هفتمین کنفرانس بین المللی انجمن رمز ایران
۲۴ و ۲۵ شهریورماه ۱۳۸۹، دانشگاه صنعتی خواجه نصیرالدین طوسی
انجمن رمزایران
دانشگاه صنعتی خواجه نصیرالدین طوسی

تعمیمی بر رمزنگاری طلایی به کمک حاصلضرب هادامارد ماتریس‌های k- فیبوناتچی

سید مقتدی هاشمی‌پرست[۱]، مهدی خمسه[۲]، شاهد مشهودی[۳]

گروه ریاضی دانشکده علوم دانشگاه صنعتی خواجه نصیرالدین طوسی[۱]
hashemiparast@kntu.ac.ir

دانشگاه پیام نور قزوین[۲] عضو باشگاه پژوهشگران جوان و دانشجوی کارشناسی ارشد دانشگاه آزاد اسلامی واحد کرج[۳]
khamseh.mahdi@gmail.com , mashhoodi.m@srbiau.ac.ir

چکیده

در سال‌های اخیر رمزنگاری‌طلایی به عنوان روش جدیدی در سیستم‌های رمزنگاری مورد توجه قرار گرفته است. علی رغم مزایای این شیوه به تدریج بعضی نقاط آسیب‌پذیر نیز در آن کشف گردید. در نتیجه پژوهشگران سیستم‌های رمزنگاری تلاش‌هایی را در جهت رفع این معایب آغاز کرده‌اند، که منجر به پیشرفت‌هایی در الگوریتم رمزنگاری طلایی شده است. در این مقاله سعی خواهد شد بستری جدید برای اصلاح الگوریتم اولیه با استفاده از تعمیم ریاضی دنباله فیبوناتچی ارائه گردد. در این راستا ابتدا دنباله k- فیبوناتچی را معرفی و سپس ماتریس‌های طلایی را به کمک آن خواهیم ساخت. در پایان به وسیله حاصلضرب هادامارد این ماتریس‌ها، روش رمزنگاری طلایی k- فیبوناتچی را عرضه خواهیم کرد.

واژه‌های کلیدی

دنباله فیبوناتچی، دنباله k- فیبوناتچی، ماتریس‌های طلایی، رمزنگاری‌طلایی، حاصلضرب هادامارد.

۱- مقدمه

با پیشرفت تکنولوژی و استفاده از روش‌های ارتباطی نوین مانند اینترنت، سیستم‌های مخابراتی بیسیم و موارد مشابه، نیاز به استفاده از روش‌های امن به منظور انتقال مناسب اطلاعات مورد توجه کاربران سیستم بوده است. در عصر حاضر دانشمندان همواره به دنبال ابداع روش‌هایی هستند که اطمینان بیشتری را در حفظ اطلاعات ایجاد کنند. یک راه حل عمومی برای این مشکل استفاده از روش‌های رمزنگاری است. یکی از این روش‌ها رمزنگاری‌طلائی می‌باشد که در سال ۲۰۰۶ توسط Stakhov ارائه گردید. در این روش به کمک دنباله فیبوناتچی و ماتریس‌های طلایی، الگوریتمی برای رمز کردن متن اولیه ارائه شده است. در طی چند سال گذشته دانشمندان زیادی سعی در ارتقا روش رمزنگاری طلایی داشته‌اند. به طور مثال در [Nalli 2007] سعی شده تا با تغییر ماتریس‌های رمزنگار و رمزگشا معایب برطرف و امنیت ارتقا یابد و یا در [Hashemiparast 2010] با تعمیم Q- ماتریس و ماتریس‌های طلایی به بیش از یک پارامتر ارتقای مناسبی در امنیت ایجاد شده است.

در مقاله حاضر قصد داریم تعمیمی جدید از حاصلضرب هادامارد ماتریس‌های فیبوناتچی به کمک دنباله k- فیبوناتچی معرفی کنیم. سپس از این ماتریس‌ها برای تعمیم الگوریتم رمزنگاری‌طلایی بهره خواهیم برد به گونه‌ای که رمزگشایی بدون در اختیار داشتن کلید بسیار مشکل خواهد شد.

۲-پیشنیازها!

۲-۱-ماتریس‌های فیبوناتچی !

از تعمیم رابطه بازگشتی فیبوناتچی

$$F_{n+1}=F_n+F_{n-1}\quad,\quad n=1,2,3,\ldots \qquad (1)$$

می‌توان به ازای هر عدد صحیح n ماتریس‌های فیبوناتچی را به صورت

$$Q=\begin{pmatrix}1&1\\1&0\end{pmatrix}\ ,\ Q^n=\begin{pmatrix}F_{n+1}&F_n\\F_n&F_{n-1}\end{pmatrix} \qquad (2)$$

تعریف نمود. [El Naschie 1999] , [Stakhov 2007]

همچنین در [Stakhov 2007] توابع سینوس و کسینوس هذلولوی متقارن فیبوناتچی به صورت

$$sFh(x)=\frac{\tau^x-\tau^{-x}}{\sqrt{5}} \qquad (3)$$

$$cFh(x)=\frac{\tau^x+\tau^{-x}}{\sqrt{5}} \qquad (4)$$

تعریف می‌شوند که در آنها $\tau=\frac{1+\sqrt{5}}{2}$ (نسبت طلایی) می‌باشد.

