د خطي مقايسي د حل الجبري الگورېتم او په RSA رمز جوړوني سېستم کې يې کارونه

پوهنيار اسدالله ترابي اوپوهنمل محمد فاروق حکيمی

لنډيز: الجبري الگورېتم د خطي مقايساتو د حل په لاسته راوړلو کې د يوه ميتود په توگه کاريدلي دي. د دي تگلاري اصلي موخه خطي مقايسه د خطي معادلو شکل ته بدلول او الجبري حل موندل دي. څېړنه يوه کتابتونې څېړنه ده، د معتبرو داخلي او خارجي منابعو څخه استفاده شوي ده، تر ژوري پلټني او پرتله وروسته دا پايله لاسته راغلي چي الجبري الگورېتم په مرسته په ساده ډول محاسبات تر سره کېږي څکه په محاسباتو کې د الجبري مفاهيمو څخه گټه پورته کېږي او د الجبري مفاهيمو درک هر زده کونکي ته تر ډيره بريده اسانه دي. د خطي معادلو د حل تگلاري موثريت د تاکيد په موخه څو ښکاره بيلگي راوړل شوي دي. د رمزجوړونه په برخه کې د پورتني الگورېتم کارونه د RSA رمز جوړوني سېستم په چوکات کې تشريح شوي چي دالجبري الگورېتم اغېزمنتيا را په گوته کوي.

کليدي کلمې: خطي مقايسه، عددونو تيوري، خطي معادله. رمز جوړونه، RSA

سريزه

د انترنيټ اوبرېښنايي سودا گرۍ وده، د برېښنايي اړيکو خونديتوب هر وگړي د سري کرښي مفهوم خپل کړ. هر ورځ په زيا شمېر پټ شخصي معلومات په برېښنايي توگه لېږد او ذخيره کېږي. سازمانونه په دولتي او سوداگريزه بزخه کې بايد معلوماتو د لېږد په وخت کې خويندي وساتي. رمز ورکول او رمز لري کول د کمپيوټر د علم يو مهمه موضوع گڼل کېږي چي هر څوک ور ته اړتيا لري مگر مشخص کسان په مرسته رمز ورکولو او رمز لري کولو پروسه مخته وړل کېږي. د رمز ورکولو په مرسته کولای شو معلومات په خوندي توگه و لېږد وو. د رمزورکولو لپاره دوه بيلا بيل سېستمونه شتون لري. يو د خصوصي کلي رمز ورکول چې د پيغام د لېږونکي او د پيغام تر لاسه کوونکي تر منځ پټه کلي دي چې د پيغام رمز لري کولو لپاره يې کاريږي. د دي ډول رمز مشهور بيلگه د سيزار (Caesar's cipher) رمز دي چې د $f(p) = (p + k) mod\ 26$ مساوات په مرسته لاسته راځي.

د رمز ورکولو دويم سېستم د عمومي کلي رمز په نوم ياديږي په دي سېستم کې د عمومي کلي څخه د پيغام رمز ورکول په برخه کې استفاده کېږي او د خصوصي کلي څخه د پيغام د رمز لري کولو کې ور څخه گټه پورته کېږي. ښه بيلگه يې د RSA رمز ورکولو سېستم دي. چې په کال ۱۹۷۸ م کې د (Rivest, Shamir and Adlemann) په نوم نومول شوي دي. د RSA سيستم خصوصي کلي له دوو لومړنيو عددونو p او q څخه جوړه ده. عمومي کلي د n او e عدد لاسته راځي، چې n د p او q ضرب حاصل او e د $(q - (p - 1)$ $(1$سره متقابلا لومړني عدد دي. په رمز ورکول او رمز لري کول دغه ډول سيستم د خطي مقايساتو له مفهوم څخه گټه پورته کوي نو خطي مقايسات په رمزورکولو په سېستم کې اغېزمن رول لوبوي چي د خطي مقايساتو حل لاري د تيرو څو لسېزو راهېسي د پام وړ توجه خپله کړي ده. دغه ستونزه د ډيرو ليکنو په مرسته د بيلا بيلو اړخونه له مخي د مطالعي لاندي نيول شوي ده. د خطي مقايسي د حل بيلا بيلي تگلاري په ځانگړي توگه د خطي مقايساتو د سېستم لپاره شتون لري.

