په RSA کریپټوګرافۍ کې د لومړنیو اعدادو کارونه

[1] پوهنوال حنیفه حبیب، ریاضي څانګه،طبعي علومو پوهنځی، کابل د ښوونې او روزنې پوهنتون
[2] پوهنیار احمدشاه نوري، ریاضي څانګه، ښوونې او روزنې پوهنځی، ارزګان د لوړو زده کړو مؤسسه

لنډیز

کریپټوګرافي هغه تخنیک دی چې د بریښنایي معلوماتو د لېږد او خوندي ساتلو لپاره امنیتي خدمات چمتو کوي، د کریپټوګرافۍ ټول ډولونه د اعدادو تیورۍ په مفاهیمو استوار دي. په دې مقاله کې RSA کریپټوګرافي او لومړنی اعداد(Prime Numbers)داسې څېړل شوي، چې په بریښنایي صنعت کې د Private key او Public key اهمیت توضیح کوي. لدې سره په بریښنایي راکړه ورکړه کې د بانکي حساب شمېرې، فاسورډونه او د نورو ځانګړو معلوماتو تبادله معمولي کړنه ده او لازمه ده چې د تبادلې دا پروسه له لاس وهنې او انحراف خوندي وي، ددې ستونزې د حل لپاره د لومړنیو اعدادو په مرسته ترسره شوې RSA کریپټوګرافي بهتره ځواب دی. ددې پروسې پیلامه د دوه بېلا-بېلو لومړنیو اعدادو د ضرب حاصل،ریاضیکي ځانګړتیاوې او معیارونه تشکلیوي همدارنګه واضح کوو چې څنګه په RSA الګوریتم کې لومړني اعداد وکارول شی خو د Encryption او Decryption پروسه چټکه او د سیستم امنیت، پیاوړتیا او ځواک د باور وړ وګرځي. په RSA کریپټوګرافۍ کې د خوندي امنیت لپاره د لومړنیو اعدادو ارزښت پدې کې دی چې لومړني اعداد په آسانه دماتیدو او تحلیل کېدو وړ نه دي، یعنې که دوه لومړني عددونه ولرو نو په آسانه نشو کولای چې د هغې ضربي فکټورونه په لاس راوړو. په دې مقاله کې د RSA الګوریتم پر تګلاره او بیلا-بېلو اړخونو، تطبیقي ساحو او د احتمالي بریدونو پر ډولونو او اغېز باندې بحث شوی. په دې څېړنه کې د څېړنې ډول کتابتوني دی او د موادو په ټاکنه کې د استدلال او مقایسې څخه کار اخیستل شوی.

کلیدي کلیمې: الکترونیکي امنیت، الګوریتم، کریپټوګرافي، کوډینګ، لومړني اعداد.

۱. پېژندنه

د ژوند اړتیا ته په پام سره د ټولنې هر وګړی محدودو اړیکو او معلوماتو ته اړتیا لري ځینې وخت لازم وي چې دا اړیکې او د اړیکو معلومات له مداخلې او لاسوهنې خوندي وساتل شی[1] چې زیات وختونه دا ډول مواردو ته په جګړه او مبارزه کې اړتیاپېښیږي[2] بې له دې چې مقابل لوری معلومات وګوري یا ولولي له لومړني کس څخه دوهم کس ته ولېږدول شي. له دې سره؛په اوسنۍ نړۍ کې ټول هغه معلومات چې په انترنیټ کې زیرمه