سپس به کمک توابع هذلولوی متقارن فیبوناتچی و ماتریس‌های فیبوناتچی نوع جدیدی از ماتریس‌ها به نام ماتریس‌های طلایی معرفی می‌شوند:

$$Q^{2x}=\begin{pmatrix}cFh(2x+1)&sFh(2x)\\sFh(2x)&cFh(2x-1)\end{pmatrix} \qquad (5)$$

$$Q^{2x+1}=\begin{pmatrix}sFh(2x+2)&cFh(2x+1)\\cFh(2x+1)&sFh(2x)\end{pmatrix} \qquad (6)$$

این ماتریس‌ها دارای ویژگی‌های خاصی نیز می‌باشند و از جمله مهمترین آنها می‌توان به فرمول‌های زیر موسوم به Cassini اشاره نمود، که با دترمینان‌گیری از این ماتریس‌ها حاصل می‌گردند:

$$\det Q^{2x}=cFh(2x+1)cFh(2x-1)-\left[sFh(2x)\right]^2=1 \qquad (7)$$

$$\det Q^{2x+1}=sFh(2x+2)sFh(2x)-\left[cFh(2x+1)\right]^2=-1 \qquad (8)$$

همچنین وارون ماتریس‌های (۵) و (۶) به صورت

$$Q^{-2x}=\begin{pmatrix}cFh(2x-1)&-sFh(2x)\\-sFh(2x)&cFh(2x+1)\end{pmatrix} \qquad (9)$$

$$Q^{-(2x+1)}=\begin{pmatrix}-sFh(2x)&cFh(2x+1)\\cFh(2x+1)&-sFh(2x+2)\end{pmatrix} \qquad (10)$$

تعریف می‌شوند.

۲-۲-حاصلضرب هادامارد ماتریس‌های طلایی فیبوناتچی (HP.FM)

تعریف ۱. اگر $A=[a_{ij}]$ و $B=[b_{ij}]$ دو ماتریس دلخواه و هم‌اندازه $(n\times n)$ باشند، آنگاه

$$A\circ B=(a_{ij}b_{ij}) \qquad (11)$$

را حاصلضرب هادامارد یا ضرب شور دو ماتریس هم‌اندازه‌ی A و B می‌نامند [Zhang, 1999] .

تعریف ۲. ماتریس $Q^n\circ Q^{-n}$ را HP.FM یا ماتریس حاصلضرب هادامارد ماتریس‌های فیبوناتچی Q^n و Q^{-n} می‌نامند. این ماتریس دارای دامنه‌ی حقیقی می‌باشد.

زمانی که این ماتریس‌ها تابعی از متغیر حقیقی x باشند می‌توان حاصلضرب هادامارد ماتریس‌های طلایی (۵) با (۹) ، و (۶) با (۱۰) را به صورت زیر نمایش داد:

$$Q^{2x}\circ Q^{-2x}=\begin{pmatrix}cFh(2x+1)cFh(2x-1)&-\left[sFh(2x)\right]^2\\-\left[sFh(2x)\right]^2&cFh(2x+1)cFh(2x-1)\end{pmatrix} \qquad (12)$$

$$Q^{2x+1}\circ Q^{-(2x+1)}=\begin{pmatrix}-sFh(2x+2)sFh(2x)&\left[cFh(2x+1)\right]^2\\\left[cFh(2x+1)\right]^2&-sFh(2x+2)sFh(2x)\end{pmatrix} \qquad (13)$$

با توجه به فرمول Cassini می‌توان ماتریس‌های (۱۲) و (۱۳) را به صورت

$$Q^{2x}\circ Q^{-2x}=\begin{pmatrix}1+\left[sFh(2x)\right]^2&-\left[sFh(2x)\right]^2\\-\left[sFh(2x)\right]^2&1+\left[sFh(2x)\right]^2\end{pmatrix} \qquad (14)$$

$$Q^{2x+1}\circ Q^{-(2x+1)}=\begin{pmatrix}1-\left[cFh(2x+1)\right]^2&\left[cFh(2x+1)\right]^2\\\left[cFh(2x+1)\right]^2&1-\left[cFh(2x+1)\right]^2\end{pmatrix} \qquad (15)$$

نمایش داد.

قضیه ۳. دترمینان ماتریس‌های (۱۴) و (۱۵) به صورت زیر است

$$\det\left(Q^{2x}\circ Q^{-2x}\right)=1+2\left[sFh(2x)\right]^2 \qquad (16)$$

$$\det\left(Q^{2x+1}\circ Q^{-(2x+1)}\right)=1-2\left[cFh(2x+1)\right]^2 \qquad (17)$$

برهان: با توجه به فرمول Cassini برای رابطه‌ی (۱۶) خواهیم داشت

$$\det\left(Q^{2x}\circ Q^{-2x}\right)=\left(cFh(2x+1)cFh(2x-1)\right)^2-\left(sFh(2x)\right)^4$$
$$=\left(cFh(2x+1)cFh(2x-1)+\left[sFh(2x)\right]^2\right)\times 1$$
$$=1+2\left[sFh(2x)\right]^2$$

و به طریق مشابه رابطه (۱۷) نیز ثابت می‌گردد.