د خطي مقايسي حل په لاسته راوړلو په موخه په ۲۰۰۵ م کال کې Gold او د هغه ملگريو د تغير شکل تگلاري څخه د وسيلي په توگه استفاده کړي ده. ترڅو د خطي مقايسي د حل ساحه او شرايط تعين کړي. د حل دغه کړنلاره د $cx \equiv a\ mod\ b$ د حل سره ورته

والي درلود کوم چې د اويلر توشن تابع (Euler totient function) په مرسته د c سره اړيکه لري چې په پرمختګ سره به يې د رمز ورکولو او رمز لرې کولو اړوند مسايلوشتون ته د عمومي کلي په سېستم کې لاره برابره کړي (Gold et al،2005).

د ستين (Stein) په نوم رياضي پوه په خپل کتاب کې ويلي دي د عددونو په تيوري کې داسي تګلاره شتون لري چې په مرسته يې راکړل شوي خطي مقايسي د ډايوپنتاين دوه مجهوله خطي معادلې شکل $ax + by = c$ ته د حل په موخه تبديلولای شو(Stein, 2009). کوشي د خطي مقايسي د حل لپاره د مودولو ضربي معکوس الګوريتم وړاندي کړ که څه هم په دي اړه بيلا بيلي تګلاري شتون لري ليکن د خطي مقايسي حل لاسته راوړل ستونزمن کار دي دا ځکه چې تګلاري د پيچليوالګوريتمونو څخه ګټه پورته کړي ده(Koshy, 2007). په همدي دليل په د غه ليکنه کې هڅه کېږي چې يو جامع ، ګام په ګام او د پيچليو محاسبو څخه خالي الګوريتم په نښه شي، چې د خطي معادلو په حل کې د پيچليو محاسبو څخه مخنيوي وکړي دغه کار به د رياضي زده کړلايانو سره په خاصه توګه د نويو زده کوونکو او د هغوځانګو زده کړلايانو سره چې د عددونو تيوري مضمون لولي مرسته وکړي. ځکه چې هر زده کوونکي د الجبري مفاهيمو سره تر ډيره بريده بلد او ګټه تر پورته کولای شي. د الجبري الګوريتم کارونه به زده کوونکو او لوستونکو په دي پوه کړي چې په رياضی کې لنډې او ساده لارې هم سته دا په دې مانا چې نوموړي الګوريتم د نورو الګوريتمو په څېر د پيچلو عمليو څخه استفاده نه کوي(*Adams*،2010). دغه تګلاره به له استادانو او زده کوونکو سره د مقايساتو تيوري په مفهومي زده کړه کې ډيره مرسته وکړي. د يادي موضوع مطالعه به زمونږ سره د رمزجوړوني په برخه کې هم مرسته وکړي ځکه چې د خطي مقايساتو سېستم د مفهوم له مخې د انټرنيټي معلوماتو د خونديتوب په موخه رمز ورکولای او رمز لري کولای کې تغيرات راوستلي شو. د الجبري الګوريتم څخه په هغو پرګرام جوړه ونکي ګټه اخېستلي شو چې په اتومات ډول د خطي مقايساتو سېستم ستونزي حلوي(Gold et al،2005). دغه ليکنه به د هغو ليکونکو لپاره لاره پرانيزي چې دي موضوع ته ورته څېړني ممکن تر سره کړي کيدای شي دغه الګوريتم د نورو پرمختلو الګوريتمونو لپاره پيلامه شي تر څو د خطي مقايساتو اړونده مسايلو دقيقي حل لاري لاسته راوړو. ذکر شويو ستونزو ته په کتو اړينه ده چې په دې اړه نوري ليکني هم تر سره شي.

ابتدائي موضوعات.

د دي لپاره چې د خطي مقايسي مفهوم په سمه توګه درک کړو اړينه ده چې د لاندي تعريفونو، قضيو او ځانګړنو باندي بحث و کړو تر څو چې ليکنه نور هم غني او پر مفهوم شي.

