تحلیل امنیت سیستم های رمز نوع RSA مبتنی بر خم های بیضوی

محمد حسن مجیدی
دانشگاه امام حسین(ع)
E-mail:mh_majidi12@yahoo.com

چکیده - سیستم های رمز کلید عمومی نقش مهمی در مدیریت کلید ،تعیین اصالت وامضا های رقمی ایفا می کنند .یکی از مطرح ترین این سیستم ها،سیستم رمز RSA می باشد که در سال۱۹۷۸ معرفی گردید.پس از آن نمونه های دیگر که به نام سیستم های رمز نوع RSA مبتنی بر خم های بیضوی شناخته می شوند معرفی و مورد استفاده قرار گرفته اند.
این مقاله به معرفی سیستم های رمز نوع RSA مبتنی بر خم های بیضوی (سیستم $KMOV$ودمیتکو)و تجزیه وتحلیل حملات انجام گرفته به این سیستم ها می پردازد.به منظور تجزیه وتحلیل دقیق تر این سیستم ها علاوه بر سیستم RSA سیستم LUC که سیستم RSA مبتنی بر دنباله های لوکاس می باشد، نیز مورد تجزیه وتحلیل قرار گرفته است.
این مقاله می تواند در انتخاب سیستم مناسب برای کاربرد مورد نظر، به کاربران کمک نماید.

کلید واژه- سیستم های رمز با کلید عمومی،دنباله های لوکاس،خم های بیضوی،سیستم های رمز RSA،LUC،$KMOV$و Demytko.

۱- مقدمه

پس از معرفی سیستم رمزRSA در سال ۱۹۷۸ ،سیستم های مشابه دیگری بر پایه سیستم رمزRSA طراحی ومعرفی گردیدند .از جمله در سال ۱۹۸۱ سیستم رمزی بر مبنای چندجمله ای های دیکسون معرفی وسپس بر پایه دنباله لوکاس ،بازسازی وبه نام LUC معرفی شد.

درسال ۱۹۸۵کوبلیتز ومیلر مستقلاً استفاده از خم های بیضوی را در سیستم های رمز پیشنهاد کردند.پس از آن کویاما، ماورر،اکاموتوو ونستون و پس از آنها دمیتکو توابع یکطرفه دریچه ای جدیدی را روی خم های بیضوی تعریف شده بر حلقه Z_n معرفی نمودند.سیستم های رمز حاصل از توابع یکطرفه به ترتیب $KMOV$ و دمیتکو نامیده شدند.

در این مقاله حملات معلوم در مقابل سیستم های رمزنگاری نوعRSA وامنیت هر یک از این سیستم ها بررسی می شود.

۲- ریاضیات زمینه

در این بخش دنباله های لوکاس وخم های بیضوی به طور مختصر بیان می شوند.

۲-۱- دنباله های لوکاس

دنباله های لوکاس، کاربردهای زیادی در ریاضیات دارند .از جمله می توان به نقش آنها در آزمون های تعیین اعداد اول ومرکب اشاره کرد.همچنین می توان به کاربرد دنباله های لوکاس، در ساخت مربعهای لاتین دوبدو متعامد ،محاسبه دترمینال برخی ماتریسهای خاص دوری ،محاسبه تعداد نقاط روی یک خم بیضوی که بر روی $GF(2^m)$ تعریف شده و بالاخره به نقش آنها در طراحی سیستم های رمز اشاره کرد.

تعریف۱:فرض کنید P,Q اعداد طبیعی و $\Delta = P^2 - 4Q$ یک غیر مربع باشد، اگر $\alpha = \frac{P+\sqrt{\Delta}}{2}$ و $\beta = \bar{\alpha} = \frac{P-\sqrt{\Delta}}{2}$ ریشه های $x^2 - Px + Q = 0$ در میدان درجه دوم $Q(\sqrt{\Delta})$باشند.آن گاه دنباله های لوکاس $\{V_k\}_{k\geq 0}, \{U_k\}_{k\geq 0}$،متشکل از اعداد طبیعی U_i, V_iمی باشد ،که در رابطه زیر صدق می کنند:

$$V_i + U_i\sqrt{\Delta} = 2\alpha^i \qquad (۱)$$

نماد: k امین جمله های دنباله های لوکاس $\{V_i\}_{i\ge 0},\{U_i\}_{i\ge 0}$ با پارامترهای P,Q ، به ترتیب با $V_k(P,Q),U_k(P,Q)$ نمایش داده می شود.

