری این امضا می‌باشد. در این راستا این پایان‌نامه قصد دارد با استفاده از الگوریتم‌ها و معماری‌های کارآمد به یک پیاده‌سازی سخت‌افزاری سریع از امضای دیجیتال مبتنی بر خم‌های بیضوی دست یابد.

ساختار پایان‌نامه

این پایان‌نامه به نحوی که در ادامه آمده است سازماندهی شده است. فصل ۲ پیش‌زمینه‌های رمزنگاری، ریاضی وسخت‌افزاری جهت پیاده‌سازی امضای دیجیتال را ارائه خواهد نمود. به این ترتیب که ابتدا راجع به مبانی رمزنگاری نامتقارن بحث می‌شود. سپس به پیش‌زمینه‌های ریاضی مانند گروه، میدان، عملیات ریاضی روی میدان (جمع، مجذور، ضرب و معکوس‌گیری) و خم‌های بیضوی و عملیات روی خم‌های بیضوی اشاره می‌شود. پس از آن الگوریتم‌های امضای دیجیتال مبتنی بر خم بیضوی، تکنیک‌های سخت‌افزاری و در نهایت حمله‌ها و مقابله با حمله بیان خواهد شد. فصل ۳ به الگوریتم‌های مورد نیاز جهت امضای دیجیتال خواهد پرداخت. در این فصل ابتدا الگوریتم‌هایی جهت پیاده‌سازی عملیات مقدماتی ریاضی چندجمله‌ای (از قبیل جمع، تفریق، ضرب، کاهش و تقسیم روی میدان‌ها) اشاره خواهد شد. در ادامه راجع به الگوریتم‌هایی به منظور پیاده‌سازی ریاضیات خم‌های

[1] Digital signature algorithm

بیضوی بحث خواهیم کرد. فصل ۴ معماری مناسب برای پیاده‌سازی امضای دیجیتال ارائه خواهد نمود. به این ترتیب که برای تمام مواردی که در فصل‌های قبل به عنوان مباحث ریاضی یا الگوریتمی بیان شده‌اند، یک معماری کارا ارائه خواهد شد. در نهایت در فصل ۵ به ارائه نتیجه‌گیری و طرح پیشنهاداتی جهت ارتقا سرعت پیاده‌سازی امضای دیجیتال خواهیم پرداخت.

فصل دوم
پیش‌زمینه‌های رمزنگاری، ریاضی و سخت‌افزاری

مقدمه

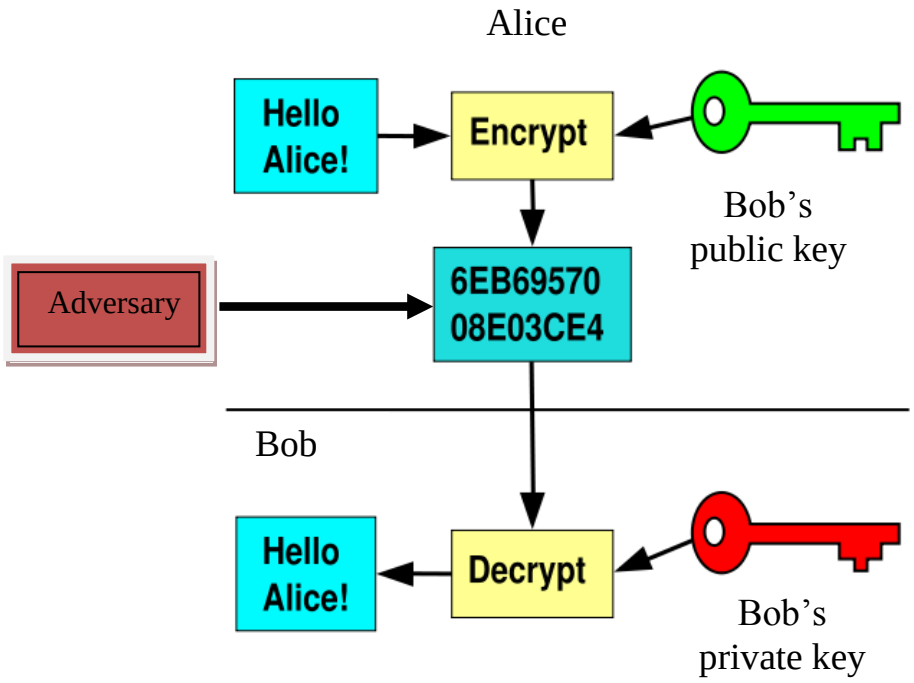
بلوک کلیدی در پیاده‌سازی رمزنگاری مبتنی بر خم‌های بیضوی ضرب نقطه‌ای است. پیاده‌سازی این ضرب مبتنی بر ریاضیات چند جمله‌ای‌ها و خم‌های بیضوی می‌باشد. همچنین برای حصول یک پیاده‌سازی بهینه آشنایی با سخت‌افزار مورد نیاز برای این کار الزامی است. بخش‌هایی که در ادامه خواهند آمد به شرح ذیل می‌باشند : مقدمات رمزنگاری کلید عمومی، پیش زمینه‌های ریاضی، عملیات ریاضی روی میدان‌های دودویی، معرفی خم‌های بیضوی، امضای دیجیتال به وسیله خم‌های بیضوی و در نهایت تکنیک‌های پیاده‌سازی