تعريف : هغه خطي معادله چې د برابرښت رابط ولري د مقايسي په نوم يادېږي. فرضوو چې n مثبت تام عدد اوb, a دوه تام عددونه د n په مودولو برابرښت لري،که چېري $a - b$ پهn باندي د هر k تام لپاره $a - b = nk$ صدق وکړي. امکان لري چې د مساوات تولې ځانګړني دي په مقايسه کې صدق ونه کړي مګر ځيني اساسي ځانګړني يې سره ورته دي لري چې په لاندي قضيه کې واړندي شي(Koshy, 2007).

لومړي قضيه: که چېري a او b تام عددونه او n مثبت تام عدد وي نو د $ax \equiv b \ mod \ n$ خطي مقايسي حل شتون لري که چېري يوازي که چېري د a او b ګډ لوی وېشونکي د b فکتور وي.

دويم قضيه : د $n \neq 0$، $ax \equiv b\ (mod\ n)$ مقايسه چې $gcd(a, n) = d|b$ د n په مودولو d نابربره حلونه لري.

انعکاسي ځانګړنه: که چېرې $\boldsymbol{a}$ تام عدد وي نو $\boldsymbol{a \equiv a \bmod n}$.

تناظري ځانګړنه: که چېرې $\boldsymbol{a \equiv b \bmod n}$ ، نو $\boldsymbol{b \equiv a \bmod n}$ دي.

انتقالي ځانګړنه: که چېرې $\boldsymbol{a \equiv b \bmod n}$ او $\boldsymbol{b \equiv c \bmod n}$ نو $\boldsymbol{a \equiv c \bmod n}$ دي.

ساده کولو ځانګړنه: که چېرې $\boldsymbol{k}$ د $\boldsymbol{a}$ او $\boldsymbol{b}$ وېشونکي وي نو $\boldsymbol{\frac{a}{k} \equiv \frac{b}{k} mod\ \frac{n}{k}}$ مقایسه هم صحت لري.

لري کولو ځانګړنه: که چېرې $\boldsymbol{gcd(k,n) = 1}$ وي نو د $\boldsymbol{ak \equiv bk(\ mod\ n)}$ مقایسه په $\boldsymbol{a \equiv b \bmod n}$ ډول لیکلي شو.

د جمع عملیه ځانګړنه: که چېرې $\boldsymbol{a \equiv b \bmod n}$ وي نو $\boldsymbol{a + k \equiv b + k(\ mod\ n)}$.

د تفریق عملیه ځانګړنه: که چېرې $\boldsymbol{a \equiv b \bmod n}$ وي نو $\boldsymbol{a - k \equiv b - k(\ mod\ n)}$.

د ضرب عملیه ځانګړنه: که چېرې $\boldsymbol{a \equiv b \bmod n}$ وي نو $\boldsymbol{ak \equiv bk(\ mod\ n)}$.

مواد او تګلاره

په دې لیکنه کې الجبري الګورېتم ته وده ورکړل شوي ترڅو په مرسته يې د خطي مقايسي حل په اسانه توګه لاسته راوړو. د الګورېتم اغېزمنيا د ثبوت په موخه يو لړ ازمايښتونو او محاسبو څخه استفاده شوي ده. الګورېتم د يو شمېره واضح مثالونو په وړاندې کولو سره امتحان شوي دي. ياد الګورېتم د RSA رمز ورکولو په سېستم کاريدلي دي. د مقالي د ښه فهم او درک په موخه د خطي معادلي او خطي مقايسي اړونده ټول اړين موضوعات په پوره توګه تر بحث لاندي نيول شوي دي. د داخلي او خارجي معتبرو منابعو څخه استفاده شوي مواد د رياضيکي اصولو په رڼا کې تحليل او تفسير او په منظم توګه ترتيب شوي ترڅو زده کړلايان او لوستونکي په اسانه توګه پوه شي چې کوم موضوعات په دې ليکنه کې تر بحث لاندي نيول شوي دي. د ډېرو موضوعاتو په تحليل او ترتيب کې د هم مسلک استادانو سره مشوره شوي ده. به د ښکاره مثالونه او پايلي په مرسته به وښودل شي چې له الجبري الګورېتم څخه د خطي مقايسي په حل او د RSA د رمز جوړوني سېستم کې موثره استفاده شوي ده.