قضیه ۴. وارون ماتریس‌های HP.FM به صورت زیر است

$$\left(Q^{2x}\circ Q^{-2x}\right)^{-1}=$$
$$\begin{pmatrix}\frac{1+\left[sFh(2x)\right]^2}{1+2\left[sFh(2x)\right]^2} & \frac{\left[sFh(2x)\right]^2}{1+2\left[sFh(2x)\right]^2}\\ \frac{\left[sFh(2x)\right]^2}{1+2\left[sFh(2x)\right]^2} & \frac{1+\left[sFh(2x)\right]^2}{1+2\left[sFh(2x)\right]^2}\end{pmatrix} \quad (18)$$

$$\left(Q^{2x+1}\circ Q^{-(2x+1)}\right)^{-1}=$$
$$\begin{pmatrix}\frac{1-\left[cFh(2x+1)\right]^2}{1-2\left[cFh(2x+1)\right]^2} & \frac{-\left[cFh(2x+1)\right]^2}{1-2\left[cFh(2x+1)\right]^2}\\ \frac{-\left[cFh(2x+1)\right]^2}{1-2\left[cFh(2x+1)\right]^2} & \frac{1-\left[cFh(2x+1)\right]^2}{1-2\left[cFh(2x+1)\right]^2}\end{pmatrix} \quad (19)$$

۳-دنباله k- فیبوناتچی!

تعریف۵. برای هر عدد صحیح $k\geq 1$ تابع بازگشتی تعریف شده بوسیله

$$F_{k,0}=0, F_{k,1}=1, F_{k,n+1}=kF_{k,n}+F_{k,n-1}\ ,n\geq 1 \quad (20)$$

را با $\{F_{k,n}\}_{n\in N}$ نمایش داده و k- امین دنباله فیبوناتچی از اعداد k- فیبوناتچی می‌نامند. [Falcon and Plaza 2009]

باید توجه داشت که اگر در تعریف (۵) مقدار حقیقی x را جایگزین عدد صحیح k نماییم آنگاه خواهیم داشت:

$$F_{n+1}=\begin{cases}1 & if\ \ n=0\\ x & if\ \ n=1\\ xF_n(x)+F_{n-1}(x) & if\ \ n>1\end{cases} \quad (21)$$

۳-۱-توابع هذلولوی k- فیبوناتچی !

به طور مشابه با آنچه در مورد توابع هذلولوی متقارن فیبوناتچی ذکر گردید و با توجه به [Falcon and Plaza 2009] می‌توان توابع هذلولوی k- فیبوناتچی را به صورت زیر معرفی نمود.

سینوس هذلولوی متقارن k- فیبوناتچی:

$$sF_k\,h(x)=\frac{\sigma^x-\sigma^{-x}}{\sigma+\sigma^{-1}} \quad (22)$$

کسینوس هذلولوی متقارن k- فیبوناتچی:

$$cF_k\,h(x)=\frac{\sigma^x+\sigma^{-x}}{\sigma+\sigma^{-1}} \quad (23)$$

که در آنها

$$\sigma=\frac{k+\sqrt{k^2+4}}{k} \quad (24)$$

بنابر این به سادگی از طریق محاسبه خواهیم داشت

$$F_{k,n}=\begin{cases}sF_k\,h(m) & for\ \ m=2n\\ cF_k\,h(m) & for\ \ m=2n+1\end{cases} \quad (25)$$

که در آن

$$F_{k,n}=\frac{\sigma^x-\left(-\sigma^{-x}\right)}{\sigma+\sigma^{-1}} \quad (26)$$

. [Falcon and Plaza 2009]

۳-۲-ماتریس k- فیبوناتچی !

تعریف ۶. ماتریس ۲×۲ به صورت

$$Q^{k,1}=\begin{pmatrix}k & 1\\ 1 & 0\end{pmatrix} \quad (27)$$

را Q- ماتریس k- فیبوناتچی می‌نامند. [Johnson 2007]

همچنین n- امین توان Q- ماتریس k- فیبوناتچی برای هر عدد صحیح $k\geq 1$ و $n=0,\pm1,\pm2,\pm3,...$ به فرم

$$Q^{k,n}=\begin{pmatrix}F_{k,n+1} & F_{k,n}\\ F_{k,n} & F_{k,n-1}\end{pmatrix} \quad (28)$$

می‌باشد.

تذکر: مشابه فرمول Cassini داریم:

$$F_{k,n-1}.F_{k,n+1}-\left(F_{k,n}\right)^2=(-1)^n \quad (29)$$

که (۲۹) را از این پس فرمول Cassini تعمیم یافته می‌نامیم، بنابراین خواهیم داشت:

$$\det Q^{k,n}=(-1)^n \quad (30)$$

۳-۳-ماتریس‌های k- فیبوناتچی طلایی !