مبانی رمزنگاری کلید عمومی

رمزنگاری کلید عمومی[1] در سال ۱۹۷۶ توسط دیفی و هلمن معرفی شد مفهوم کلی رمزنگاری کلید عمومی که به آن رمزنگاری نامتقارن نیز می‌گویند، در شکل ۱.۲ نمایش داده شده است. در این نوع رمزنگاری همان گونه که در مرجع [۲] اشاره شده است، هر طرف باید یک زوج کلید شامل کلید عمومی و کلید خصوصی مرتبط با آن را برگزیند (کلید خصوصی باید به صورت مخفیانه حفظ شود). در مدل نامتقارن الزامی است که موجودیت‌ها

[1] Public Key Cryptography

کلیدهای عمومی را به صورت احراز اصالت شده برای یکدیگر ارسال نمایند. این زوج کلید باید دارای این خصوصیت باشند که با در دست داشتن کلید عمومی رسیدن به کلید خصوصی به لحاظ محاسباتی نشدنی باشد.



شکل۱.۲ . نمای کلی رمزنگاری کلید عمومی(نامتقارن)

در این تحقیق از نمادهای زیر به منظور ارائه مفاهیم اولیه رمزنگاری استفاده خواهد شد.

طرف اول ارتباط : Alice (A)

طرف دوم ارتباط : Bob (B)

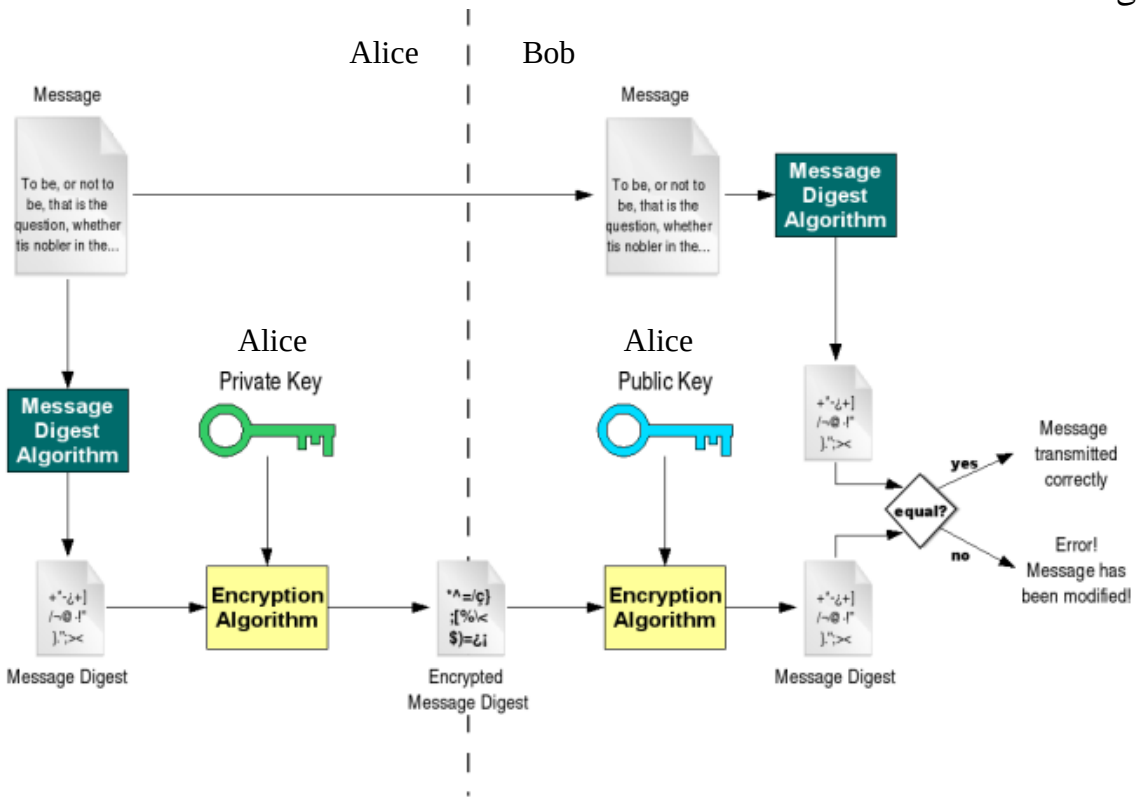
دشمن : Adversary(E)