چون $\alpha \in Q(\sqrt{\Delta})$ یک ریشه $x^2-Px+Q=0$ است α یک عضو $\mathfrak{I}_{\sqrt{\Delta}}$ است(حلقه اعداد صحیح میدان $Q(\sqrt{\Delta})$).

چون $V_i-U_i\sqrt{\Delta}=2\beta^i$ داریم:

$$U_i=\frac{\alpha^i-\beta^i}{\alpha-\beta},V_i=\alpha^i+\beta^i$$

۲-۲- خم های بیضوی

خم های بیضوی یکی از قدیمی ترین مباحث در ریاضیات می باشند که اخیراًبه دلیل کاربردهائی که در رمزنگاری یافته اند، مورد توجه بیشتری قرار گرفته اند.در سال ۱۹۷۸ لنسترا به قابلیت این شاخه از ریاضیات در تجزیه اعداد پی برد.سپس کوبلیتز ومیلر، مستقلاً پروتکل های رمزنگاری که بر خم های بیضوی استوار شده اند را ارائه دادند.به دلیل گستردگی مباحث مربوط به خم های بیضوی، از وارد شدن به جزئیات مطالب مربوط در این بخش خودداری کرده وتنها به معرفی پارهای از مفاهیم ونتایج مورد استفاده در سیستم های رمزنگاری بسنده می شود.

۲-۳-۱-خم های بیضوی روی یک میدان:

تعریف۲:فرض کنید K یک میدان باشد که مشخصه آن مخالف۲و۳ است.همچنین فرض کنید x^3+ax+b ، $(a,b\in K)$ یک چند جمله ای درجه سوم رویK است، که دارای ریشه مکرر نمی باشد..یک خم بیضوی$E(a,b)$ روی K را به عنوان مجموعه کلیه نقاط (x,y) رویK که در معادله $y^2=x^3+ax+b$ صدق می کنند و همچنین یک نقطه که با $\mathcal{O}_k$ نمایش داده می شود و به عنوان نقطه در بی نهایت نام می گیرد، تعریف می شود.به عبارت دیگرداریم

$$E(a,b)=\{(x,y)\in K^2; y^2=x^3+ax+b\}\cup\{\mathcal{O}_k\}$$

تعریف ۳:اگر $E_p(a,b)$ یک خم بیضوی روی میدان اول F_p باشد. D_p مانده غیردرجه دوم به پیمانه p باشد، گروه مکمل $E_p(a,b)$ بوسیله $\overline{E_p(a,b)}$ نشان داده می شود، که خم بیضوی مشخص شده با معادله وایرشتراس

$$D_p y^2=x^3+ax+b \qquad (۲)$$

وبانضمام نقطه در بی نهایت $\mathcal{O}_p$ است.

۲-۳-۲- خم های بیضوی روی یک حلقه: خم های بیضوی روی حلقه ها،مشابه روی میدان F_p می باشند.اختلاف آنها این است که این خم ها یک گروه جابجائی تشکیل نمی دهند.

تعریف۴:فرض کنید n حاصلضرب دو عدد اول p,q باشد وa,b بنحوی باشند که $\gcd(4a^3+27b^2,n)=1$ ، یک خم بیضوی $E_n(a,b)$ روی حلقه Z_n،مجموعه نقاط $(x,y)\in Z_n\times Z_n$ به طوری که $y^2=x^3+ax+b$ به همراه نقطه $\mathcal{O}_n$(نقطه در بی نهایت) می باشد.

۳- سیستم های رمز نوع *RSA*:

۳-۱-*RSA*:

دراین سیستم هرکاربر ابتدا دوعدد اول بزرگ q,p راانتخاب وسپس $n=pq$ را تشکیل ومنتشر می کند. آنگاه عددeکه نسبت به $\phi(n)=(p-1)(q-1)$اول باشد را انتخاب ونهایتاً کلید رمزگشایی مخفی را به صورت زیرمحاسبه می کند:

$ed=1(\bmod\,\phi(n))$برای رمزکردن پیامm،کافی است $c=m^e\ (\bmod\, n)$ وبرای رمزگشایی $m=c^d \bmod n$ محاسبه شوند.

