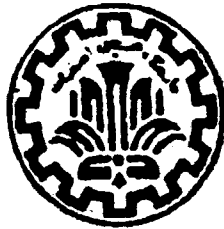


بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

تقديم به همسر و فرزندان عزیزم

۱۷۰۱۴



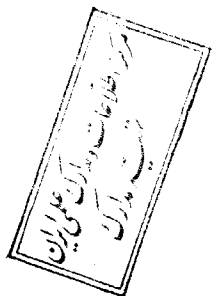
کاربرد نظریه اعداد در رمزنگاری پی در پی

رضا ربیعی

پایان نامه تحصیلی برای اخذ درجه کارشناسی ارشد

در رشته

مهندسی مخابرات



دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

زمستان ۶۸

۱۴۰۱ع

بسمه تعالی

کاربرد نظریه اعداد در رمزنگاری بی درپستی

رضا ربیعی

پایان نامه تحصیلی برای اخذ درجه کارشناسی ارشد

در رشته

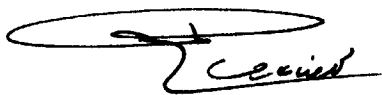
مهندسی مخابرات

دانشگاه صنعتی امپهان

دانشکده برق و کامپیوتر

زمستان ۶۸

کیفیت و ارزش گزارش حاضر بعنوان پایان نامه کارشناسی ارشد مورد تأیید
است .



دکتر محمد رضا عارف (استاد راهنمای پروژه)

کیفیت و ارزش گزارش حاضر بعنوان پایان نامه کارشناسی ارشد مورد تأیید
است .



دکتر علی محمد دوست حسینی

قدر دانسی

" من علمتی حرفا "فقد صیرنی عبدا" "

(امیرالمومنین علی علیه السلام)

بعدا ز ستایش حضرت با رب تعالی که حمد و ستایش مختص ذات اوست و اوست اول معلم انسان

" علم الانسان ما لم يعلم "

از استاد محترم جناب آقای دکتر محمد رضا عارف که در طول انجام پروژه همواره از راهنمایی‌های
بیدریغ و الطافات آمیز ایشان بهره‌مند بودم سپاسگزارم، همچنین از آقای دکتر علی محمد
دوست حسینی ریاست محترم دانشکده که مطالعه و ویرایش این رساله را تقبل نمودند
تشکر می‌کنم و از آقای دکتر حسین علوی که لطف کرده در سمینار اینجانب شرکت نمودند
نیز ممنونم.

فهرست مطالب

صفحه	عنوان
پنج	فهرست مطالب
هشت	فهرست شکل ها
نه	فهرست جدا ول
ده	خلاصه
۱	فصل اول : مقدمه
	فصل دوم : آشنایی با نظریه اعداد بعنوان مبنای ریاضی مورد نیاز در رمزنگاری
۵	پی در پی
۵	مقدمه
۶	۱+۲ همبستگی ها
۹	۲-۲ بررسی خواص اعداد اول و روشهای تولید آنها
۱۰	۱-۲-۲ روش های بررسی قطعی اعداد اول
۱۲	۲-۲-۲ توزیع احتمالی اعداد اول
۱۳	۳-۲ روش بررسی احتمالی اعداد اول
۱۴	۱-۳-۲ تست مونت کارلو
۱۵	۲-۳-۲ تست رابین
۱۷	۴-۲ میدان های گالوا، چندجمله ای های دوره ای، ساده نشدنی و اولیه
۱۷	۱-۴-۲ عملیات در میدان گالوا $GF(p^m)$
۱۷	۲-۴-۲ نمایش اعضای میدان $GF(2^m)$ بصورت توانهای یک عنصر اولیه
۱۸	۳-۴-۲ چندجمله ای های دوره ای
۱۹	۴-۴-۲ چندجمله ای های ساده نشدنی
۱۹	۵-۴-۲ ارتباط چندجمله ای های دوره ای و ساده نشدنی
۱۹	۶-۴-۲ چندجمله ای های ساده نشدنی در میدان گالوا $GF(p)$
۲۰	۷-۴-۲ تعیین چندجمله ای های ساده نشدنی بوسیله غربال آراتستن
۲۰	۸-۴-۲ چندجمله ای های اولیه
۲۱	۵-۲ ریشه ها و عناصر اولیه