شوي او یا له یوه کس څخه بل کس ته لیږل کیږي اړتیا ده ،چې له لاسوهنې او انحراف څخه خوندي وساتل شي. کریپټوګرافي دې ستونزې ته ژوندۍ او اغیزمنه حل لار مومي[5]. یعنې کریپټوګرافي د معلوماتو د خوندي استولو یا ذخیره کولو لپاره دکوډ کولو داسې میتود کاروي چې معلومات له لاس وهنې خوندي وساتي [5]. د پروسې په لومړي سر کې د Encryption لپاره یوې کیلي ته اړتیا ده چې له 1970 کال د مخه د Encryption کیلي باید د پیغام لیږونکی شخص څخه پیغام ترلاسه کوونکی شخص ته د خوندي لارې لیږل شوې واي [9] څرګنده ده ،چې دا چاره ستونزمنه ده یعنې که د کیلي لیږلو لپاره خوندي چینل موجود وي نو بیا د پیغام Encryption ته اړتیا نشته، نولازمه وه چې یوه بله داسې لاره ومومندل شي چې د Encryption کیلي لیږلو ته اړتیا پیدا نشي او دوهم کس(پیغام ترلاسه کوونکی) له یوې بلې لارې پیغام د لوستلو وړ شکل ته واړوي[10]. له دې سره د ټکنالوژۍ چټک پرمختګ د کیلي لیږلو د تخنیک ارزښت نور هم ورکم کړ[11] همغه ؤ چې د MIT درېو څېړنکو Adleman،Shamirاو Rivest د کریپټوګرافي نوې ډول رامنځته کړ او د RSA کریپټوګرافي نوم یې ورکړ[12] چې د وخت پرمختللې ټکنالوژۍ په مرسته نه ماتیدونکي بلل کېده او د Asymmetric کریپټوګرافي یو ځانګړی ډول ؤ. په دې ډول کریپټوګرافي کې دوه اړخونه کولای شي چې د یوې ناامنې ارتباطي کرښې په اوږدو کې د کوډ کولو په کیلي موافقه وکړي او د Cipher امنیت ته پام ونه کړي.د RSA امنیت د تام عددونو د فکټور کولو له عمومي ستونزې څخه راځي چې د دوه لویو لومړنیو اعدادو ضرب دی. په دې میتود کې د امنیت کچه په هغه لومړنیو اعدادو پورې اړه لري، چې د کیلي په جوړولو کې کارول شوي وي[1] یعنې په هره کچه لومړني اعداد لوی او الګوریتم یې پیچلي وي په همغه اندازه یې امنیت خوندي بلل کیږي. د RSA په نوي شکل کې اړتیا ده چې دEncryption دکلیي لپاره داسې لومړني اعداد وکارول شي چې په سلګونو ارقام ولري[8]. په دې مقاله کې په ځینو الګوریتمونو بحث شوی چې له ډلې یې Primality Tests دی څو معلومه کړي چې وضعه شوي مثبت تام عدد لومړني، په ډېر احتمالVery likely prime ،مرکب(Composite)دي چې دغه آزموینې د لویو لومړنیو اعدادو د ټاکلو لپاره خورا ګټورې دي همغه وچې په1997کې Rivest، Adi Shamir اوLeonard Adleman د RSA کریپټوګرافي سیستم ته داسې پرمختګ ورکړ چې د عصر غوښتنو ته ځواب وو[9]. مشهور امنیتي سیستمونه له درېو برخو جوړ شوي دي چې د لومړنیو عددونو څخه تشکیل شوې کیلي، د Encryption او Decryption پراوونو څخه عبارت دي[5]، دلته بحث په داسې میتود کیږي چې د Encryption او Decryption لپاره دوه جلا کلیو ته اړتیا لري یعنې کله چې لومړی پیغام د لیږلو لپاره تیاریږي نو دPublic Key په وسیله Encrypt کیږي چې Public Key پټه کیلي نه ده هرڅوک پرې پوهیدای شي[9]. له دې سره؛ کله چې پیغام د موخې کس ته ورسیږي وروسته د Private Key په وسیله Decrypt پروسه صورت نیسي چې دلته Private Key ته پټه کیلي ویل کیږي او هرڅوک یې نشي ترلاسه کولای [8]. په دې تخنیک کېn تعداد لومړني اعداد ددې لپاره کارول کیږي چېn شمیر لومړني اعداد په

اسانۍ سره د تحلیل وړ نه دي نو ځکه يې ماتیدل ستونزمن کار دی. د لومړنیو اعدادو په مرسته چمتو شوي RSA کریپټوګرافي په مخابراتي شبکو کې ډېر اغیزمنتیا او اعتبار لري[6].

۲. تیرو لیکنو ته کتنه

RSA الګوریتم په 1997 میلادي کال کې د Adi Shamir Ron Revister او Leonard Adleman له خوا په MIT کې د عصر د تکنالوژۍ سره سم تشریح او توضیح شو. هغه وخت RSA الګوریتم د Public Key کریپټوګرافي لپاره ارزښتمن تخنیک بلل کیده ځکه دا لومړني الګوریتم ؤ چې دبریښنایی لاسلیک او کوډ کولو لپاره يې اغیزمنه پایله ورکړه او د تخنیک تګلاره يې د ضرب او توان پورته کولو پر بنسټ ولاړه وه.