۳-۲-*LUC*:

دراین سیستم نیزهمانندRSA،هرکاربردوعدد اول بزرگ q,pراانتخاب و$n=pq$ را تشکیل می دهد، سپس اعداد $d,$ را به گونه ای کهe نسبت به اعداد$(p+1),(p-1)$ و $(q+1),(q-1)$ ،اول باشد وd،نیز درشرایط زیر صدق کند:

$$ed\equiv 1 \qquad (\bmod\ \psi(n))$$
$$\psi(n)=lcm(p-(\frac{\Delta}{p}),q-(\frac{\Delta}{q})) \qquad (۳)$$

کلیدهای عمومیe,n وکلیدهای خصوصی n,q,d می باشد. هرگاه $V_i=(m,1)$ معرف iامین عضویک دنباله لوکاس با پارامترهای mو1 باشد آنگاه رمزنگاری ورمزگشایی توسط روابط زیرانجام می شود.

$$\begin{aligned} c&=V_e(m,1) \quad (\bmod\, n)\\ m&=V_d(c,1) \quad (\bmod\, n)\end{aligned} \qquad (۴)$$

۳-۳-سیستم های خم بیضوی:

فرض کنید $E_n(a,b)$ یک منحنی بیضوی روی Z_n باشد و $n = pq, N_n = LCM\left(\#E_p(a,b), \#E_q(a,b)\right)$ باشد. با انتخاب کلید عمومی e که نسبت به N_n اول باشد ومحاسبه d با شرط $ed = 1(\bmod N_n)$، بتوان یک سیستم رمز کلید عمومی به گونه زیر طراحی نمود:

کلیدهای عمومی: $E_n(a,b)$, n,e

کلیدهای خصوصی: q,p,d

برای رمز کردن پیام m، ابتدا m را با استفاده ازیکی ازروشهای شناخته شده ،به نقطه M برروی منحنی بیضوی متناظر ساخته، سپس $C=[e]M$ را بعنوان پیام شده M درنظرمی گیرد. برای رمزگشایی کافی است $[d]C=[de]M=M$ محاسبه شود.مشکلی که در اجرای روند فوق ظاهر می شود این است که برای نشاندن پیام m برنقطه M ازمنحنی بیضوی $E_n(a,b)$ نیاز به داشتن q,p می باشد. لذا این روش تنها می تواند برای انجام عمل امضا بکار رود، درنتیجه برای سری کردن پیامها روشهای دیگری ابداع گردیده اند که درادامه دوروش $Demytko$, $KMOV$ معرفی می شوند.

۳-۳-۱-KMOV:

هرکاربر دو عدداول q,p که هردو همنهشت با۲ به پیمانه ۳ می باشند را انتخاب و $n=pq$ را محاسبه ومنتشر می سازد. سپس کلید عمومی e که نسبت به $N_n = lcm(p+1, q+1)$ اول باشد را انتخاب کرده وکلید خصوصی d را به قسمی محاسبه می کندکه:

$$ed \equiv 1 \pmod{N_n} \qquad (۵)$$

برای ارسال پیام $M = (m_1, m_2)$ ابتدا پارامتر b را ازرابطه زیر محاسبه کرده

$$b = m_2^2 - m_1^3 \pmod{n} \qquad (۶)$$

وسپس بااستفاده از کلید عمومی e، پیام $M \in E_n(a,b)$ را بصورت: $C=[e]M=(c_1,c_2)$ رمز می کند.

برای رمزگشایی کافی است ابتدا پارامتر b راازرابطه $b = c_2^2 - c_1^3 \pmod{n}$ محاسبه نموده وسپس با استفاده ازکلید خصوصی d، C $M=[d]C$ را روی منحنی بیضوی $E_n(a,b)$ محاسبه کرد.

۳-۳-۲-دمیتکو:

هرکاربر دوعدد اول بزرگ q,p را انتخاب و $n=pq$ را تشکیل می دهد وبصورت عمومی منتشرمی کند. کاربر یکباربرای همه،پارامترهای b,a را انتخاب وسپس مقادیر زیر رامحاسبه می کند.

$$N_{n,1} = 1cm\left(p+1-a_p, q+1-a_q\right)$$
$$N_{n,2} = 1cm\left(p+1-a_p, q+1+a_q\right)$$
$$N_{n,3} = 1cm\left(p+1+a_p, q+1-a_q\right)$$
$$N_{n,4} = 1cm\left(p+1+a_p, q+1+a_q\right)$$
$$a_q = q+1-\#E_q(a,b)\ ,\ a_p = p+1-\#E_p(a,b)$$

آنگاه کلید عمومی e را که نسبت به کلیه $N_{n,i}$ها $(1 \le i \le 4)$ اول باشد را انتخاب وسپس کلید خصوصی d_i که در رابطه

$$ed_i \equiv 1 (\bmod N_i) \text{ و } 1 \le i \le 4، \qquad (۷)$$

صدق کند را محاسبه می کند.