۲۱	۱-۵-۲ ریشه‌های اولیه
۲۲	۲-۵-۲ وجود و عدم وجود ریشه‌های اولیه
۲۵	۳-۵-۲ عناصر اولیه
۲۶	۴-۵-۲ تعداد عناصر اولیه
۲۷	فصل سوم: رمزکننده‌های پی در پی
۲۷	۱-۳ مقدمه
۲۸	۲-۳ رمزنگاری پی در پی
۲۹	۳-۳ دنباله‌های تما دفی و شبه تما دفی
۳۰	۱-۳-۳ خواص دنباله‌های تما دفی با یتری
۳۱	۲-۳-۳ مولد دنباله‌های PN
۳۴	۳-۳-۳ تعیین نمای یک تابع دلخواه بر حسب نمای عوامل ساده نشدنی آن
۳۴	۴-۳-۳ حالت $f(x)$ ساده نشدنی
۳۶	۵-۳-۳ چند جمله‌ای‌های مینیمال و توابع اثر
۳۷	۴-۳ پیچیدگی خطی دنباله‌ها
۳۹	۱-۴-۳ رابطه برگشتی پیچیدگی خطی دنباله با تما یزبعدی
۳۹	۲-۴-۳ رابطه برگشتی تعداد دنباله‌های بطول n و پیچیدگی خطی L
۴۱	۳-۴-۳ پیچیدگی خطی دنباله‌های متناوب
	۵-۳ روش بدست آوردن چند جمله‌ای‌های ساده نشدنی با استفاده از خواص
۴۲	دنباله‌های PN
۴۴	۱-۵-۳ کاست‌های دوره‌ای
۴۵	۲-۵-۳ رابطه ضرب کاست‌ها
۴۸	فصل چهارم: ساختارهای غیرخطی
۴۸	۱-۴ شیفت رجستری با فیدبک غیرخطی
	۲-۴ اعمال توابع غیرخطی بر روی دنباله‌های با چند جمله‌ای مینیمال
۵۲	مشترک
	۳-۴ اعمال توابع غیرخطی بر روی دنباله‌های با چند جمله‌ای مینیمال
۵۷	مجزا

۵۹	۴-۴ مصونیت از همبستگی توابع غیرخطی بدون حافظه
۶۵	۴-۵ تاثیر حافظه بر ساختارهای غیرخطی
۷۱	فصل پنجم : معیارهای ارزیابی دنباله‌ها و مولدهای آنها
۷۱	۵-۱ سیستم‌های رمزنگاری ایده‌آل
۷۵	۵-۲ یک ساختار پیشنهادی
۸۰	فصل ششم : نتیجه‌گیری و پیشنهاد
۸۵	ضمیمه : الگوریتمی برای بدست آوردن چند جمله‌ای‌های اولیه درجه ۲
۸۷	مراجع :

فهرست شکل ها

شماره شکل	عنوان	صفحه
۱-۳	بلوک دیاگرام کلی یک سیستم رمزنگساری	۲۸
۲-۳	سیستم رمزنگاری پی در پی با یئری	۲۹
۳-۳	ساختار یک فیدبک شیفت رجیستر	۳۲
۴-۳	ساختار LFSR	۳۲
۵-۳	پیچیدگی خطی برای یک دنباله تولیدشده بوسیله پرتاب سکه و مقایسه آن با یک دنباله PN نظیر	۴۲
۱-۴	بلوک دیاگرام یک NLFSR	۴۹
۲-۴	کوتاه کردن طول حلقه با اضافه کردن یک تابع f برای ترکیب	۵۱
۳-۴	اعمال اپراتور غیرخطی f بر روی دنباله های با چند جمله ای S_{r_1} و S_{r_2} و تبدیل آن به S_k	۵۲
۴-۴	مینیمال مشترک	۶۶
۵-۴	ساختار غیرخطی با N ورودی و با یک بیت حافظه	۶۶
۶-۴	ساختار غیرخطی با حافظه معادل یک فلیپ فلاپ jk	۶۸
۷-۴	یک جمع کننده دوبیتی با بیت انتقالی بعنوان بردار حالت	۷۰
۱-۵	یک ساختار با یک بیت حافظه	۷۶
۲-۵	بلوک دیاگرام ساختار پیشنهادی	۷۸
۳-۵	ساختار پیشنهادی برای $N=2$	۷۸