کلید عمومی : Public Key

کلید خصوصی : Private Key

همان گونه که از شکل ۱.۲ مشخص است اگر بخواهیم از نوع نامتقارن به منظور رمز کردن یک پیام استفاده نماییم مکانیزم اجرایی این گونه است که طرف اول (A) باید از کلید عمومی B که در دسترس همگان می‌باشد برای رمزنگاری پیام مورد نظر استفاده نماید. این پیام رمز شده تنها به وسیله کلید خصوصی مرتبط با کلید عمومی مورد استفاده در فرایند رمزگذاری قابل رمزگشایی می‌باشد.

استفاده دیگر و مهمتر رمزنگاری نامتقارن امضای دیجیتال می‌باشد که بـه ایـن وسـیله مـی‌تـوان شـخص ارسـال کننده و پیام دریافت شده را احراز اصالت نمود. شکل ۲.۲ نحوه انجام امضا به وسیله رمزنگاری نامتقـارن را نمـایش می‌دهد.



شکل ۲.۲. نمای کلی امضای دیجیتال

همان گونه که در شکل مشاهده می‌کنید جهت امضا کردن یک متن طرف اول (A) نتیجه درهم شده متن مورد نظر را با کلید خصوصی خود رمز کرده و متن و نتیجه امضا را برای B ارسال می‌کند. B نیز ابتدا مـتن را درهـم کـرده و سپس امضای دریافت شده را با کلید عمومی A (کلید احراز اصالت شده) رمزگشایی مـی‌کنـد، اگـر نتیجـه حاصـل شده با آنچه که خود از درهم ساختن متن بدست آورده یکی باشد، بنابراین می‌تواند نتیجـه بگیـرد طـرف اول همـان کسی است که ادعا نموده است.

با توجه به اینکه اصولا رمزنگاری نامتقارن به لحاظ میزان توان محاسباتی مورد نیاز جهت تامین حـد مناسـبی از امنیت در مقایسه با نوع متقارن خود توان به مراتب بیشتری را طلب می‌کند، از این رو معمولا برای رمزنگـاری داده-های حجیم از رمزنگاری متقارن استفاده می‌شود و رمزنگاری نامتقارن بیشتر برای امضای دیجیتال به کار گرفته مـی-شود.

۲ ۲ ۱ اهداف امنیتی

باعنایت به اینکه به طور کلی اعمال الگوریتم‌های رمز بار زیادی روی ارتباط و سطح سرویس‌دهی دارد پس باید توجه داشت تنها زمانی استفاده شوند که اهداف امنیتی که دنبال می‌کنیم در مقایسه با سطح کیفی سرویس‌دهی که از بین می‌رود ارزش بیشتری داشته باشد. معمولا اهداف امنیتی که در راستای به کارگیری انواع رمزنگاری مد نظر است به شرح ذیل می‌باشند: [۳]