د RSA کریپټوګرافي او لومړنیو اعدادو په اړیکو او کارولو بېلا-بېلې څېړنې ترسره شوي. په دې برخه کې د هغو څېړونکو کار ته کتنه ترسره کېږي چې RSA کریپټوګرافي او لومړني اعداد يې تربحث لاندې نیولي. له دې ډلې. (2001) .Paillier، m. J د Fast Generation of Prime Numbers on Portable Devices ترسر لیک لاندې مقاله کې د دوه لومړنیو اعدادو په ځای څلور لومړني اعداد وکارول چې د محاسبې لپاره يې زیات وخت ته اړتیا درلوده او له امنیتي اړخه د ډاډ وړ وه ځکه محاسبه يې پیچلې ترسره کېده په کریپټوګرافي کې دا اصل دی چې محاسبه يې هرځومره پیچلې ترسره شي په همغه اندازه يې امنیت د ډاډ وړ بلل کېږي. همدارنګه د B.Persis Urbana Lvy، Purshotam Mandiwa د A modified RSA Cryptosystem based on 'n' Prime Numbers ترسرلیک لاندې په څېړنیزه مقاله کې دRSAکریپټوګرافي Encryption او Decryption یوازې په N پورې تړلي پاتې نه کړل بلکې د هغې لپاره يې نوي فکټورونه محاسبه کړل داځکه چې Encryption او Decryption تخنیکونه یوځه پېچلي دي. همدارنګه Choi، S.-H. S په 2019کال کې د of Modified RSA Development Algorithm using fixed Mersenne Prime numbers for Medical Ultrasound Imaging instrumentation ترسرلیک لاندې یو نوی الګوریتم رامنځته کړ چې دوه تطبیقات يې درلودل یوه يې blind Signature او بل Security و. دوي هڅه وکړه چې د کیلي د ذخیرې او د تولید د وخت په کمولو تمرکز وکړي. له دې سره M.Burton (2014) د Pell's د معادلې څخه په ګټه اخیستنې سره یوه داسې نظریه رامنځته کړه چې له مخې يې بې له دې چې فکټورنه مشخص شي ځانګړې کیلي تشخیص کېږي چې دا چاره د ځانګړې کیلي استحکام زیاتوي. همدارنګه Alda David،M (2006)پردې کار وکړ چې پهRSA کریپټوګرافي کې د دوه لومړنیو اعدادو پر ځای درې لومړني اعداد داسې وکاروي چې د Encryption او Decryption پروسه يې د اصلي RSA په رقم ترسره شي، همدارنګه د ځانګړې توان په راکمولو سره يې د امنیت د تضمین د کچې د لوړولو هڅه وکړه چې ددې کار په کولو سره د Decryption او لاسلیک پروسه پیاوړې کېږي، ددې تګلارې عمده نېمګړتیا داده چې د مستطیل جوړلو لپاره نوروخت ته اړتیا لري لیکن (2017) Kanwar، D د Advanced

Discrete Mathematics تر سرلیک لاندې په کتاب کې یوه ټګلاره معرفي کړه چې د N د لپردولو اړتیا پې له منځه یوړه په دې صورت کې د هیکرانو لپاره دا ستونزمنه شوه چې کارول شوي لومړني اعداد په لاس راوړي که څه ممکنه وه چې سیستم د k_p او d د مجهولاتو د قیمتونو پوسیله د ماتیدو وړ ؤ مګر دلته امنیت د دوه ګڼوني موډل او دوه ځله Encryption او Decryption پر بنسټ د Jordan تابع په کارولو سره د تضمین وړ ؤ. همدارنګه له دې سره ځینې نورو یو نوي مفهوم رامنځته کړ، چې له مخې یې په پروسه کې درېیم لومړني عدد زیاتیږي او د N موډلو د وېشلو وخت زیاتوي او د معمولي RSA کریپټوګرافي په پرتله د Encryption او Decryption پروسه یې چټکه کوي.

د څېړنې ستونزې

دا چې په دې موضوع کې لومړني اعداد او کریپټوګرافي څېړل شوې او کریپټوګرافي د اعداد تیوري او معلوماتي تکنالوژي ترمنځ ارزښت لرونکی ارتباطي پول دی. ددې څېړنې په اوږدو کې ستونزه دا وه چې داسې امکانات او وسایل نشته ترڅو د معلوماتي تکنالوژۍ په ډګر کې د لومړنیو اعداو کارول او تطبیقي موارد په عملي ډول وښیي او تطبیق یې کړي، همدې ته ورته دې موضوع ته په ملي ژبه هیڅ کار نه دی شوی، لوستونکي مجبور دي، چې په نورو ژبو لیکل شویو علمي اثارو او سرچینو ته مراجعه وکړي چې دا کار ټول نشي ترسره کولای.

له دې سره د اعداد تیوري موضوعات په ریاضي څانګه کې لوستل کیږي خو د تطبیق موارد یې په تحصیلي نصاب کې ځای نه لري نو ځکه د ریاضي څانګې لوستونکي د کریپټوګرافي د زدکړې لپوالتیا نه لري.

د څېړنې موخې

- ✓ په الکترونیکي امنیت کې د لومړنیو اعدادو اهمیت.
- ✓ د کریپټوګرافي په کوډینګ اود کیلي په تولید کې د لومړنیو اعدادو کارول.
- ✓ د اعدادو تیوري او معلوماتي تکنالوژي ترمنځ د وصل ټکی موندل.

د څېړنې پوښتنې

- ✓ په RSA کریپټوګرافي کې د لومړنیو اعدادو د کارولو ارزښت څه دی؟
- ✓ په RSA کریپټو ګرافي د احتمالي بریدونو په مخنیوي کې د لومړنیو اعدادو رول څه دئ؟
- ✓ د اعداد تیوري او معلوماتي تکنالوژۍ ترمنځ د اړیکو اهمیت.