طبق [Er 1984] داریم

$$Q^{k,n}=\begin{pmatrix}kF_{k,n}+F_{k,n-1} & kF_{k,n-1}+F_{k,n-2}\\ kF_{k,n-1}+F_{k,n-2} & kF_{k,n-2}+F_{k,n-3}\end{pmatrix}$$
$$=k\begin{pmatrix}F_{k,n} & F_{k,n-1}\\ F_{k,n-1} & F_{k,n-2}\end{pmatrix}+\begin{pmatrix}F_{k,n-1} & F_{k,n-2}\\ F_{k,n-2} & F_{k,n-3}\end{pmatrix}$$
$$=kQ^{k,n-1}+Q^{k,n-2} \quad (31)$$

بنابراین برای هر عدد صحیح $k\geq 1$ داریم

$$Q^{k,n} = kQ^{k,n-1} + Q^{k,n-2}\ , \qquad (۳۲)$$

و همچنین با توجه به خواص ماتریس‌ها داریم

$$Q^{k,n}.Q^{k,m} = Q^{k,m}.Q^{k,n} = Q^{k,n+m}\ , \qquad (۳۳)$$

اکنون با توجه به زوج یا فرد بودن مقدار n خواهیم داشت

$$n = ۲t \qquad Q^{k,۲t} = \begin{pmatrix} F_{k,۲t+۱} & F_{k,۲t} \\ F_{k,۲t} & F_{k,۲t-۱} \end{pmatrix} \qquad (۳۴)$$

$$n = ۲t+۱ \quad Q^{k,۲t+۱} = \begin{pmatrix} F_{k,۲t+۲} & F_{k,۲t+۱} \\ F_{k,۲t+۱} & F_{k,۲t} \end{pmatrix} \qquad (۳۵)$$

که در اینجا t یک عدد صحیح می‌باشد.

حال مشابه با آنچه در [Stakhov 2007] آمده، با جای‌گذاری توابع هذلولوی k- فیبوناتچی متقارن در روابط (۳۴) و (۳۵) خواهیم داشت

$$Q^{k,۲t} = \begin{pmatrix} cF_k h(۲t+۱) & sF_k h(۲t) \\ sF_k h(۲t) & cF_k h(۲t-۱) \end{pmatrix} \qquad (۳۶)$$

$$Q^{k,۲t+۱} = \begin{pmatrix} sF_k h(۲t+۲) & cF_k h(۲t+۱) \\ cF_k h(۲t+۱) & sF_k h(۲t) \end{pmatrix} \qquad (۳۷)$$

که در آن t یک متغیر صحیح می‌باشد. با جای‌گذاری متغیر حقیقی x به جای t در روابط (۳۶) و (۳۷) خواهیم داشت:

$$Q^{k,۲x} = \begin{pmatrix} cF_k h(۲x+۱) & sF_k h(۲x) \\ sF_k h(۲x) & cF_k h(۲x-۱) \end{pmatrix} \qquad (۳۸)$$

$$Q^{k,۲x+۱} = \begin{pmatrix} sF_k h(۲x+۲) & cF_k h(۲x+۱) \\ cF_k h(۲x+۱) & sF_k h(۲x) \end{pmatrix} \qquad (۳۹)$$

همچنین با توجه به فرمول Cassini تعمیم یافته (۲۹) و دترمینان‌گیری از ماتریس‌های (۳۸) و (۳۹) می‌توان ثابت نمود

$$cF_k h(۲x+۱)cF_k h(۲x-۱) - [sF_k h(۲x)]^۲ = ۱$$

$$sF_k h(۲x+۲)sF_k h(۲x) - [cF_k h(۲x+۱)]^۲ = -۱$$

بنابراین داریم

$$\det Q^{k,۲x} = ۱ \qquad (۴۰)$$

$$\det Q^{k,۲x+۱} = -۱ \qquad (۴۱)$$

لذا ماتریس‌های (۳۸) و (۳۹) وارون‌پذیرند. اکنون وارون این ماتریس‌ها را معرفی می‌نماییم.

تعریف ۷. برای هر عدد صحیح t ، وارون ماتریس‌های (۳۶) و (۳۷) به صورت زیر است

$$Q^{k,-۲t} = \begin{pmatrix} cF_k h(۲t-۱) & -sF_k h(۲t) \\ -sF_k h(۲t) & cF_k h(۲t+۱) \end{pmatrix} \qquad (۴۲)$$

$$Q^{k,-(۲t+۱)} = \begin{pmatrix} -sF_k h(۲t) & cF_k h(۲t+۱) \\ cF_k h(۲t+۱) & -sF_k h(۲t+۲) \end{pmatrix} \qquad (۴۳)$$

اکنون با جایگزینی مقدار حقیقی x به جای مقدار صحیح t در ماتریس‌های (۴۲) و (۴۳) خواهیم داشت

$$Q^{k,-۲x} = \begin{pmatrix} cF_k h(۲x-۱) & -sF_k h(۲x) \\ -sF_k h(۲x) & cF_k h(۲x+۱) \end{pmatrix} \qquad (۴۴)$$

$$Q^{k,-(۲x+۱)} = \begin{pmatrix} -sF_k h(۲x) & cF_k h(۲x+۱) \\ cF_k h(۲x+۱) & -sF_k h(۲x+۲) \end{pmatrix} \qquad (۴۵)$$

که همان وارون ماتریس‌های (۳۸) و (۳۹) می‌باشند.