- محرمانگی[1]: پنهان نگه‌داشتن اطلاعات از همه در حالی که افراد مجاز می‌توانند آن را ببینند.
- صحت اطلاعات[2]: اطمینان از اینکه اطلاعات به وسیله افراد غیر مجاز تغییر نکرده باشد، یعنی طرف دوم بتواند متوجه تغییر اطلاعات ارسالی از طرف اول ارتباط توسط دشمن شود.
- احراز اصالت مبدا داده[3]: وارسی اصالت مبدا اطلاعات، یعنی طرف دوم بتواند وارسی کند که آیا اطلاعات ارسال شده از طرف اول توسط او تولید شده‌اند یا نه.
- احراز اصالت موجودیت‌ها[4]: تایید کردن اصالت طرف مقابل، یعنی طرف دوم باید از اصالت طرف مقابل ارتباط به طور زنده مطمئن شود.
- انکارناپذیری[5]: جلوگیری از انکارکردن تعهد یا انجام عمل قبلی، یعنی وقتی طرف دوم پیام را از طرف اول دریافت می‌کند نه تنها متقاعد می‌شود که این پیام از طرف اول ارسال شده است بلکه می‌تواند طرف سوم مورد قبول دو طرف را نیز از دریافت آن متقاعد کند؛ بنابراین طرف اول نمی‌تواند ارسال پیام را انکار کند.

۲ ۲ ۲ مدل دشمن [۳]

در رابطه با ایجاد مدل واقعی دشمن که دو طرف اول و دوم با آن مواجه هستند، ما فرض می‌کنیم که دشمن دارای توانایی‌های زیادی است. علاوه بر اینکه دشمن می‌تواند اطلاعات روی کانال ارتباطی را بخواند، در ضمن می‌تواند اطلاعات را تغییر داده و همچنین اطلاعات مورد نظر خود را نیز به آن اضافه کند. فرض می‌شود که دشمن به هنگام عمل واکاوی توانایی زیادی به لحاظ محاسباتی دارد. در نهایت فرض می‌شود دشمن از تمام پروتکل‌ها و

[1] Confidentiality
[2] Data integrity
[3] Data origin authentication
[4] Entity authentication
[5] Non-repudiation

مکانیزم‌های رمزنگاری (به استثنای اطلاعات کلیدی) مطلع است. چالش اصلی سیستم رمزنگار این است که با دشمنی، با این توانایی‌ها مقابله کند.

پیش‌زمینه ریاضی

رمزنگاری خم بیضوی بر مبنای دو ساختار جبری بنیان نهاده شده است: گروه متناهی[1] و میدان‌های متناهی[2]. در اینجا یک سری مفاهیم پایه‌ای از نظریه گروه بیان خواهد شد. سپس به بحث راجع به نظریه میدان خواهیم پرداخت و نوع میدان استفاده شده جهت پیاده‌سازی امضای دیجیتال را معرفی خواهیم کرد.

۲ ۳ ۱ گروه‌های متناهی [٤]

اگر G مجموعه‌ای ناتهی و * عملگری دوتایی روی G باشد، آن گاه(G,*) را یک گروه می نامیم اگر شرایط زیر برقرار باشد:

- برای هر $a , b \in G$ ، داشته باشیم $a * b \in G$ (بسته بودن گروه G نسبت به عمل *)
- برای هر $a , b \in G$ ، داشته باشیم، $a * (b * c) = (a * b) * c$ (خاصیت شرکت‌پذیری)
- برای هر $a \in G$ وجود داشته باشد $e \in G$ به قسمی که $a * e = e * a = a$ (وجود عضو همانی)
- برای هر $a \in G$ وجود داشته باشد $b \in G$ به قسمی که $a * b = b * a = e$ (وجود عضو معکوس)

تعریف۱.۲ . مرتبه[3] گروه G با |G| نمایش داده می‌شود که برابر است با تعداد اعضای گروه G

تعریف۲.۲ . مرتبه عضو $g \in G$ را با |g| نمایش می‌دهند و برابر است با کوچکترین عدد صحیح t به قسمی که $g^t = e$ که در اینجا e عضو همانی گروه است.