کله چې خطي مقايسي حل د الجبري الګورېتم په مرسته لاسته راوړو د $\boldsymbol{ax \equiv b \bmod n}$ شکل لرونکي خطي مقايسه د $\boldsymbol{x \equiv b + nq}$ خطي معادلي شکل ته بدلوو په لاسته راغلي خطي معادله کې $\boldsymbol{b}$ پاتي شوني، $\boldsymbol{n}$ مودولو او $\boldsymbol{q}$ اختياري تام عدد دي. د دې کار اصلي موخه په الجبري توګه د خطي مقايسي حل لاسته راوړل دي. د خطي مقايسي د حل الجبري الګورېتم پړاونه په لاندي توګه درپېژنو (Gold et al، 2005).

لومړي پړاو: د خطي مقايسه حل لرل او نه لرل ډاډمن کړي.

دويم پړاو: د نامعلوم مجهول له مخي خطي مقايسه د خطي معادلي شکل ته واړوي.

درېیم پړاو: د خطي معادلې کوچیني مثبت حل داسې پیدا کړي چې مجهول ته مثبت تام قیمت لاسته راشي.

څلورم پړاو: لاسته راغلي قیمت په خطي معادله کې امتحان کړي. تر څو معلومه شي چې یاد قیمت د خطي مقایسې اصلي حل دي. د مقایسې په شکل کې عمومي حل داسې $x \equiv b(\ mod\ n)$ ښودلې شو چې b کوچیني مثبت تام عدد او n راکړل شوي مودولو دي. د الګوریتم سموالی په موخه لاندې مثال ته ورځو.

مثال : د $16x \equiv 22\ mod\ 26$ خطي مقایسه حل کړي.

لومړي پړاو: د دې له پاره چې خطي مقایسه حل لري، د ابتدائي معلوماتو له لومړي قضیې څخه ګټه پورته کوو. که چېرې aاو b تام عددونه او n مثبت تام عدد وي، نو د $ax \equiv b\ mod\ n$ خطي مقایسې حل شتون لري که چېرې یوازې که چېرې $gcd(a, n)$ د b فکتور وي.څرنګه چې د 16 او 22ګډ لویوېشونکي2 ، د 26 فکتور دي نو د $16x \equiv 22\ mod\ 26$ خطي مقایسه حل لري.

دویم پړاو: د نامعلوم مجهول له مخې خطي مقایسه د خطي معادلې شکل ته بدلوو. که چېرې د $16x \equiv 22\ mod\ 26$ خطي مقایسه د خطي معادلې شکل ته بدله کړو نو وبه لرو: $x = \frac{22+26q}{16}$ یا $x = \frac{11+13q}{8}$

درېیم پړاو: د خطي معادلې لپاره کوچیني مثبت تام قیمت معینوو ترڅو x ته مثبت تام قیمت لاسته راشي. q ته 1 قیمت په پام کې نیسو تر څو x ته مثبت تام قیمت لاسته راوړو.

څلورم پړاو: لاسته راغلي قیمت په خطي معادله کې امتحانوو پایله یې ممکن داسې کوچیني مثبت تام عدد وي چې په خطي مقایسه کې صدق وکړي. د مقایسې په بڼه کې عمومي حل داسې $x \equiv b(\ mod\ n)$ لیکلې شو. b کوچیني مثبت تام عدد او n راکړل شوي مودولو دي. که چېرې $q = 1$ وضع کړو نو لرو:

$$x = \frac{11 + 13)(1)}{8} = \frac{11 + 13}{8} = \frac{24}{8} = 3$$

پوهیږو چې د $16x \equiv 22\ mod\ 26$ خطي مقایسې حل $3mod\ 26$ دي(Stein, 2009).

د خطي مقایسې حل د مفهوم په مرسته د RSA رمز جوړونې سېستم کې د الجبري الګوریتم کارونه

د RSA رمز جوړونې سېستم کې الجبري الګوریتم د هغې خطي مقایسې د حل په لاسته راوړلو کې کارېږي چې د پیغام په رمز ورکولو او رمزلرې کولو کې ور څخه ګټه پورته کېږي. د RSA (Rivest Shamir Adleman) سېستم د رمز جوړونې هغه سېستم دي چې د p او q لومړنیو عددونو څخه د خصوصي کلي په توګه استفاده کېږي. په دې سېستم کې n د p او q د ضرب حاصل او e د $(p - 1)\ (q - 1)$ سره متقابلا لومړني عدد دي. د رمز ورکولو لپاره د مقایسې څخه ګټه پورته کوو. د لاندې موخو د لاسته راوړلو لپاره دغه ډول سېستم کارېږي(Koshy, 2007).