۴-حاصلضرب هادامارد ماتریس‌های طلایی k- فیبوناتچی (HP.k-FM)

اکنون با تعمیم تعریف حاصلضرب هادامارد ماتریس‌های طلایی فیبوناتچی (۱۲) و (۱۳) به کمک دنباله اعداد k- فیبوناتچی و ماتریس‌های طلایی (۳۸) و (۳۹) و وارون آنها (۴۴) و (۴۵) حاصلضرب هادامارد ماتریس‌های طلایی k- فیبوناتچی را تعریف می‌کنیم. (باید توجه داشت که در این بحث متغیر x حقیقی است.)

تعریف ۸. ماتریس‌های

$$Q^{k,۲x} \circ Q^{k,-۲x} = \begin{pmatrix} cF_k h(۲x+۱)cF_k h(۲x-۱) & -[sF_k h(۲x)]^۲ \\ -[sF_k h(۲x)]^۲ & cF_k h(۲x+۱)cF_k h(۲x-۱) \end{pmatrix} \qquad (۴۶)$$

$$Q^{k,۲x+۱} \circ Q^{k,-(۲x+۱)} = \begin{pmatrix} -sF_k h(۲x+۲)sF_k h(۲x) & [cF_k h(۲x+۱)]^۲ \\ [cF_k h(۲x+۱)]^۲ & -sF_k h(۲x+۲)sF_k h(۲x) \end{pmatrix} \qquad (۴۷)$$

که در آنها $\circ$ همان عملگر ضرب هادامارد رابطه (۱۱) در تعریف (۱) و توابع $sF_k h$ و $cF_k h$ نیز به ترتیب توابع هذلولوی متقارن k- فیبوناتچی رابطه‌های (۲۲) و (۲۳) می‌باشند، را HP.k-FM یا حاصلضرب هادامارد ماتریس‌های طلایی k- فیبوناتچی می‌نامیم.

همانند آنچه در بخش (۲-۲) ذکر گردید و با توجه به فرمول Cassini تعمیم یافته می‌توان ماتریس‌های (۴۶) و (۴۷) را به صورت

$$Q^{k,۲x} \circ Q^{k,-۲x} = \begin{pmatrix} ۱+[sF_k h(۲x)]^۲ & -[sF_k h(۲x)]^۲ \\ -[sF_k h(۲x)]^۲ & ۱+[sF_k h(۲x)]^۲ \end{pmatrix} \qquad (۴۸)$$

$$Q^{k,۲x+۱} \circ Q^{k,-(۲x+۱)} = \begin{pmatrix} ۱-[cF_k h(۲x+۱)]^۲ & [cF_k h(۲x+۱)]^۲ \\ [cF_k h(۲x+۱)]^۲ & ۱-[cF_k h(۲x+۱)]^۲ \end{pmatrix} \qquad (۴۹)$$

نمایش داد.

قضیه ۹. دترمینان ماتریس‌های (۴۸) و (۴۹) به صورت زیر است

$$\det\left(Q^{k,2x}\circ Q^{k,-2x}\right)=1+2\left[sF_k\,h\left(2x\right)\right]^2 \qquad (50)$$

$$\det\left(Q^{k,2x+1}\circ Q^{k,-(2x+1)}\right)=1-2\left[cF_k\,h\left(2x+1\right)\right]^2 \qquad (51)$$

برهان: مشابه برهان قضیه (۳).

اکنون با توجه به روابط (۵۰) و (۵۱) می‌توان وارون ماتریس‌های (۴۸) و (۴۹) را تعریف نمود.

قضیه ۱۰. وارون ماتریس‌های HP.k-FM به صورت زیر است

$$\left(Q^{k,2x}\circ Q^{k,-2x}\right)^{-1}=$$

$$\begin{pmatrix} \frac{1+\left[sF_k\,h\left(2x\right)\right]^2}{1+2\left[sF_k\,h\left(2x\right)\right]^2} & \frac{\left[sF_k\,h\left(2x\right)\right]^2}{1+2\left[sF_k\,h\left(2x\right)\right]^2} \\ \frac{\left[sF_k\,h\left(2x\right)\right]^2}{1+2\left[sF_k\,h\left(2x\right)\right]^2} & \frac{1+\left[sF_k\,h\left(2x\right)\right]^2}{1+2\left[sF_k\,h\left(2x\right)\right]^2} \end{pmatrix} \qquad (52)$$

$$\left(Q^{k,2x+1}\circ Q^{k,-(2x+1)}\right)^{-1}=$$

$$\begin{pmatrix} \frac{1-\left[cF_k\,h\left(2x+1\right)\right]^2}{1-2\left[cF_k\,h\left(2x+1\right)\right]^2} & \frac{-\left[cF_k\,h\left(2x+1\right)\right]^2}{1-2\left[cF_k\,h\left(2x+1\right)\right]^2} \\ \frac{-\left[cF_k\,h\left(2x+1\right)\right]^2}{1-2\left[cF_k\,h\left(2x+1\right)\right]^2} & \frac{1-\left[cF_k\,h\left(2x+1\right)\right]^2}{1-2\left[cF_k\,h\left(2x+1\right)\right]^2} \end{pmatrix} \qquad (53)$$