تعریف ۳.۲ . عضو $g \in G$ را مولد[4] گروه می گویند اگر تمام اعضا گروه را بتوان به فرم g^i که i یک عدد صحیح است تعریف کرد آنگاه $|g| = |G|$

مثال : گروه $G = Z^*_5 = \{1,2,3,4\}$ را تحت عملگر ضرب در نظر بگیرید آنگاه مرتبه گروه G برابر است با:

$$|G| = 4$$

---

[1] Finite group
[2] Finite field
[3] Order
[4] Generator

اکنون عضو $g = 2$ و تمامی توان‌های آن را در نظر می‌گیریم:

$$2^0 \bmod 5 = 1$$

$$2^1 \bmod 5 = 2$$

$$2^2 \bmod 5 = 4$$

$$2^3 \bmod 5 = 3$$

$$2^4 \bmod 5 = 1$$

همچنین می‌توان عضو $g = 4$ و تمامی توان‌های آن را در نظر گرفت

$$4^0 \bmod 5 = 1$$

$$4^1 \bmod 5 = 4$$

$$4^2 \bmod 5 = 1$$

همان گونه که ملاحظه می‌شود مرتبه عضو ۲ که مولد گروه G است (زیرا اعضای گروه G را می‌توان با توان‌هایی از ۲ به دست آورد) برابر مرتبه خود گروه یعنی ۴ است در صورتی که مرتبه عضو ۴ که مولد گروه نیست برابر ۲ است.

۲ ۳ ۲ میدان‌های متناهی [٤]

یک میدان متناهی$(* , + , G)$ متشکل است از مجموعه متناهی G به همراه دو عملگر + و * به قسمی که اعضای مجموعه G اعضای یک گروه تحت دو عملگر دوتایی[1] باشند(بنابراین باید شرایط عمومی گفته شده برای یک گروه را دارا باشد) که این عملگرها معمولا ضرب و جمع نامیده می‌شوند.

تعریف ٤.۲. $(* , + , F)$ را یک میدان گوییم اگر شرایط زیر را دارا باشد

- اعضای F تحت عملگر جمع باید یک گروه آبلی باشند(گروه آبلی به گروهی گفته می‌شود که در آن خاصیت جابجایی وجود دارد).
- اعضای غیر صفر F باید تحت عملگر ضرب و جمع باید یک گروه با خاصیت انجمنی باشند.
- دو عملگر باید نسبت به هم دارای خاصیت توزیع‌پذیری باشند (توزیع‌پذیری ضرب روی جمع)یعنی برای تمام a و b و c های عضو F [۴]

$$a . (b + c) = a.b + a.c \qquad (b + c) . a = b.a + c.a$$

[1] Binary operators

تعریف ۵.۲ . یک میدان F با تعداد محدود اعضا را میدان متناهی F می‌نامند.

تعریف ٦.۲. مرتبه میدان F برابر است با تعداد اعضای میدان F.

تعریف ۷.۲. یک مولد از اعضای غیر صفر یک میدان متناهی مانند F را عضو بنیادین[1] یا مولد F می گویند.

تعریف ۸.۲. مشخصه یک میدان[2] متناهی کمترین مقدار عدد صحیح j است به قسمی که

$$\underbrace{1 + 1 + \ldots + 1}_{j} = 0$$

مثال : میدان متناهی GF(7) که شامل اعداد ۰ تا ۶ می‌باشد را در نظر بگیرید.

مرتبه میدان برابر است با ۷ ، در عین حال مشخصه این میدان متناهی نیز ۷ است زیرا

$$1 + 1 + 1 + 1 + 1 + 1 + 1 = 0 \pmod 7$$

و عضو ۳ مولد میدان متناهی GF(7) می‌باشد.

$$3^0 \bmod 7 = 1$$

$$3^1 \bmod 7 = 3$$

$$3^2 \bmod 7 = 2$$

$$3^3 \bmod 7 = 6$$

$$3^4 \bmod 7 = 4$$

$$3^5 \bmod 7 = 5$$

$$3^6 \bmod 7 = 1$$

تعریف ۹.۲. برای هر توان صحیح از یک عدد اول تنها یک میدان متناهی یکتا[3] وجود دارد که آن را با $GF(p^m)$ نمایش می‌دهند (p عدد اول و m یک عدد صحیح مثبت می‌باشد).

در کاربردهای رمزنگاری، دو نوع از میدان‌های متناهی به وفور مورد استفاده واقع می‌شوند که به شرح زیر می باشند

میدان‌های اول[4] : GF (p) که p یک عدد اول بزرگ است.

میدان‌های دودویی[5] : $GF(2^m)$ که در اینجا m یک عدد صحیح مثبت است.

---

[1] Primitive element

[2] Characteristic of field

۳ - یکتا به این مفهوم که هر میدانی که از توانی از یک عدد اول ساخته شود با میدان‌های دیگر که با همین عدد ساخته می‌شود همریخت است

[4] Prime fields

[5] Binary fields