د څېړنې اړتیا او ارزښت

د الکترونیکي ډاټا د خوندي ساتلو اولپرلو په وخت کې کارونکي باید ډاډه شي چې د معلوماتو امنیت پې خوندي دی، درېیم کس د مداخلې او یا د معلوماتو د انحراف موقع نشي موندلی دا چاره هلته ممکنه ده چې

د کریپټوګرافي الګوریتم په هغه کچه پیچلی جوړ شي چې د ماتوونکي تر توان لوړ وي، پس د کریپټوګرافي د امنیت پیاوړتیا د هغو اعدادو په نوعیت پورې اړه لري چې د الګوریتم په پروسه کې کارول کیږي. اړینه ده چې داسې لوی او پیچلي ارقام وکارول شي چې آسانه او ارزانه د فکټور نیونې او تجزیې وړ نه وي، دا چاره یوازې د n شمیر لومړنیو عددونو په وسیله کیدای شي او همدارنګه د Public Key او Private key په لاس راوړلو لپاره د JAWA Language اغیزمن تمامیدای شي. له دې سره د غیرمتناسب کریپټوګرافي په لړ کې د داسې میتود پیاوړتیا او استحکام ته اړتیا ده چې د نورو میتودونو او تخنیکونو په پرتله چټک وي چې دا چاره د RSA کریپټوګرافي کې ترلاسه کېدای شي. په دې برخه کې J.J Quisquater او C.Couveur د RSA الګوریتم د چټکتیا لپاره کار وکړ چې C.Couveur د Chicness Remainder Theorem څخه د RSA الګوریتم د توضیح او فعالیت لپاره ګټه واخیسته.

۳. د څېړنې میتودولوژي(کړنلاره) :

د موضوع نوعیت ته په پام سره څېړنه اوکتابتوني تګلاره تشریحي ده، د موضوع دلا ښه وضاحت او غنا لپاره ګڼ شمېر بهرني علمي او معتبرو ژورنالونه،کتابونه،ویب سایټونه ، مقالو او علمي اثارو څخه ګټه اخستل شوې او مفاهیم یې په ساده او روانه ژبه د کمپیوټر د ورډ پروګرام په مرسته ترتیب او تنظیم شوي.

۱،۳. لومړني عددونه Prime Numbers

هر تام عدد چې له (1) څخه لوی اعداد لومړني یا مرکبو اعدادو پورې اړه لري، چې د اعدادو دغه طبقه بندي د اعدادو تیوري د بحث لپاره بنسټیزه پیلامه بلل کیږي.په دې مقاله کې هڅه شوې چې د لومړنیو اعدادو بنسټیز مفاهیم، ځانګړتیاوې او په ګڼو ساحو کې د لومړنیو اعدادو د ارزښت کچه تر څېړنې لاندې ونیول شي همدارنګه هڅه شوې چې د لومړنیو اعدادو د لومړیتوب(Primality)د څرنګوالي لارې-چارې تر څېړنې لاندې ونیسو یعنې معلوم کړو چې آیا یو کیفي عدد لومړنی دی کنه!

۲،۳. د لومړنیو اعدادو تعریف

لومړی تعریف: لومړني عدد هغه طبعي عدد ته ویل کیږي، چې دقیقا یوازې دوه مختلف طبیعي فکټورونه (ویشونکي)ولري.

دویم تعریف: هغه طبیعي عدد چې له یوه څخه لوی وي او لاندې ځانګړتیاوې تصدیق کړي

$$\forall a, b \in \mathbb{N} \; (b|a) \Longrightarrow b = 1 \; or \; b = a \quad \ldots \quad (1)$$

د پورتني تعریف له مخې(1) عدد نه مرکب او نه هم لومړنی عدد دی، همدارنګه د مرکبو او لومړنیو اعدادو بحث یوازې تر مثبت تام عددونو پورې محدود پاتې دی.

۳،۳. د لومړنیو اعدادو بنسټیز مفاهیم

له (1) څخه لوی تام اعداد یا لومړني دي او یا به د لومړنیو اعدادو د ضرب حاصل وي، چې داد ټولو تام عددونو لپاره د استقرأ(Induction)پوسیله آسانه ثبوت کېدلای شی. یعني له(1) څخه لوی هر تام عدد د لومړنیو اعدادو له سیټ څخه د یو یا زیاتو عناصرو د ضرب حاصل په پایله کې تعریف کولای شو.

Gödel's Numbering: ګوډیل داسې عملیه ده چې د هر عبارت د کوډ کولو د ټاکل کېدو او تشریح لپاره کاریږي یعنې د ریاضیکي یادښت هر سمبول ته یوه شمېره ټاکل کېږي، چې څانګړی طبعي عدد د هغه کوډیل شمېره بلل کېږي. Kurt Gödelچې د ګوډیل عدد جوړونکی دی هغه په دې سلسله کې د هر عدد د کوډ کولو لپاره لومړني اعدادوکارول. څرنګه چې یو لومړنی عدد تر خپل څان کوچنی فکټور نه لري، نو هر عبارت(بیان) ددې لپاره چې ابهام لیرې کړي کولای شي یوازې یوه ګوډیل شمېره ولري،همدارنګه هره ګوډیل شمېره یوازې له یوه بیان سره اړیکه پیداکولای شي. سربېره پردې مورږ کولای شو دا عملیه ددې لپاره وکارو څو معلومه کړو چې آیا ورکړل شوي شمېره ګوډیل ده یانه.