حال فرض کنید m متن اصلی است که قراراست رمزشود، عملکرد سیستم دمیتکو براین حقیقت مبتنی است که، اگر $m(mod\ p)$، مختص اول هیچ نقطه ای روی $E_p(a,b)$ نباشد، دراین صورت مختص اول نقطه ای روی منحنی $\overline{E_p(a,b)}$ خواهد بود.

فرض کنید $[k]_x\, p_1 = g_k(p_1) = x([k]p)$ مبین k برابر مؤلفه اول نقطه $p=(p_1,p_2)$ باشد اگر m پیام موردنظر برای رمزنگاری باشد، آنگاه:

$$c = [e]_x\, m \qquad (۸)$$

برای رمز گشائی c به طریق زیر عمل می کنیم:

$$[d_i]_x\, c = [d_{ie}]m = m \qquad (۹)$$

که در آن کلید رمزگشائی به صورت زیر محاسبه می شود:

$$\begin{cases} d_1 & if \ \left(\frac{w}{p}\right)=1\,,\left(\frac{w}{q}\right)=1 \\ d_2 & if \ \left(\frac{w}{p}\right)=1\,,\left(\frac{w}{q}\right)\neq 1 \\ d_3 & if \ \left(\frac{w}{p}\right)\neq 1\,,\left(\frac{w}{q}\right)=1 \\ d_4 & if \ \left(\frac{w}{p}\right)\neq 1\,,\left(\frac{w}{q}\right)\neq 1 \end{cases}$$

که درآن $w = c^3 + ac + b (\bmod n)$.

۴-تحلیل امنیت

استفاده گسترده از *RSA* موجب شده است که، تحلیل آن نیز موردتوجه تحلیل گران قرار گیرد. انواع حمله های انجام گرفته براین سیستم را می توان، به سه گروه کلی تقسیم کرد:

۱-حمله هایی که ازساختارچندجمله ای *RSA*بهره می گیرند.

۲- حمله هایی که برپایه طبیعت همریختی*RSA* بنا شده اند

۳- حمله هایی که درنتیجه انتخاب پارامترهای نامناسب به انجام رسیده اند

اغلب این حملات را می تـوان کمـا بیش تعمیم داده وبه حملاتی بر علیه سیستمهای مبتنی بردنباله های لوکـاس و خم های بیضوی تبدیل نمود. حملات گروه اول که ازساختار چندجمله ای *RSA*بهره می جویند را می توان مستقیماًبرعلیه سیستم *LUC*به کاربرد، زیرا دنباله های لوکاس را می توان برحسب چندجمله ای های دیکسون بیان نمود.همچنین به دلیل وجود رابطه بین چندجمله ای های تقسیم وخم های بیضوی، می توان نتایج مشابهی را درموردسیستم های مبتنی بر خم های بیضوی بدست آورد.

نوع دوم حملات را نمی توان به سادگی به حملاتی بر علیه سیستم های *LUC*ودمیتکو تعمیم داد.زیرا این دو سیستم دارای ساختار وطبیعی غیر همریخت می باشند. بنابراین این دو سیستم دربرابر این نوع حملات مقاوم بنظر می رسند.ولی حملات ضربی را می توان دربرخی ازموارد به گونه ای بازنویسی کرد که بر سیستم مزبور نیزقابل اعمال باشد.

گروه آخرحملات، بیش ازآنکه به ضعف*RSA* مربوط باشند، به ضعف درپیاده سازی سیستم وانتخاب نامناسب وبدون دقت پارامترها مرتبط اند.

۴-۱-حملات چند جمله ای:

۴-۱-۱حمله هستد:

با تعمیم حمله بلوم وداویدا، هستد نشان داد، که استفاده از*RSA*با کلید رمزنگاری کوچک*e*،روی شبکه های بزرگی که پیامهای آن بطور خطی به هم وابسته اند، امنیت ندارد. هستد برای انجام این کار به تعمیم روشی برای حل دستگاه معادلات یک متغیره پیمانه ای پرداخت. این روش بعداً توسط تاکاجی ونیاتو به روشی برای حل معادلات چند متغیره ارتقاء یافت.