۵-تعمیمی بر روش رمزنگاری طلایی

در سال ۲۰۰۷ ، Ayse Nalli به کمک حاصلضرب هادامارد ماتریس‌های فیبوناتچی روش رمزنگاری طلایی را تا حد زیادی بهبود بخشیده و بر امنیت آن افزود [Nalli 2007] . اکنون در این‌جا قصد داریم تا این روش را به کمک دنباله k- فیبوناتچی و ماتریس‌های طلایی (۳۸) و (۳۹) تعمیم دهیم تا بر قدرت رمزنگاری آن افزوده شود و عملیات رمزگشایی در ضمن سادگی هنگام استفاده از کلید، به کاری بس دشوار در زمان رمز شکنی بدون مجوز بدل گردد.

در ابتدا فرض می‌کنیم اطلاعات اولیه به صورت دنباله‌ای از اعداد حقیقی مجزای

$$a_1,a_2,a_3,a_4,a_5,a_6,a_7,\ldots \qquad (54)$$

باشد که هر کدام را یک خوانده گوییم. می‌دانیم که تعداد زیادی دنباله عددی مانند (۵۴) وجود دارد که می‌توان به عنوان مثال آورد.

ابتدا چهار خوانده ابتدائی a_1,a_2,a_3,a_4 را از (۵۴) انتخاب نموده و آنها را در یک ماتریس مربعی ۲×۲ مانند M قرار می‌دهیم:

$$M=\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \qquad (55)$$

از این به بعد ماتریس ابتدائی M را به عنوان متن گسترده در نظر خواهیم گرفت (متن ساده رمز نشده)، همچنین می‌دانیم که !۴ جایگشت برای تشکیل ماتریس M از چهار خوانده‌ی a_1,a_2,a_3,a_4 وجود دارد.

تعریف ۱۱. i- امین جایگشت ماتریس ابتدایی M را به صورت $P_i=\left(i=1,2,3,4,\ldots,24\right)$ نمایش می‌دهیم.

حال ماتریس‌های حاصلضرب هادامارد طلایی k- فیبوناتچی (۴۶) و (۴۷) را به عنوان ماتریس‌های رمزنگار و نیز ماتریس‌های وارون آنها یعنی ماتریس‌های (۵۲) و (۵۳) را به عنوان ماتریس‌های رمزگشا برمی‌گزینیم. اکنون روش رمزنگاری و رمزگشایی طلایی مبتنی بر این ماتریس‌ها را معرفی می‌نماییم.

۵-۱-روش رمزنگاری و رمزگشایی HP.k-FM !

در این قسمت الگوریتم‌های رمزنگار و رمزگشا را بر پایه ضرب ماتریس‌ها همانند آنچه در (Stakhov 2007) بیان شده است معرفی می‌نماییم. برای این منظور M متن گسترده (۵۴) می‌باشد که مطابق جایگشت P_i تشکیل یافته است. $E_1(x)$ و $E_2(x)$ متن (پیام) رمز شده؛ $Q^{k,2x}\circ Q^{k,-2x}$ و $Q^{k,2x+1}\circ Q^{k,-(2x+1)}$ ماتریس‌های رمزگذار (۴۶) و (۴۷) و $\left(Q^{k,2x}\circ Q^{k,-2x}\right)^{-1}$ و $\left(Q^{k,2x+1}\circ Q^{k,-(2x+1)}\right)^{-1}$ ماتریس‌های رمزگشای (۵۲) و (۵۳) می‌باشند. می‌توانیم متغیر x را به عنوان یک کلید رمزنگاری یا یک کلید ساده استفاده کنیم. به این معنی که مقدار x عددی متناهی و وابسته به تبدیل متن گسترده M به متن رمزشده‌ی $E(x)$ می‌باشد. مقدار k نیز بیانگر حالتی از دنباله k- فیبوناتچی که برای رمزنگاری به کار گرفته شده است می‌باشد. K نیز همان کلید محرمانه در الگوریتم‌های رمزنگاری متقارن است.