Calculating Hash Codes

د هش کوډ د هرې موخې لپاره د شمیرې کوډ دی، چې د یوه پروګرام په وسیله جوړ شوی. هش کوډونه د هش میز څخه د پیچلو موخو د ګړندي ترلاسه کولو او یا ذخیره کولو لپاره کارول کېږی. هش کوډونه باید د هرې موخې لپاره څانګړي وي، څو سمواليې وساتل شي. ددې موخې د هش کوډ په محاسبه کې لومړني اعداد کارول کېږي د بیلګې په توګه دjava تارونو د هش کوډ د محاسبې لپاره لرو چې:

$$s[0] * 31^{(n-1)} + s[1] * 31^{(n-2)} + \cdots + s[n-1] * 31^{0}$$

په دې ډول چېs له 0 څخه تر $n-1$ پورې د n شمیر ارقامو اوږدوالي ښیي او $s[x]$ په s د x^{th} لپاره د $ASCII$ قیمت په ګوته کوي. اوس ګورو چې 31 داسې لومړنی عدد دی چې د 2 طاقت ته نژدې دی(په حقیقت کې $Mersenne$ لومړنی عدد دی).دلته لومړني اعداد ځکه ټاکل کېږي چې د هش بالټونو لپاره خورا ښه معلومات توضیع کوي. په دې ډول دوي له (1) او خپل څان پرته بل ګډ فکټور نه لري. کله چېx لومړنی عدد وي نو د $Modulo\ x$ عملیه د ځوابونو د موندلو لپاره پراخه ساحه تضمینوي، خو که x لومړنی عدد نه وي نو د هش بالټونو شمېر زیاتوالی مومي.

د لومړنیو اعدادو څانګړتیاوې

Mersenne Primes: دا هغه لومړني اعداد دي چې د (2) له طاقت څخه د (1) په اندازه کوچنی وي او د $M_n = 2^n - 1$ په شکل ښودل کېږي. اوس که $2^n - 1$ لومړنی عدد وي نو n لومړنی عدد دی.

قضیه(Theorem): کله چې $2^n - 1$ یو لومړنی عدد وي نو ثبوت کړئ چې n پخپله لومړنی عدد دی

ثبوت(Proof): لومړی فرض کوو چېn مرکب عدد دی، نو ځکه د n لپاره لیکو چې

$$n = n_1, n_2, \ldots. \quad where \quad 1 < n_1 < n_2$$

همدارنګه $1 < n_2 < n$ نو پس $2^{n_1 n_2} - 1$ فکټور عبارت دی له $2^{n_1} - 1$ څخه ، چې نه (1) او نه هم $2^n - 1$ دی.نو ځکه $2^n - 1$ مرکب عدد نه دی بلکې لومړنی عدد دی، په پایله کې وایو چې n لومړنی عدد دی خو باید په پام کې ولرو چې ددې قضې برعکس صحت نه لري.

تراوسه پورې لوی ترین پېژندل شوې لومړنی عدد د میرسن لومړنی عدد دی چې قیمت یې $(2^{57885161} - 1)$ دی ځکه په دوه ګڼي سیستم کې n رقمی عدد تر $(2^n - 1)$ ارقامو پورې نیول کېدای شی. میرسن لومړني عددونه کولای شی بې له دې چې اضافي ساحې ته اړتیا ولري په ښه توګه په دوه ګڼي سیستم وښودل شي همدارنګه Mersenne Twisterیو ښه نیمه تصادفي شمېره ده چې ګټور ریاضیکي الګوریتمونه تولیدوي او د لومړي ځل لپاره د Matsumoto او Takuji Nishimura په وسیله منځ ته راغلي.