1. د رمز ورکولو تابع چې په RSA کې کارېږي د (trapdoor function) تابع ده. trapdoor function هغه تابع ته وايي چې له يوه لوري يې محاسبه اسانه او بل لوري يې محاسبه ډېره ستونزمنه او يا د دقيقو معلوماتو په نه درلودلو سره ناممکنه وي.
2. د رمز ورکولو لوري يې ډېر اسانه ده ځکه د توان رفع کول او په مودولو د نوموړي عدد ساده کول دي.
3. د خصوصي کلي په نه ستون کې د رمز لري کول ډېر ستونزمن کار دي ځکه د رمز ورکولو مودولو بايد په دوو لومړنيو عددونو باندي تجزيه شي تر څو د رمز لري کولو لپاره نوي مودولو لاسته راشي او په مرسته يې رمز لري شي.

1. په رمز ورکولو کې د (e, n) الگورېتم څخه په لاندي توگه استفاده کوو.
2. د پيغام تام قيمتونه د 0 او $(n-1)$ تر منځ لاسته راوړي. لوي عدد کولای شو په دوه رقمی بلاکونو ووېشو او د بلاک رقمونه د پيغام له يوه توري سره مطابقت لري.
3. ساده متن د n په نوي مودولو سره لاسته راوړو.

د بيلگي په توگه : الف : د RSA رمز جوړوني سېستم له مخي د "PASSWORD" پيغام ته رمز ورکړي که چېري $n = 85$ او $e = 3$ وي.

1. د جدول له مخي د پيغام هر توري تا م قيمت لاسته راوړو.

$$= 16 \ \ A = 01 \ \ S = 19 \ \ S = 19 \ \ W = 23 \ \ O = 15 \ \ R = 18 \ \ D = 04$$

2. د تورو په نبنه شوي قيمتونه په دوه رقمي ډول د تورو په ترتيب سره ليکو.

$$6\ 01\ 19\ 19\ 23\ 15\ 18\ 04$$

3. د کين لوري څخه هر عدد په ترتيب سره د $C \equiv M^3 \ mod\ 85$ په مرسته محاسبه کړي.

$$16^3 \text{ mod } 85 = 16, \ \ 01^3 \text{ mod } 85 = 01. \ \ 19^3 \text{ mod } 85 = 59\ , 19^3 \text{ mod } 85 = 59$$

$$23^3\ mod\ 85 = 12, \ \ 15^3\ mod\ 85 = 04. \ \ 18^3\ mod\ 85 = 52\ , 04^3\ mod\ 85 = 64$$

رمز شوي متن په دي ډول دي: **16 01 59 59 12 04 52 64**

ب : د رمز شوي پيغام رمز لري کړي.

د **16 01 59 59 12 04 52 64** رمز شوي متن د RSA رمز لري کولو سېستم په مرسته ساده متن ته بدلوو پوهېږو چې $q = 17, p = 5$ او $e = 3$ دي. لري کووشودي څخه به جوته شي چې د رياضيکي مسايلو له حل سره لږ بلديت لري(2010، *Adams*).

1. د $(p-1)(q-1)$ په مودولود d قيمت د e عدد په معکوسه شکل محاسبه کوو.

$$(p-1)(q-1) = 4(16) = 64$$

ځکه نو $3d \equiv 1(\ mod\ 64)$ دي.

2. د الجبري الگورېتم په مرسته $3d \equiv 1(\ mod\ 64)$خطي مقايسه حلوو.

$$3d = 1 + 64q \ \ \ d = {(1 + 64q)}/_{3}$$

که چېرې $q = 2$ شي نو د d لپاره تام قیمت 43 لاسته راځي.