فهرست جدول

<u>صفحه</u>	<u>عنوان</u>	<u>شماره جدول</u>
۳۹	مقادیر $N_n(L)$ با زاویه $0 \leq L \leq 10$ ، $0 \leq n \leq 10$	۱-۳
۴۵	جدول کاست ها	۲-۳
۴۶	جواب مناسب دستگاره معادلات	۳-۳
۶۰	جدول صحت تابع $S = S_0 + S_0 S_1$	۱-۴

خلاصه

برای ارسال پیام‌های خاصی به گیرنده (های) مورد نظر و محافظت آن از دستبرد دشمن و اطمینان گیرنده از صحت پیام، لازم است که پیام دارای امنیت و اعتبار باشد، برای این منظور قبل از ارسال پیام، آن را رمز می‌کنند.

یکی از روش‌های مختلف رمزنگاری، رمزنگاری پی در پی است که در آن تصادفی بودن دنباله (ویا حداقل داشتن خصوصیات تصادفی) کلید دارای اهمیت است.

آنچه در این رساله مورد بررسی قرار می‌گیرد علاوه بر مطالب ریاضی که در رمزنگاری بکار می‌رود، مسائلی است که در رابطه با تولید دنباله‌های کلیمه‌ساز می‌گردد. بررسی و تولید اعداد اول، روش تعیین چند جمله‌ای‌های اولیه و ساده‌نشده با استفاده از خصوصیات دنباله‌های PN و رابطه یک الگوریتم در این ارتباط، بررسی خصوصیات دنباله‌ها، تصادفی بودن، پیچیدگی خطی و مصونیت از همبستگی آنها مورد بحث قرار گرفته، سیرتکاملی ساختارهایی که خاصیت گفته شده را برآورده می‌کنند بیان و آنها را "ساختارهای غیرخطی" با حافظه می‌رسیم، با توجه به معیارهایی برای ارزیابی دنباله‌ها و ساختارهای بیان و یک ساختار پیشنهادی شده با معیارهای بیان شده مقایسه می‌گردد.

مقدمه .

در سیستم‌های مخابراتی معمولی مثل تلفن، تلگراف، تلکس، رادیو، تلویزیون و... هدف اصلی ارسال اطلاعات از یک منبع (فرستنده) و دریافت و تشخیص صحیح آن بوسیله منبع دیگر (گیرنده) می‌باشد. در این سیستم‌ها، معمولاً اطلاعات (پیام) محرمانه نبوده نیازی به اغتفانظر عموم نیست ولی سیستمهای مخابراتی که اطلاعات سیاسی، نظامی و حتی اقتصادی خاصی را منتقل می‌کنند باید بتوانند این اطلاعات را از دستبردگیرنده‌های اجنبی محافظت نمایند تا پیام‌های امنیتی باشد، همچنین لازماًست سیستم‌دربرابر دخالت اجنبی مقابله با شدت‌گیرنده از صحت پیام مطمئن بوده پیام‌ها را اعتباری باشد. برای نیل به دو منظور بالا این گونه پیام‌ها بصورت رمز شده ارسال می‌گردند.

ایده رمزنگاری از قدیم‌الایامحتی در فرهنگ عامه جوامع نیز وجود داشته‌است، ولی دیرزمانی نیست که بصورت یک علم درآمده، بسرعت پیشرفت نموده و امروزه کاربردهای فراوانی نیز پیدا کرده‌است.