به طور کلی کلید محرمانه K شامل سه قسمت جایگشت P_i، متغیر x و مقدار k (که همان مقدار k در دنباله k- فیبوناتچی می‌باشد) است و آن را به فرم $K=\{P,x,k\}$ نمایش می‌دهیم. بنابراین روش رمزنگاری و رمزگشایی طلایی ماتریس‌های حاصلضرب هادامارد k- فیبوناتچی را می‌توان به صورت زیر نمایش داد:

(رمزنگاری)
$$M\times\left(Q^{k,2x}\circ Q^{k,-2x}\right)=E_1(x)$$
$$M\times\left(Q^{k,2x+1}\circ Q^{k,-(2x+1)}\right)=E_2(x)$$

(رمزگشایی)
$$E_1(x)\times\left(Q^{k,2x}\circ Q^{k,-2x}\right)^{-1}=M$$
$$E_2(x)\times\left(Q^{k,2x+1}\circ Q^{k,-(2x+1)}\right)^{-1}=M \qquad (56)$$

اکنون نشان می‌دهیم که روش رمزنگاری (۵۶) یقیناً یک تبدیل منحصربفرد از متن گسترده‌ی M به متن رمز شده‌ی E و همچنین از متن رمز شده‌ی E به متن گسترده‌ی M بدست خواهد داد. ما تنها به بررسی حالتی که ماتریس حاصلضرب

هادامارد طلایی k- فیبوناتچی (۴۶) به عنوان ماتریس رمزنگار انتخاب شده باشد اکتفا می‌کنیم.

فرض می‌کنیم مقدار کلید محرمانه $x = x_1$ معلوم باشد. در این صورت با توجه به روش (۵۶) خواهیم داشت

$$M \times \left(Q^{k,2x} \circ Q^{k,-2x}\right) = \begin{pmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{pmatrix} = E_1(x) \quad (۵۷)$$

که در آن

$$e_{11} = a_1\left(1+\left[sF_k h(2x_1)\right]^2\right) - a_2\left[sF_k h(2x_1)\right]^2, \quad (۵۸)$$

$$e_{12} = -a_1\left[sF_k h(2x_1)\right]^2 + a_2\left(1+\left[sF_k h(2x_1)\right]^2\right), \quad (۵۹)$$

$$e_{21} = a_3\left(1+\left[sF_k h(2x_1)\right]^2\right) - a_4\left[sF_k h(2x_1)\right]^2, \quad (۶۰)$$

$$e_{22} = -a_3\left[sF_k h(2x_1)\right]^2 + a_4\left(1+\left[sF_k h(2x_1)\right]^2\right), \quad (۶۱)$$

اکنون عمل رمزگشایی در رابطه (۵۶) ایجاب می‌نماید که

$$E(x_1) \times \left(Q^{k,2x} \circ Q^{k,-2x}\right)^{-1} = \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix} \quad (۶۲)$$

و در نتیجه با توجه به روابط (۶۱-۵۸) و (۴۶) خواهیم داشت

$$d_{11} = e_{11}\left(\frac{1+\left[sF_k h(2x_1)\right]^2}{1+2\left[sF_k h(2x_1)\right]^2}\right) + e_{12}\left(\frac{\left[sF_k h(2x_1)\right]^2}{1+2\left[sF_k h(2x_1)\right]^2}\right) \quad (۶۳)$$

$$d_{12} = e_{11}\left(\frac{\left[sF_k h(2x_1)\right]^2}{1+2\left[sF_k h(2x_1)\right]^2}\right) + e_{12}\left(\frac{1+\left[sF_k h(2x_1)\right]^2}{1+2\left[sF_k h(2x_1)\right]^2}\right) \quad (۶۴)$$

$$d_{21} = e_{21}\left(\frac{1+\left[sF_k h(2x_1)\right]^2}{1+2\left[sF_k h(2x_1)\right]^2}\right) + e_{22}\left(\frac{\left[sF_k h(2x_1)\right]^2}{1+2\left[sF_k h(2x_1)\right]^2}\right) \quad (۶۵)$$

$$d_{22} = e_{21}\left(\frac{\left[sF_k h(2x_1)\right]^2}{1+2\left[sF_k h(2x_1)\right]^2}\right) + e_{22}\left(\frac{1+\left[sF_k h(2x_1)\right]^2}{1+2\left[sF_k h(2x_1)\right]^2}\right) \quad (۶۶)$$

برای محاسبه‌ی درایه‌های ماتریس حاصل از روابط (۶۶-۶۳) می‌توانیم از روابط (۶۱-۵۸) استفاده نماییم. آنگاه خواهیم داشت:

$$d_{11} = a_1 \ , \ d_{12} = a_2 \ , \ d_{21} = a_3 \ , \ d_{22} = a_4 \quad (۶۷)$$

بنابراین

$$D = \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = M \quad (۶۸)$$

که نشان می‌دهد این تبدیل رمزنگاری منحصربفرد بوده و متن گسترده ابتدائی M در ورودی رمزنگار با M در خروجی رمزگشا یکسان می‌باشد.