د رمز شوي پیغام د رمز لرې کولو په موخه هر دوه رقمي عدد د $d \ mod \ n$ محاسبه کوو.

$$16^{43} \ mod \ 85 = 16, \quad 01^{43} \ mod \ 85 = 01, \qquad 59^{43} \ mod \ 85 = 19, 59^{43} \ mod \ 85 = 19$$

$$12^{43} \ mod \ 85 = 23, \quad 04^{43} \ mod \ 85 = 15, \qquad 52^{43} \ mod \ 85 = 18, 64^{43} \ mod \ 85 = 04$$

د PASSWORD پیغام ساده متن په دې ډول دی: **16 01 19 19 23 15 18 04**

(*William*, ۲۰۰۹)

موندنې:

1. الجبري الګورېتم د خطي مقایسي په حل کې له پیچلیو محاسبو څخه مخنیوی کوي.
2. ریاضي زده کړلایانو سره په خاصه توګه د نویو زده کوونکو سره د خطي مقایسي د حل په لاسته راوړلو کې مرسته کوي.
3. د الجبري الګورېتم کارونه به زده کوونکو او لوستونکو په دې پوه کړي چې په ریاضی کې لنډې او ساده لارې هم سته چې ریاضیکي موضوعات ور باندې حل شي.
4. د هغو لیکنو لپاره لاره پرانیزي چې یادې موضوع سره ورته والې ولرې کیدای شي دغه الګورېتم د نورو پرمختلو الګورېتمونو لپاره پیلامه شي، تر څو د خطي مقایساتو اړونده مسایلو دقیقې حل لارې لاسته راوړو.

پایله

د الجبري الګورېتم او مشهورې تګلارې د خطي مقایسي د نویو حل لارو لپاره لاره برابروي. الجبري الګورېتم د خطي مقایسي په حل کې د هغو زده کوونکو سره مرسته کوي چې د خطي مقایساتو په زده کړه یې نوې پیل کړې وي او یا د دې موضوع په اړه لږ معلومات ولري ځکه د نورو الګورېتمونو په پرتله محاسبه یې اسانه او په لږ وخت کې تر سره کېږي. د واضح مثالونه د حل په مرسته وښودل شول چې له الجبري الګورېتم څخه د خطي مقایسي په حل او د RSA د رمز جوړوني سېستم کې موثره استفاده ګټوره ده.

References:

Adams, D.G. (2010). Distinct Solutions of Linear Congruences. Acta Arithmetical Vol. 141 No. 2.pp. 103- 152

Burger, E. B. (2006). Small Solutions of Linear Congruence over Number of Fields. Rocky Mountain Journal of Mathematics Vol. 26 No. 3.pp 875-888.

Frieze, A. et al. (2006). Reconstructing Truncated Integer Variables Satisfying Linear Congruences. SIAM Journal on Computing. Vol. 17 No. 2. pp 262-280.

Koshy, T. (2007). Elementary Number Theory with Applications. 2nd Ed. Elsevier Publishing Inc. pp. 211-245.

Lindahl, L. A. (2003). Number Theory. Retrieved from http://www2.math.uu.se/~lal/kompendier/Talteori.pdf. Accessed on August 14, 2013.

Stein, W. (2009). Elementary Number Theory: Primes, Congruences and Secrets. 1st Ed. Springer Publication. pp 21-44.

Sburlati, G. (2003). Counting the Number of Solutions of Linear Congruences. Rocky Mountain Journal of Mathematics Vol. 33 No. 4. pp 1487-1497

William Stein. (2009). Elementary number theory: Primes, Congruences and Secrets,. (S. A. Ribert, Ed.) New York, NY 10013, 233 Spring Street, USA: Springer Science and Business Media, LLC.

Algebraic algorithm of the solution of linear congruences and its application in RSA encryption system

Teaching Assist.Asadullah Torabi

Teaching Assist. Mohammad Farooq Hakimi

Abstract:

Algebraical algorithms are used as a method to obtain the solution of linear equations. The main purpose of this approach is to convert linear congruences into linear equations and find algebraic solution. The research is bibliographic research, reliable internal and external sources have been used. After deep study and comparison, we can say that the computations by using algebraic algorithm is very simple and understanding the algebraic concepts are easy for any student. Several clear examples are given to emphasize the effectiveness of the linear equation solving strategy. The workings of the above algorithm in the encryption section are explained in the framework of the RSA encryption system, which shows the effectiveness of the algebraic algorithm.

Key words: Linear congruence, Number theory, Linear equation, Encryption, RSA