بطور کلی روش‌های مختلف رمزنگاری را می‌توان بدو دسته عمده " رمزنگاری قالبی" و " رمزنگاری پی‌درپی" تقسیم نمود. در هر دو دسته فرستنده و گیرنده پیام هر یک دارای الگوریتم خاصی برای به ترتیب رمز کردن و گشودن رمز پیام هستند که بر مبنای یک دستور

مشترک بنام "کلید" استوار است، کلید عامل انحصاری تما یزگیرنده و فرستنده خودی از اجنبی است. بنا بر این امنیت کلید مترا دفا منیت سیستم و در نتیجه معادل امنیت و اعتبار پیام است. بهمین دلیل دشمن (گیرنده اجنبی) نیز بدنبال دستیابی به آن مویا شد و بدین منظور به اقدامات مختلفی دست مویا زد که اصطلاحاً به حمله موسومند. اگر منظور از حمله دشمن فقط دستیابی با طلاعات ارسالی باشد (شکستن امنیت پیام)، این نوع حمله را حمله پای سیومی گویند و اگر علاوه بر آن بخواد در کمال طلاعات دخالت کند و طلاعات معمول ارسالی نماید (شکستن اعتبار پیام) به حمله اکتیو دست زده است. نوع حملات بر حسب کم و کیف طلاعات دشمن به سه دسته تقسیم می شوند، در حمله نوع اول دشمن بر اساس طلاعاتی که از متن رمز شده بدست آورده عمل می کند، در حمله نوع دوم علاوه بر طلاعات متن رمز شده از قسمتهایی از متن اصلی معادل آنها نیز با اطلاع است. در حمله نوع سوم دشمن از متنهای اصلی و متن رمز شده معادل آنها بهر مقدار که بخواد در اختیار دارد.

در روشهای دسته اول رمزنگاری، پیام را به قالبهای چند سمبلی تقسیم نموده و آنرا قالب به قالب رمز و ارسالی می کنند، در حالی که در روشهای دسته دوم عمل رمزنگاری سمبل به سمبل انجام می شود. در روشهای دسته اخیر کلید بصورت یک دنباله است که با متن پیام (متن اصلی) بصورت سمبل به سمبل ترکیب می شود و به متن رمز شده تبدیل می گردد، در گیرنده نیز عمل رمزگشایی با ترکیب سمبل به سمبل متن رمز شده و کلیدها انجام می شود.

معمولاً دنباله های پیام و کلید بصورت دنباله های با یضری هستند و عمل ترکیب سمبلها بصورت جمع در مبنای ۲ می باشد، بنا بر این برای اینکه دنباله کلید برای دشمن قابل دستیابی نباشد کافی است که این دنباله ای تصادفی باشد و یا شود و یا حداقل برای بلندترین متن، تصادفی نشان داده شود (شبه تصادفی باشد). این دنباله ها که معمولاً بوسیله ماشین های با حالت محدود تولید می شوند، دنباله های متناوب هستند؛ اما چون میخواهیم این دنباله ها دارای خصوصیت تصادفی باشند باید با معیارهایی که خاصیت فوق را ارزیابی می کنند، قابل قبول باشند. از جمله این معیارها شیفتر رجیسترها یا فیدبک خطی (LFSR) هستند که برای تولید دنباله های دوره تناوب حداکثر، لازم است که چند جمله ای مشخص آنها (چند جمله ای که با بطنه فیدبک و طبقات شیفتر رجیستر تعیین می کند) چند جمله ای اولیه باشد، در ارتباط با این مطلب یعنی تعیین چند جمله ای اولیه با مسئله مشابهی بنا م تعیین اعداد اول بزرگ نیز مصادف می شویم، همچنین مسائلی چون چگونگی تولید دنباله های مطلوب و معیارهای ارزیابی آنها مطالبی هستند که در این

رسا له به آنها پردا خته خوا هشد .