مکمل عددونه Perfect Numbers

یو مثبت تام عدد (n) هغه وخت مکمل عدد بلل کېږي کله چې د ټولو مثبتو ویشونکو له مجموعې سره برابر وي بې له دې چې (n) پکې حساب کړل شي. په بل عبارت د (n) عدد هغه وخت مکمل عدد بلل کېږي کله چې د(n) په ګډون د ټولو فکټورونو مجموعه یې $(2n)$ په لاس راکړي د عددونو په بحث کې ددې لپاره چې یو عدد مکمل وښودل شي لازمي او کافي شرط دادی چې تر یوه(1) لوی هر مثبت جفت تام عدد د$2^{(n-1)} * (2^n - 1)$ شکل ولري او راتلونکی حد یې $2^n - 1$ لومړنی وي(چې په حقیقت کې هغه میرسن لومړنی دی) د بیلګې په توګه $6 = 2 + 3 + 1 = 2^1 * (2^2 - 1)$ یو مکمل عدد دی او له (6) څخه وروسته (28) راتلونکی پېژندل شوی مکمل عدد دی. د بشپړو عددونو په څانګړتیاو کې په زړه پورې داده چې د یوه عدد لوګاریتم د هغې د فکټورونو د لوګارتمونو له مجموعې سره برابره دی د بیلګې په توګه همدا پورته مثال په پام کې نیسو

$$log(6) = log(2 * 3 * 1) = log(2) + log(3) + log(1)$$

Goldbach's Conjecture:

د ۱۷۴۲ کال د جون میاشتې په ۷مه نېټه Leonhard Euler په خپل لیک کې Christian Goldbach ته اټکل وکړ چې((هر عدد چې د دوه لومړنیو اعدادو مجموعه وي کېدای شي د زیاتو لومړنیو عددونو د مجموعې په شکل ولیکل شي))چې دا بیان په خپل جوړښت کې له دې سره برابر دی چې هر جفت عدد د دوه لومړنیو اعدادو مجموعه ده ځکه چې Goldbach د(1) د لومړني عدد په حیث په پام کې نیولی و، پس کولای شو دا اټکل په دې ډول بیا تکرار کړو چې له(2) څخه لوی هر جفت عدد د دوه لومړنیو عددونو د مجموعې په شکل لیکلای شو چې دGoldbach اټکل تراوسه پورې تر $4 * 10^{14}$ عددونو پورې درست ثابت شوي، خو دا تراوسه نه ده معلومه چې ایا د ټولو عددونو لپاره صحت لري کنه!

نسبي لومړني عددونهRelatively Prime Numbers

دوه تام عددونه هغه وخت نسبي لومړني عددونه بلل کېږي چې له (1) څخه پرته بل ګډ فکټور ونه لري. یا هم د دوی ګډ قاسم د(1) عدد وي. د بیلګې په توګه (7) او (8) نسبي لومړني اعداد دي.

Euler's Totient Function:

دې ته ځېنې وخت Euler Phi Function هم ویل کېږي او$\phi(n)$ په سمبول سره ښودل کېږي او د هغه مثبت تام عددونو شمیر راښیي چې له(n) څخه کوچنی وي او له (n) سره نسبي لومړني وي، یعنې مشترک قاسم یې (1) وي .اوس که (p) یو اختیاري لومړنی عدد وي نو پس د(p) د Euler's Totient Function قېمت$-(p$ (1په لاس راځي، ځکه هر عدد پې له قید او شرطه په خپل ځان د وېش وړ دی او د (p) اختیاري تام عدد لپاره$(p-1)$ د Euler's Totient Function لوی ترین قېمت دی چې دا ددې لپاره یو دلیل دی چې ولې لومړني عددونه د هش کوډ د محاسبې لپاره کارول کېږي.

Sieve of Eratosthenes

دا ممکن تر ټولو پراخه منل شوی او ګټور الګوریتم وي چې د پخوانیو وختونو راهیسې کارول کېږی دا الګوریتم له(1) څخه تر(n) یا له (2) څخه تر(n) پورې ټول شمیرې لست کوي، ځکه چې(1) نه لومړنی او نه هم مرکب عدد دی. وروسته د اول لومړني عدد ټول ضریبونه په نښه کوي چې په حقیقت کې(2) دي. له هغې څخه د راتلونکي لومړني عدد ضریبونه په نښه کول پیل کوو راتلونکی لومړني عدد 3 دي چې دې معمولي دورې ته تر هغې ادامه ورکوو څو داسې یوې پړاو ته ورسیږو چې تر(n) کوچنی لومړنی عدد پاته نشي، په پای کې ټول په نښه شوي عددونه تر(n) کوچني لومړني عددونه دي.

د Sieve of Eratosthenes الګوریتم

کهA له(2) څخه تر(n) پورې د تام عددونو لست وي په دې ډول چې(n) په دې پروسه کې شامل نه وي.

او$A[i]\ ,\ i = 2,3,4, \ldots . , n$ په پام کې نیسو اوس که چیرې$A[i]$ په نښه شوي نه وي نو لرو چې

$$j = i^2; i^2 + i, i^2 + 2i, i^2 + 3i, \ldots . not\ exceeding\ n$$

دلته ټول$A[j]$ په نښه کېږی.

قضیه: که تر(p) پورې د لومړنیو عددونو ټول مضربونه داسې په نښه کړو چې(p) هم په کې شامله وي نو پس د راتلونکي لومړني نمبر یعنې$(p+x)$کوچني ترین مضرب ؛چې نه دي په نښه شوي$(p+x)^2$ دي، په دې ډول چېx یو جفت عدد وي.

