بسم الله الرحمن الرحیم

تقدیم به همسر و فرزندان عزیزم

کاربرد نظریه اعداد در رمزنگاری پی در پی

رضا ربیعی

پایان نامهٔ تحصیلی برای اخذ درجه کارشناسی ارشد

در رشته

مهندسی مخابرات

دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

زمستان ۶۸

بسمه‌تعالی

کاربردنظریه اعـــــداد دررزمزنگاری پی درپـــــی

رضا ربیعـــــی

پایان نامه تحصیلی برای اخذدرجه کارشناسی ارشـــــد

دررشتـــــــه

مهندســـــی مخابـــــرات

دانشگاه صنعتـــــی اصفهـــان

دانشکده برق وکامپیـــــوتـــــر

زمستـــــان ۶۸

کیفیت وارزش گزارش حاضربعنوان پایان نامه‌کارشناسی ارشدموردتائید است .

دکترمحمدرضا عارف (استادراهنمای پروژه)

کیفیت وارزش گزارش حاضربعنوان پایان نامه کارشناسی ارشدموردتائید است .

دکترعلیمحمددوست حسینی

قدردانی

" من علمنی حرفا "فقدصیرنی عبدا " "

(امیرالمومنین علی علیه السلام)

بعدازستایش حضرت باریتعالی که حمدوستایش مختص ذات اوست واوست اول معلم انسان

" علم الانسان مالم یعلم "

ازاستادمحترم جناب آقای دکتر محمدرضا عارف که درطول انجام پروژه همواره ازراهنمایی های بیدریغ والطفات آمیزایشان بهره مندبودم سپاسگزارم ،همچنین ازآقای دکتر علیمحمد دوست حسینی ریاست محترم دانشکده که مطالعه و ویرایش این رساله را تقبل نمودند تشکرمی کنم وازآقای دکترحسین علوی که لطف کرده درتسمینار را بنجانب شرکت نمودند نیزممنونم.

فهـــــــرست مطالب

عنوان	صفحه

عنوان	صفحه

فهرست شکـــــــل ها

فهرست جداول

خلاصه

برای ارسال پیام‌های خاصی به‌گیرنده (های) موردنظر 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، آنرا رمز می‌کنند.

یکی از روش‌های مختلف رمزنگاری، رمزنگاری پی درپی است که در آن تصادفی بودن دنباله (و یا 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، مسایلی است که در ارتباط به تولید دنباله‌ٔ کلیه مطرح می‌گردد. بررسی و تولید اعداد اول، روش تعیین چندجمله‌ای‌های اولیه و ساده نشدنی با استفاده از خصوصیات دنباله‌های PN و ارائه یک الگوریتم در این ارتباط، بررسی خصوصیات دنباله‌ها، تصادفی بودن، پیچیدگی خطی و مصونیت از همبستگی آنها مورد بحث قرار گرفته، سپس تکاملی ساختارهایی که خمایص گفته شده را برآورده می‌کنند بیان و نهایتا "به ساختارهای غیرخطی با حافظه می‌رسیم، با لاخره معیارهایی برای ارزیابی دنباله‌ها و ساختارها بیان و یک ساختار پیشنهاد شده با معیارهای بیان شده مقایسه می‌گردد.

فصل اول

مقدمه .

درسیستم‌های مخابراتی معمولی مثل تلفن ،تلگراف ،تلکس ،رادیو ،تلویزیون و . . . هدف اصلی ارسال اطلاعات از یک منبع (فرستنده) ودریافت وتشخیص صحیح آن بوسیله منبع دیگر (گیرنده)میباشد . دراین سیستم‌ها ،معمولا" اطلاعات (پیام) محرمانه نبوده نیازی به اختفا ازنظرعمومنیست ولی سیستمهای مخابراتی که اطلاعات سیاسی ،نظامی وحتی اقتصادی خاصی را منتقل میکنندباید بتوانند این اطلاعات را از دستبردگیرنده‌های اجنبی محافظت نمایندتا پیام دارای امنیت باشد ،همچنین لازم است سیستم دربرابر دخالت اجنبی مقاوم باشدتا گیرنده از صحت پیام مطمئن بوده پیام دارای اعتبار باشد .برای نیل به‌دومنظوربالااین گونه‌پیام‌ها بصورت رمزشده ارسال میگردند .

ایده‌ٔ رمزنگاری ازقدیم الایام حتّی درفرهنگ عامه‌ٔ جوامع نیزوجودداشته است ،ولی دیرزمانی نیست که‌بصورت یک علم‌درآمده ،بسرعت پیشرفت نموده‌وا موزه‌کاربردهای فراوانی نیزپیدا کرده‌است .