ازطرف دیگر، کوپراسمیت، اخیراً روشی جدید برای یافتن ریشه های کوچک یک معادله معرفی کرده است که منجر به راهی بهتر برای انجام حمله موفق به *RSA* شده است

قضیه هستد:

$N=\prod_{i=1}^{k} n_i$ ، $n=\min n_i$. یک مجموعه از k معادلات $\sum_{j=0}^{\delta} a_{ij}x^j \overset{n_i}{\equiv} 0$ داده شده که n_i ها دوبدو نسبت به هم اول هستند و $\gcd\left(\left\langle a_{i,j}\right\rangle_{j=0}^{\delta}, n_i\right)=1$ برای همه iها. بنابراین امکان پیدا کردن $x<n$ درزمان چند جمله ای وجوددارد اگر $N > 2^{\frac{(\delta+1)(\delta+2)}{4}}\left(\delta+1\right)^{\delta+1} n^{\frac{\delta(\delta+1)}{2}}$.

قضیه۵: درسیستم رمز*RSA*، یک مجموعه k پیام وابسته خطی با کلیدهای عمومی e_i رمز می شوند.(به پیمانه n_i) در این صورت m کشف می شود اگر $k>\frac{e(e+1)}{2},\ n_i > 2^{\frac{(e+1)(e+2)}{4}}\left(e+1\right)^{e+1}$ جایی که $e=\max e_i$

نتیجه۶: درسیستمهای رمز دمیتکو یا *KMOV*، یک مجموعه ازk پیامهای وابسته خطی رمز شده توسط*RSA* باکلید عمومی e_i وپیمانه n_i کشف می شوند اگر: $k>e^2\frac{\left(e^2+1\right)}{2},\ n_i > 2^{\frac{\left(e^2+1\right)\left(e^2+2\right)}{4}}\left(e^2+1\right)^{e^2+1}$ جایی که $e=\max e_i$.

قضیه ۷ (کوپر اسمیت):فرض کنید که یک چند جمله ای صحیح تکین $\mathcal{P}(x)$ ازدرجه δ وعدد صحیح مثبتN، با تجزیه نامعلوم ،داشته باشیم می توان درزمان چند جمله ای همه جواب های صحیح x_0 تا $\mathcal{P}\left(x_0\right)=0\left(\bmod N\right)$ با $\left|x_0\right|<N^{1/\delta}$ را بدست آورد.

نتیجه ۸: ارسال بیشتر از e پیام وابسته خطی که با سیستم *RSA* یا *LUC* با نمای عمومی $e_i \le e$ وپیمانه n_i رمزشده اند. سیستم را آسیب پذیر می کند.

نتیجه ۹: ارسال بیشتر از e^2 پیام وابسته خطی که با استفاده از سیستم رمز دمیتکو بانمای عمومی $e_i \le e$ و پیمانه n_iرمز شوند، سیستم را آسیب پذیر می کند.

قضیه۱۰: فرض کنید $\mathcal{P}\left(x_1,\cdots,x_m\right)\left(\bmod N\right)$ یک چند جمله ای ازدرجه δ باشد. اگر یک جواب $x_i=y_i$ با$\left|y_i\right|<N^{\alpha_i}$ وجود داشته باشد، دراین

صورت جواب، پیدا می شود به شرطی که $\varepsilon - (1/\delta) > \sum_{i=1}^{m} \alpha_i$ برای بعضی $\varepsilon > 0$

۴-۱-۲-حمله GCD

فرض کنید $m_2 = m_1 + \Delta, m_1$ دو پیام و $c_2 = m_2^e \pmod n$, $c_1 = m_1^e \pmod n$ به ترتیب پیامهای رمز شده m_2, m_1 باشند

حال اگر چندجمله ای های $\mathcal{Q}(x), \mathcal{P}(x)$ بصورت زیر تعریف شوند

$$\mathcal{P}(x) = x^e - c_1 \pmod n \qquad (۱۰)$$

$$\mathcal{Q}(x) = (x+\Delta)^e - c_2 \pmod n$$

ازآنجا که m_1 هم ریشه ای از $\mathcal{P}$ وهم ریشه ای از $\mathcal{Q}$ می باشد، دراین صورت ریشه ای از(۱۱) $\mathcal{R} = \gcd(\mathcal{P}, \mathcal{Q})$ نیزهست. اما $\mathcal{R}$ با احتمال زیاد یک چند جمله ای ازدرجه ۱ است، با یافتن ریشه $\mathcal{R}$ به ترتیب می توان به m_1 و $m_2 = m_1 + \Delta$ دست یافت.