Fermat's little Theorem:

که (p) یو داسې لومړنی عدد وي چې د(n) په تام عدد د وېش وړ نه وي نو پس لرو

$$a^{p-1} = 1(mod\ p) \quad \ldots \quad (2)$$

یا هم پورته بیان په لاندې ډول لیکلای شو

$$a^p = a(mod\ p) \quad .... \quad (3)$$

د فرمټ د الګوریتم په وسیله د لومړنیتوب معلومول

لومړی د(n) عدد داسې په پام کې نیسو چې که عملیه پرې اجرأ شي نو په رښتیا سره باید (n) لومړنی عدد ثابت شي. که چېرې (x) داسې یو اختیاري عدد وي چې له (n) څخه کوچنی وي ، که چیرې $(x^n modulo\ n)$ له (x) سره برابر نه وي نو پس په پایله کې غیرلومړنی عدد په لاس راځي چې د لومړني حالت خلاف پایله ترې راوځي. پر (n) د باور کچه لوړه شي او د (x) د ګڼ قیمتونو لپاره پروسه تکرار کړل شی دلته یوشمیر مرکب عددونه شته چې د*Fermat's little Theorem* په مرسته لومړني عددونه په لاس راځي چې دې عددونو ته *Carmichael Numbers* ویل کیږي.

د *RSA* کارونه

په *RSA* الګوریتم کې د سیستم هر کارونکی دوه عمومي نمبرونه(e,n) جوړوي، چې دې ته*Public Key* ویل کیږی او یوه بله شمېره(d) پټه ساتي چې *Private exponent* بلل کیږي. اوس که دAپه نامه یو کارونکی وغواړي چې یو پیغام دB په نامه یو بل کس ته ولیږي، A غواړي چې B کس *Public Key*وګوري او د M پیغام ولري(په دې ډول چې پیغام د تام عددونو په ارقامو لیکل شوی وي) نو د A کس د پیغام بلاک داسې جوړوي چې اندازه یې ترn کوچنې وي او وروسته د $C = M^e mod(n)$ پیغام یعنې *Cipher text* دB اړخ ته لیږي، د B کس ترلاسه شوي پیغام د $M = C^d mod(n)$ په وسیله بیرته *Decrypt* کوي، چې دلته د الګوریتم امنیت د *Public Key* او *Private Key* په ټاکلو پورې اړه لري نو په دواړو کې باید د امکان تر کچې پیچلي او لوی ارقام وکارول شي.

د RSA کریپټوګرافي د کیلي جوړول

په تصادفي ډول دوه لوی لومړني اعداد یعنې p او q په پام کې نیسو په دې ډول چې $p \neq q$.

I. د P او q د ضرب حاصل په n سره ښیو، یعنې $n = p \cdot q$.

II. د Euler's Totient Function لپاره لرو چې $\phi(n) = (p-1)(q-1)$.

III. د *Encryption* توان په e سره ښییو او داسې یې ټاکو $1 < e < \phi(n)$ وي او $\gcd(\phi(n), e) = 1$.

IV. همدارنګه د *Decryption* توان پهd سره ښییو او داسې یې په لاس راوړو چې

$d \cdot e \ mod\ \phi(n) = 1$ یا هم $d \cdot e = 1\ mod\ \phi(n)$

V. اوس یې $k_{Public} = \{e,n\}$ او $k_{Privat} = \{d,n\}$ او یا هم $k_{Privat} = \{d,p,q\}$ په لاس راغلل.

د Encryption پروسه: په RSA کریپټوګرافي په Encryption کېBپه نامه کارونکی دM پیام دA د عمومي کیلي څخه په ګټه اخستنې سره Encrypt کوي، دلته دB لپاره اړتیا ده چې لاندې کارونه ترسره کړي

a) د A عمومي کیلي یعنې $\{e,n\}$ په لاس راوړل.

b) د M پیغام د $[0, n-1]$ په انتروال کې په تام شکل ترتیبول.

c) د $C = m^e mod\ n$ په لاس راوړل.

d) په لاس راغلي Cipher Text د A کس ته لیږل.

د RSA د Decryption پروسه: ددې لپاره چې پیغام له non-readable شکل څخه د لوستلو وړ بڼې ته تبدیل شي، یعنې Cipher text په Plaintext تبدیل کړل شي نو اړتیا ده چې A له private key څخه په ګټه اخیستنی سره $M = C^d \mid n$ په لاس راوړو.