بطورکلی روش‌های مختلف‌رمزنگاری را می‌توان بدودسته‌ٔ عمده " رمزنگاری قالبی" و "رمزنگاری پی درپی " تقسیم‌نمود . درهردودسته‌فرستنده‌وگیرنده‌ٔ پیام‌هریک دارای ـ الگوریتم‌خاصی برای به‌ترتیب رمزکردن وگشودن رمزپیام‌هستندکه‌برمبنای یک دستور

مشترک بنا م "کلید" ا ستوا را ست ،کلیدعا مل ا نحصا ری تما یزگیرنده وفرستنده خودی ا ز ا جنبی ا ست .بنا برا ین ا منیت کلیدمترا دف ا منیت سیستم ودرنتیجه معا د ل ا منیت وا عتبار پیا م ا ست . بهمین دلیل دشمن (گیرنده ا جنبی)نیزبدنبا ل دستیا بی به آن مویا شد وبدین منظوربه ا قدا ما ت مختلفی دست مویا زدکه ا صطلاحا "به حمله موسومند .ا گرمنظور ا زحمله دشمن فقط دستیا بی با طلاعات ا رسا لی با شد (شکستن ا منیت پیا م) ،ا ین نوع حمله را حمله پا سیو می گویندوا گرعلاوه برآن بخوا هددرکا نا ل ا طلاعات دخا لت کندوا طلاعات مجعول ا رسا ل نما ید (شکستن ا عتبا رپیا م)به حمله ا کتیودست زده ا ست. نوع حملات برحسب کم وکیف ا طلاعات دشمن به سه دسته تقسیم میشوند ،درحمله نوع ا ول دشمن برلسا س ا طلاعا تی که ا زمتون رمزشده بدست آورده عمل میکند ،درحمله نوع دوم علاوه برا طلاعات متن رمزشده ا زقسمتها یی ا زمتن ا صلی معا د ل آنها نیزبا اطلاع ا ست . درحمله نوع سوم دشمن ا زمتن های ا صلی ومتن رمزشده معا د ل آنها بهرمقدا رکه بخوا هددراختیا ردا رد .

درروش های دسته ا ول رمزنگا ری،پیا م را به قا لب های چندسمبلی تقسیم نموده وآنرا قا لب یعقا لب رمزوا رسا ل میکنند ،درحا لیکه درروش های دسته دوم عمل رمزنگا ری سمبل به سمبل ا نجا م میشود . درروش های دسته ا خیرکلیدبصورت یک دنبا له ا ست که با متن پیا م (متن ا صلی)بصورت سمبل به سمبل ترکیب میشودوبه متن رمزشده تبدیل میگردد ،در - گیرنده نیزعمل رمزگشا یی با ترکیب سمبل به سمبل متن رمزشده وکلیه ا نجا م میشود .

معمولا "دنبا له های پیا م وکلیدبصورت دنبا له های با ینری هستندوعمل ترکیب سمبل - ها بصورت جمع درمبنا ی ۲ میبا شد .بنا برا ین برا ی اینکه دنبا له کلیدبرا ی دشمن قا بل دستیا بی نبا شدکا فی استکه ا ین دنبا له ،دنبا له ا ی تصا دفی با شدویا حدا قل برا ی بلندترین متون ،تصا دفی نشا ن دا ده شود (شبه تصا دفی با شد) . ا ین دنبا له ها که معمولا" بوسیله ما شین های با حا لت محدودتولیدمیشوند ،دنبا له های متنا وب هستند ؛ ا ما چون میخوا هیم ا ین دنبا له ها دا را ی خصوصیت تصا دفی با شندبا یدبا معیا رها یی که خصا یص فوق را ا رزیا بی میکنند ،قا بل قبول با شند . ا زجمله ا ین ما شینها شیفت رجیسترها با فیدبک خطی(LFSR)هستندکه برا ی تولیددنبا له ها یبا دوره تنا وب حدا کثر ،لازم ا ست که چند جمله ا ی مشخصه آنها "(چندجمله ا ی که وا بطه فیدبک وطبقا ت شیفت رجیستررا تعیین میکند) چندجمله ا ی ا ولیه با شد ،درا رتبا ط با ا ین مطلب یعنی تعیین چندجمله ا یها ی ا ولیه با مسئله مشابهی بنا م تعیین ا عدادا ول بزرگ نیزمصا دف میشویم ،همچنین مسا یلی چون چگونگی تولیددنبا له های مطلوب ومعیا رها ی ا رزیا بی آنها مطا لبی هستندکه درا ین

رسا له به آنها پردا خته خوا هدشد .