فصل دوم این رسا له به را شه مبانی ریاضی موردنیا زو همچنین روش های تولید اعداد اول بزرگ اختصاص دارد . در این فصل ابتدا به بیان مطلب وقضای مربوط به اعداد اول پردا خته و روش قطعی و احتمالی برای تشخیص اول بودن یک عدد بیان میگردند و به مزایای روش احتمالی و همچنین تعیین درصد خطای تصمیم گیری اشاره می شود . سپس میدانهای گالوا ، چند جمله ای های دوره ای ، چند جمله ای های ساده نشدنی و چند جمله ای های اولیه معرفی شده و روابط مربوط به تعدا د چند جمله ای های ساده نشدنی و اولیه از درجه معین و روشی کلاسیک برای تعیین ساده نشدنی بودن چند جمله ای ها بیان میگردند . بخش آخر این فصل به معرفی ریشه ها و عناصر اولیه و ارائه قضایا و مطالب مربوطه پردا خته و صورت کلی اعدادی که دارای ریشه اولیه هستند ، تعدا د عناصر اولیه و ارتباط آنها با چند جمله ای های اولیه بیان می نماید . در دو بخش اول فصل سوم ، رمزکننده های پی در پی معرفی میشوند . دنباله های تصادفی و شبه تصادفی و خصوصیات آنها و مولدهای شیفت رجیستری فیدبک خطی در بخش سوم این فصل بیان میگردند و همچنین شرایط لازم برای تولید دنباله شبه نویز نیز بیان خواهد شد . در بخش بعدی این فصل به خصوصیت دیگری از دنباله های یعنی پیچیدگی خطی آنها پردا خته و پیچیدگی خطی دنباله های شبه تصادفی (متناوب) یا دنباله تصادفی مقایسه میگردند . در آخر این فصل با استفاده از خواص دنباله های شبه نویز و روشی برای بدست آوردن چند جمله ای های اولیه و یل زده نشدنی بیان می شود که در ارتباط با آن الگوریتمی جهت تعیین چند جمله ای های اولیه نیز ارائه می گردد . به منظور ابرای پیچیدگی خطی دنباله های با پیدای روش های غیرخطی استفاده نمود ، این مطلب عنوان فصل چهارم رسا له است که در آن با روش مختلف ، ساختارهای غیرخطی آشنا خواهیم شد . در ابتدا این فصل ساختار شیفت رجیستری فیدبک غیرخطی معرفی و بررسی می شود . در بخش دوم طبقات مختلف یک شیفت رجیستری فیدبک خطی بعنوان متغیرهای یک تابع غیرخطی مورد استفاده قرار می گیرند . در بخش سوم ورودی های تابع غیرخطی از LFSR های مختلف گرفته می شود و در چهارمین بخش این فصل موضوع جدیدی که بخاطر اعمال ساختار غیرخطی مطرح می گردد یعنی "مصونیت از همبستگی" مورد توجه و بررسی قرار خواهد گرفت و خواهیم دید که مجموع کمیت های "مصونیت از همبستگی" و "پیچیدگی خطی" محدود میباشند . در بخش آخری این فصل اثر اضافه نمودن حافظه به ساختارهای غیرخطی و تاثیر آن در شکستن ارتباط "پیچیدگی خطی" و "مصونیت از همبستگی" دنباله های بیان می گردد و بدنبال آن نمونه هایی از ساختارهای

ساده در این زمینه ارائه می‌گردند.

در فصل پنجم معیارهایی برای ارزیابی دنباله‌ها و مولدهای آنها ارائه خواهد شد. برای ارزیابی دنباله‌های PN دو معیار اساسی یعنی تصادفی بودن و پیچیدگی خطی آنها بیان می‌شود و سپس چند معیار نیز برای ارزیابی و مقایسه سیستم‌های رمزنگاری بیان خواهد شد. در بخش دوم این فصل یک ساختار پیشنهادی دوباعی برای بخش اول مورد ارزیابی قرار خواهد گرفت.

و با لاخره در فصل ششم نتیجه‌گیری‌های کلی رساله بیان می‌گردد و در انتها پیشنهاداتی برای ادامه کار ارائه خواهد شد.