قضیه ۱۲. دترمینان ماتریس‌های رمزشده‌ی $E_1(x)$ و $E_2(x)$ به صورت زیر است

$$\det E_1(x) = \det M \cdot \left(1+2\left[sF_k h(2x)\right]^2\right) \quad (۶۹)$$

$$\det E_2(x) = \det M \cdot \left(1-2\left[sF_k h(2x+1)\right]^2\right) \quad (۷۰)$$

قضیه (۱۲) ابزار لازم برای آزمون درستی روش رمزنگاری و رمزگشایی (۵۶) را در اختیار می‌گذارد تا به کمک آن اطمینان حاصل شود که فرآیند رمزنگاری بدون اشتباه صورت گرفته و آنچه ما به عنوان متن رمز شده در اختیار داریم، در واقع صورت محرمانه اطلاعات اولیه مورد نظر است. [Tahghighi, et al., 2009]

اکنون به بررسی کارایی روش رابطه (۵۶) از طریق محاسبه زمان مورد نیاز برای اجرای آن می‌پردازیم. اگر زمان اجرای هر عمل ضرب و یا تقسیم را به ترتیب با Δt_m و Δt_f و زمان اجرای هر عمل جمع را با Δt_{ad} نمایش دهیم، آنگاه با توجه به روابط (۶۱-۵۸) زمان تبدیل ماتریس اولیه M به ماتریس رمز $E(x)$ را که با T_e نشان می‌دهیم برابر است با :

$$T_e = 16\Delta t_m + 8\Delta t_{ad} \quad (۷۱)$$

و به همین ترتیب اگر زمان عملیات رمزگشایی را با T_d نمایش دهیم، آنگاه با توجه به روابط (۶۶-۶۳) خواهیم داشت:

$$T_d = 32\Delta t_m + 8\Delta t_f + 16\Delta t_{ad} \quad (۷۲)$$

اما آنچه که در مورد امنیت این روش می‌توان گفت آن است که در این روش متغیر k گرفته شده از دنباله k- فیبوناتچی باعث افزایش چشم‌گیر تعداد حالات مختلف انتخاب کلید رمزنگار و رمزگشای محرمانه K می‌گردد که کار رمزگشایی غیرمجاز را بسیار طاقت فرسا می‌نماید.

۶-نتیجه‌گیری!

در این مقاله روش رمزنگاری طلایی به کمک حاصلضرب هادامارد ماتریس‌های طلایی را با استفاده از دنباله k- فیبوناتچی تعمیم داده‌ایم. در واقع هدف از این کار دستیابی به امنیت بیشتر از دو جهت می‌باشد، یکی رفع آسیب‌پذیری رمزنگاری طلایی [Martin del Rey, et al., 2008] و دیگری ایجاد k حالت مختلف در کلید رمزنگاری برای انتقال متغیر x، که موجب پیچیده‌تر شدن حملات خواهد شد. این سیستم به واسطه‌ی حفظ خواص ماتریس‌های طلایی و سادگی در محاسبات از دقت خوبی برخوردار بوده و دارای خطای کمتری می‌باشد. لذا امنیت و دقت در رمز نمودن که همواره مورد توجه متخصصین رمزنگاری قرار دارد و از جمله اهداف کاربران سیستم‌های رمزنگاری است در این روش به خوبی تأمین می‌گردد.!

مراجع

[1] El Naschie, MS. "The golden mean in quantum geometry, knot theory and related topics." Chaos, Solitons, and Fractals, 1999: 10(8):13037.

[2] Er, M.C. "Sums of Fibonacci numbers by matrix methods, Fibonacci Quart." Fibonacci Quart, 1984: 204-207.

[3] Falcon, S, and A Plaza. "K-Fibonacci sequence modulo m." Chaos, Solitons and fractals, 41, 2009: 497-504.

[4] Falcon, S, and A Plaza. "On the Fibonacci k-numbers." Chaos, Solitons and Fractals, 2006.
[5] Hashemiparast, S.M. Multiparametr golden ratio and its applications. Technical Report, K.N.Toosi Univ.of Technology, 2010.
[6] Johnson, RC. Fibonacci numbers and matrices. Durham University, Durham City: DH1 3LE, UK,, 2007.
[7] Martin del Rey, Angel, and Gerardo Rodriguez Sanchez. "On the Security of “Golden” Cryptography." International Journal of Network Security, Vol.7, No.3, 2008: 448-450.
[8] Nalli, A. "On the Hadamard Product of the Golden Matrices." Int. J. Contemp. Math. Sci., Vol. 2, 2007: 537 - 544.
[9] Rushdan, M, and M Tahghighi. "Development of golden cryptography." The 4th Internatinal Conference on Research and Education in Mathematics (ICREM4). Kuala Lumpur: Malaysia, 2009.
[10] Sloane, NJA. The on-line Encyclopedia of integer sequences2006.www.research.att.com/njas/sequences
[11] Stakhov, A. "The golden matrices and a new kind of cryptography." Chaos,Solitons and fractals, 32, 2007: 1138-46.
[12] Tahghighi, M, M Khamseh, and S Mashhoodi. "Fibonacci numbers and its application in Golden cryptography." 40th Annual Iranian Mathematics Conference . Tehran: Sharif University of Technology, 2009.
[13] Vajda, S. Fibonacci and Lucas numbers, and the Golden Section, Theory and applications. New York: JohnWiley & Sons, 1989.
[14] Vorob'ev, N.N. Fibonacci Numbers. Moscow: Nauka, 1978.
[15] Zhang, F.Z. Matrix theory: basic results and techniques. 1999.