جدول زیر اندازه حداکثر کلید عمومی *e* برای موفقیت حمله *GCD* را نشان می دهد

۳۲بیت	*RSA,LUC*
۱۶بیت	*Demytko*
∞	*KMOV*

۴-۱-۳-حمله *Garbage –man-in-the-middle*

ایده اصلی این حمله، براساس امکان دسترسی به صندوق گیرنده است. نمونه اولیه این حمله، ابتدا توسط داویدا برعلیه *RSA* به کار رفت. دراین حمله تحلیل گر ابتدا به قطع ارتباط پرداخته، پیام رمز شده را دریافت کرده، تابعی را برآن اثر داده وپیام تغییر یافته را برای گیرنده ارسال می دارد، گیرنده پس از دریافت پیام c' اقدام به رمزگشایی آن می کند، ولی پیام تغییر یافته ونامفهوم m' را دریافت می کند. حال اگر گیرنده اقدام به دورانداختن m' نموده وتحلیل گر به آن دستیابی داشته باشد، قادر به کشف پیام *m* خواهد شد.

۴-۲-حملات همریخت:

ویژگی همریخت بودن ساختار *RSA* باعث آسیب پذیری این سیستم دربرابر پاره ای ازحملات از جمله، حمله داویدا شده است. لذا هرحمله از نوع همریخت را می توان برعلیه سیستم *KMOV* نیز اعمال نمود (به وضوح از آن جا که روی یک منحنی بیضوی $[k](P+Q) = [k]P + [k]Q$ است) کالسیکی روشی مشابه را ارائه داد، که توسط آن میتوان سیستم دمیتکو را مورد حمله قرارداد.دراین بخش به حملات همریخت ازجمله حمله پیامهای انتخابی و حمله براساس پیمانه مشترک خواهیم پرداخت.

۴-۲-۱-حمله پیام انتخابی:

این حمله زمانی برعلیه سیستم اعمال می شود، که ازسیستم رمز برای امضاء پیامها استفاده شود. دراین صورت دشمن (تحلیل گر) درصورت موفقیت برای انجام این حمله، می تواند با گرفتن امضاء یک پیام بی معنی (بی ارزش)، به امضاء یک سند باارزش دست یابد. شمای کلی کار،به این ترتیب است که اگر هدف تحلیل گر، گرفتن امضاء ازکاربر*A* برای پیام *m* باشد، اوابتدا باانتخاب عدد*k* که نسبت به *e* اول است، با استفاده از الگوریتم اقلیدسی توسعه یافته می تواند *u* , *v* را به گونه ای انتخاب کندکه $ku + ev = 1$ باشد.سپس با محاسبه $m' = m^k \bmod n$ از *A* درخواست امضاء برای m' می نماید. امضاء *A* روی m' عبارت است از: $s' = m'^d \bmod n$به همین ترتیب وی با استفاده از رابطه(۱۲) $s = s'^u m^v \pmod n$ قادر به محاسبه امضاء*A* روی پیام *m* خواهد شد.

۴-۲-۲-حمله پیمانه مشترک:

سیمونز نشان داد که *RSA* درصورت استفاده از پیمانه مشترک برای کاربران متفاوت آسیب پذیر است. چرا که، اگر دو کاربر دارای کلیدهای همگانی $(e_2, n), (e_1 n)$ بوده واگر $\gcd(e_1, e_2) = 1$ باشد دراین صورت اعداد صحیح *v,u* موجودند بنحوی که $ue_1 + ve_2 = 1$، بنابراین اگر فرد سومی پیام مشترکی را برای دوکاربر مورد نظر ارسال کند، متون رمز شده $c_2 = m^{e_2} \pmod n$, $c_1 = m^{e_1} \pmod n$ حاصل می شود ودراین صورت تحلیل گرمی تواند بااستفاده ازرابطه زیر به پیام دست یابد

$$m = m^{ue_1 + ve_2} \equiv c_1^{u_1} c_2^{v} \pmod n \qquad (۱۳)$$

به دلیل ساختار کاملاً مشابه(فقط جمعی و نه ضربی) سیستم *KMOV* ،می توان به روش مشابه، این حمله را برعلیه این سیستم اعمال کرد.