فصل دوم این رسا له به ارا ئه مبا نی ریا ضی موردنیا زوهمچنین روش های تولید اعدا د اول بزرگ ا ختصا ص دا رد . درا ین فصل ا بتدا به بیا ن مطالب وقضا یا ی مربوط به اعدا د اول پردا خته وروش قطعی وا حتما لی برا ی تشخیص اول بودن یک عدد بیا ن میگردند وبه مزا یا ی روش ا حتما لی وهمچنین تعیین درصدخطا ی تصمیم گیری ا شا ره میشود . سپس میدا نها ی گا لوا ،چندجمله ا ی ها ی دوره ا ی ،چندجمله ا ی ها ی سا ده نشدنی وچندجمله ا ی ها ی اولیه ا ولیه معرفی شده وروا بط مربوط به تعدا د چندجمله ا ی ها ی سا ده نشدنی وا ولیه ا زدرجه معین وروشی کلاسیک برا ی تعیین سا ده نشدنی بودن چندجمله ا ی ها بیا ن میگردند .بخش آخرا ین فصل به معرفی ریشه ها وعنا صرا ولیه وا ئه قضا یا ومطا لب مربوطه پردا خته وصورت کلی ا عدا دی که دا را ی ریشه ا ولیه هستند ،تعدا د عنا صرا ولیه وا رتبا ط آنها با چندجمله ا ی ها ی ا ولیه بیا ن مینما ید . دردوبخش ا ول فصل سوم ،رمزکننده های پی درپی معرفی میشوند . دنبا له های تصا دفی وشبه تصا دفی وخصوصیا ت آنها ومولدها ی شیفت رجیستربا فیدبک خطی دربخش سوم این فصل بیا ن میگردندوهمچنین شرا یط لازم برا ی تولیددنبا له شبه نویزنیزبیا ن خوا هدشد .دربخش بعدی ا ین فصل به خصوصیت دیگری ا زدنبا له ها یعنی پیچیدگی خطی آنها پردا خته وپیچیدگی خطی دنبا له های شبه تصا دفی (متنا وب)با دنبا له تصا دفی مقا یسه میگردند .درآخرا ین فصل با ا ستفا ده ا زخوا ص دنبا له های شبه نویزروشی برا ی بدست آوردن چندجمله ا ی ها ی ا ولیه ویا زده نشدنی بیا ن میشودکه درا رتبا ط با آن ا لگوریتمی جهت تعیین چندجمله ا ی ها ی ا ولیه نیزا را ئه میگردد .به منظوربا لابردن پیچیدگی خطی دنبا له ها با یدا ز روش های غیرخطی ا ستفا ده نمود ،ا ین مطلب عنوا ن فصل چها رم رسا له ا ست که درآن با شه روش مختلف ،سا ختا رها ی غیرخطی آشنا خوا هیم شد .درا بتدا ی ا ین فصل سا ختا رشیفت رجیستربا فیدبک غیرخطی معرفی وبررسی میشود . دربخش دوم طبقا ت مختلف یک شیفت رجیستربا فیدبک خطی بعنوا ن متغیرها ی یک تا بع غیرخطی موردا ستفا ده قرا رمیگیرند . دربخش سوم ورودی ها ی تا بع غیرخطی ا ز LFSR ها ی مختلف گرفته میشود ودرچها رمین بخش ا ین فصل موضوع جدیدی که بخا طرا عما ل سا ختا رغیرخطی مطرح میگرددیعنی "مصونیت ا زهمبستگی" موردتوجه وبررسی قرا رخوا هدگرفت وخوا هیم دیدکه مجموع کمیت های "مصونیت ا زهمبستگی" و "پیچیدگی خطی" محدودمیبا شند . دربخش آخری ا ین فصل ا ثر ا ضا فه نمودن حا فظه به سا ختا رها ی غیرخطی وتا ثیرآن درشکستن ا رتبا ط "پیچیدگی خطی" و "مصونیت ا زهمبستگی " دنبا له ها بیا ن میگرددوبدنبا ل آن نمونه هایی ا زسا ختا رها ی

ساده‌در این زمینه‌ها را شه‌موگردند .

درفصل پنجم‌معیارهایی برای ارزیابی دنباله‌ها ومولدهای آنها را شه‌خواهدشد .برای ارزیابی دنباله‌های PN دومعیار اساسی یعنی تصادفی بودن وپیچیدگی خطی آنها بیان می‌شودوسپس چندمعیار نیزبرای ارزیابی ومقایسه سیستم‌های رمزنگاری بیان خواهد شد . دربخش دوم این فصل یک ساختار پیشنهادوبا معیارهای بخش اول موردارزیابی قرار خواهدگرفت .

وبالاخره‌درفصل ششم‌نتیجه‌گیری های کلی رسالـه‌بیان موگرددودرانتها پیشنهادا تی برای ادامه‌کار را شه‌خواهدشد .