دنباله های فیبوناتچی و لوکاس تعمیم یافته ی دو پارامتری و کاربرد آنها در سیستم های رمزنگاری نامتقارن

شاهد مشهودی[۱] و مهسا صادقی [۲]
[۱] گروه ریاضی، دانشکده علوم پایه، دانشگاه آزاد اسلامی واحد رشت، ایران. Shahed.Mashhoodi@Gmail.com
[۲] دانشکده علوم ریاضی و کامپیوتر، دانشگاه خوارزمی، تهران، ایران. Mahsa.Sadeghi89@Gmail.com

چکیده - حفاظت اطلاعات و امنیت ارتباطات از جنبه های نظامی، سیاسی، اقتصادی و ...، در طول تاریخ همواره از اهمیت خاصی برخوردار بوده است. در دهه‌های اخیر، با توسعه فناوری اطلاعات و گسترش شبکه‌های ارتباطی در فضای مجازی اینترنت، نیاز به طراحی سیستم‌های امنیتی پیشرفته‌تر نیز بیشتر شد. در اکثر این سیستم‌ها عموما از الگوریتم‌هایی با پیچیدگی کافی و مبتنی بر ریاضیات پیشرفته، برای به رمز در آوردن اطلاعات پیام‌ها استفاده می‌شود. در مقاله‌ی حاضر ابتدا به بررسی یکی از مباحث مشترک بین ریاضیات گسسته، جبر و نظریه اعداد تحت عنوان دنباله‌های اعداد فیبوناتچی و لوکاس می‌پردازیم و سپس آنها را به وسیله‌ی دو پارامتر، به فرم کلی یک رابطه بازگشتی خطی مرتبه دوم، تعمیم می‌دهیم و به بررسی اتحادهای تعمیم یافته‌ی حاکم بر این دنباله‌های تابعی می‌پردازیم، تا نهایتا با استفاده از ویژگی‌های جبری مناسب‌شان، از آنها در سیستم‌های رمزنگاری نامتقارن استفاده کنیم.

کلید واژه- امنیت اطلاعات و ارتباطات، سیستم‌های رمزنگاری نامتقارن، دنباله‌های فیبوناتچی و لوکاس تعمیم یافته‌ی دو پارامتری.

۱- مقدمه و پیشینه تاریخی

استفاده از رمزنگاری برای تبادل اطلاعات به زمان ژولیوس سزار باز می‌گردد. او از بیم لو رفتن پیام‌های محرمانه ای که بین دولت روم و ممالک مستعمره اش خصوصا بیزانس، رد و بدل می‌شد، تصمیم گرفت متن پیام‌های خود را قبل تحویل به پیام رسان، به متنی نامفهوم تبدیل نماید که فقط گیرنده ی اصلی پیام بتواند از مفهوم پیام اطلاع یابد. بر این اساس معمولا همه ی حروف کلمات پیام‌های خود را، طبق ترتیب الفبا، یک یا چند حرف به جلو یا عقب، جابجا می‌کرد، به عنوان مثال برای استفاده از سیستم رمزنگاری سزار، اگر با گیرنده پیام قرار بگذاریم که همه ی حروف پیام باید سه رتبه طبق الفبا به عقب شیفت داده شوند تا پیام مفهوم گردد (که این قرارداد را کلید رمزگشایی از قفل پیام نامفهموم ارسال شده می‌نامند)، آنگاه در پیام خود مثلا باید از واژه ی نامفهوم «هسش» به جای کلمه ی «مرز» استفاده نماییم. البته با توجه به محدود بودن تعداد حروف الفبا، واضح است که شکستن این رمز چندان پیچیده نیست.

تا قرن‌ها بعد امنیت سیستم‌های رمزنگاری در همین حد باقی ماند تا اینکه با آغاز جنگ جهانی دوم، ارتش آلمان دستگاه های رمزنگاری جدیدی اختراع کرد که شبیه به یک ماشین حروفچینی بودند. همین امر موجب شد تا سازمان امنیت ارتش انگلستان برای شکستن رمز پیام‌های نامفهوم مخابرات بی سیم آلمان ها، پروژه تحقیقاتی بزرگی را به سرپرستی آلن تورینگ آغاز کند که علاوه بر موفقیت در رمزگشایی از پیام‌های محرمانه نظامی و کمک به متفقین برای پیروزی در جنگ، نهایتا منجر به کشف اصول بنیادی جدیدی برای طراحی و ساخت رایانه های جدیدی گردید. یکی از نخستین گام‌ها در طراحی الگوریتم های نوین رمزنگاری برای تامین امنیت اطلاعات در قرن اخیر در دهه هشتاد میلادی توسط سه نفر به نام‌های رایوست، شمیر و آدلمن انجام گرفت که نسخه های ارتقا یافته ی پروتکل آن هنوز هم در رایانه های امروز مورد استفاده قرار می‌گیرند [۱]. در مقاله حاضر قصد داریم پس از معرفی مفاهیم اولیه رمزنگاری، به تبیین ساختار یک دستگاه رمز مبتنی بر خواص دنباله اعداد لوکاس بپردازیم.

۲- تعاریف و پیش نیازها

در این بخش اصطلاحات و مفاهیم اولیه معرفی می‌شوند.

۲-۱- رمزنگاری

علم مطالعه ی روش های مختلف سری نویسی و مبادله ی امن اطلاعات طبقه بندی شده را رمزنگاری می‌گویند.