۴-۳-سایر حملات:

۴-۳-۱-حمله وینر:

وینر،نشان داد که اگر کلید خصوصی d ،بسیار کوچک انتخاب شود ،دراین صورت قابل کشف است. درسیستم رمز RSA، کلید عمومی e وکلید خصوصی d بصورت $ed \equiv \left(\mathrm{mod}\,1cm\left(p-1,q-1\right)\right)$ ارتباط دارند.

جدول زیر به طور خلاصه، مینیمم طول کلید خصوصی، برای اجتناب ازحمله وینر را نشان می دهد:

n	۵۱۲	۱۰۲۴
KMOVوLUCوRSA	~ 128	~ 256
Demytko	~ 64	~ 128

۴-۳-۲:حمله لنسترا:

درسال ۱۹۹۶، بونه و دمیلوو لیپتون ازمشخصه بلکر،یک حمله جدید علیه RSA زمانی که با استفاده از قضیه باقی مانده چینی تشکیل شده باشد را بیان نمودند. پس از آن لنسترا این حمله را کامل نمود، نشان می دهیم که حمله لنسترا قابل اعمال روی همه سیستم های برپایه قضیه باقی مانده چینی می باشد.

فرض کنید qوp دو عدد اول و $n = pq$. فرض کنید پیام m توسط کلید خصوصی d بااستفاده از RSA ، امضا شود بااستفاده از قضیه باقیمانده چینی مقدار s با استفاده از $s_p = m_p^{dp} \bmod p$, $s_q = m_q^{dq} \bmod q$ بطور موثر محاسبه می شود

فرض کنید یک خطا درخلال محاسبات s_p اتفاق افتد .($\hat{s}_p$ مقدار دارای خطا است) اما درخلال محاسبات s_q خطائی اتفاق نیفتد.بااعمال قضیه باقیمانده چینی روی $s_q, \hat{s}_p$ ، امضای دارای خطا $\hat{s}$ برای پیامm حاصل می شود،سپس با استفاده از $\gcd\left(\hat{s}^e - m \bmod n, n\right)$فاکتور خصوصی q حاصل می شود.

۵-نتیجه‌گیری

امنیت همه این سیستمها برپایه سختی تجزیه پیمانه عمومی n است. ملاحظه می شود که سیستم LUC هیچ امتیازی نسبت به RSA ندارد، بعلاوه محاسبات دنباله لوکاس پرخرج وگران است. عملاً هیچ دلیلی برای استفاده LUC درعوض RSA برای هدف امنیت وجود ندارد. برای سیستم هایRSA مبتنی بر خم های بیضوی، جمع نقاط روی خم های بیضوی زمان بیشتری ازتوان رساندن مصرف می کند. امنیت سیستم KMOV ،قابل مقایسه با RSA است، به جزدرمقابل حملات چند جمله ای، که سیستم KMOV مقاومت کمتری دارد. همچنین سیستم دمیتکو معمولاً دارای امنیت بیشتر است.

به نظر، سیستم RSA بهترین نسبت بین امنیت و کارایی را فراهم می کند. چون اندازه فاکتوراول خصوصی برای سیستمهای براساس مسأله تجزیه، مستقل ازساختار اساسی است، طراحی یک سیستم رمز نوع RSA قابل رقابت کاملاً مشکل به نظر می رسد.

مراجع

[1]:K.Koyama,U.M.Maurer,T.Okamato,andS.A.Vanstone,New public-key schemes baseb on elliptic curves over the ring Z_n ,

[2]:N.Demytko,A new elliptic curve based analogue of RSA ,

[3]:R.G.E.Pinch,Extending the Hastad attack to LUC,Electronics Letters 31(1995),no.21,1827-1828.

[4]:security of RSA-type cryptosystems over elliptic curves against hastad attack,Electronics Letters 30(1994),no.22,1843-1844

[5]:K.Kurosawa,K.Okada,and S.Tsujii,Low exponent attack against elliptic curves RSA,

[6]:on the security of the KMOV public key cyptosystem,

[7]:Protocol failures for RSA –like functions using Lucas sequences and elliptic curves,

[8]:A chosen message attack on Demytko's elliptic curve cryptosystem,

[9]:Common modulus attack against Lucas-based systems,

[10]:D.Bleichenbacher,M.Joye,andJ.-J. Quisquater,A new and optimal chosen message attack on RSA-type cryptosystems,