دبیلګې په توګه ؛ په پام کې نیسو چې $p = 3$ او $q = 5$ ګورو چې $n = 3 \cdot 5 = 15$ په لاس راځي د Euler's Totient Function لپاره لیکو چې

$$\phi(n) = (p-1)(q-1)$$
$$\phi(n) = (3-1)(5-1)$$
$$\phi(n) = 8$$

اوس e داسې په پام کې نیسو چې $1 < e < \phi(n)$ وي، فرض کړئ $e = 3$ دی. همدارنګه

$$gcd(\phi(n), e) = 1$$
$$gcd(8,3) = 1$$

د اخیري ګام په توګه؛ د d لپاره لرو پورته په لاس راغلي قیمتونه په $d \cdot e = 1\ mod\ \phi(n)$ جوړښت کې وضع کوو او لرو چې

$$d \cdot 3\ mod\ 8 = 1$$
$$\Longrightarrow d = 3$$

نو پس د پورته مواردو په بنسټ Pubic key او Private Key په لاندې ډول په لاس راځي

$$K_{Public} = \{e, n\} = \{3,15)$$
$$K_{Privat} = \{d, n\} = \{3,15)$$

کله چې پیغام دلیږونکی شخص په وسیله Encrypt کوو نو لرو چې

$$C = P^e mod\ n$$
$$C = 8^3 mod\ 15$$
$$C = 2$$

ګورو چې د Cipher text قیمت $C = 2$ په لاس راځی او همدا دویم شخص ته لیږل کیږي، کله چې دویم کس د Decryption وغواړي نو لاندې عملیه اجراکوي

$$P = C^e mod\ n$$
$$P = 2^3 mod\ 15$$
$$P = 8$$

اوس ګورو چې $P = 8$ د *Plaintext* لومړنی قیمت دی

دلته د *RSA* کریپټوګرافي *Encryption* آسانه دي یوازې د دوه لومړنیو او څنیو ساده ریاضیکي الګوریتمونو اوعملیو پوسیله صورت نیسي لیکن برعکس پروسه پې بې له دې چې کارونکي کافي معلومات ولري ستونزمنه ده. سربیره پردې؛ ددې لپاره چې د احتمالي ماتیدو د خطر کچه لا کمه شوې وي.

۴،۳. په RSA الګوریتم باندې د بریدونو ډولونه او د هغوی اغیزې

د RSAالګوریتم د ماتولو یوه مستقیمه طریقه داده چې په ضربي ګروپ کې د n عناصرو تر هغې حساب ادامه مومي څو M په لاس راشي. لیکن دا طریقه خورا پیچلې او وخت نیونکې ده. په تیرو کلونو کې په RSA الګوریتم د بریدونو ډولونو زیات پرمختګ کړی چې ځینې یې په لاندې ډول تر څیړنې لاندې نیسو.

۵،۳. د عام ضریب برید Common Modulus Attack:

که چیرې د M یو پیغام دوه ځله د n ضریب په وسیله کوډ کړل شي نو بیا د عام ضریب(CMA)برید ممکنه دی او ددې برید په وسیله یو څوک کولای شي په لاندې ډول د M پیغام په لاس راوړي.

که $C1 = M^{e1} \bmod n$ او $C2 = M^{e2} \bmod n$ په ترتیب سره د M د پیغام Ciphertexts وي، په دې ډول چې $gcd(e_1, e_2) = 1$ وی نو پس برید کوونکی غواړي د $M = C_1{}^{a} * C_2{}^{b} \bmod n$ اصلي پیغام د $e_1 * a + e_2 * b = 1$ لپاره په لاس راوړي. دلته د لوی مشترک ویشونکی (GCD) د غځیدلي شکل په کارولو سره لومړی a او b په لاس راوړي وروسته چې Private key یعنې d ته لاس رسی ولري M محاسبه کوي. د CMA برید په Hamami او Aldariseh میتودونو کې د تطبیق وړ دی، ځکه چې دا د اصلي RSA الګوریتم په څېر Encryption او Decryption طریقې کاروي لیکن په نورو طریقو کې یوازې دېبساري تام عدد k په کارولو سره دوه Cipher texts تولیدوي او داسې جوتیږي چې په هغه میتود باندې دا برید ستونزمن یا نا ممکن دی.

Chosen Cipher Text Attack: د دوه Ciphertexts د ضرب حاصل د اړونده Plaintexts د ضرب حاصل له Encryption سره برابر دی چې $M1^e \cdot M2^e = (M1.M2)^e mod\ n$ په لاس راکوي. نو له دې امله تر بحث لاندې CCAبرید په RSA الګوریتم باندې ممکن دی. چې الګوریتم یې په دې ډول ترسره کیږي.

که $C = M^e mod\ n$ وی، برید کوونکی د r عدد په تصادفي ډول داسې انتخابوي چې $1 < r < n$ په دې ډول چې $gcd(r, n) = 1$ وی، وروسته $x = r^e \bmod n$ ، $C' = x * C \bmod n$ ، $z * r = 1 \bmod n$ محاسبه کیږي او C' د موخې په لوری لیږل کیږي او د موخې شخص $M' = (C')mod\ n$ په لاس راوړي وروسته M' برید کوونکی ته استوي او برید کوونکی اصلي پیغام یعنې $M = z * M' \bmod n$ په لاس راوړي.

دلته برید په منطقي استنباط او څېرکتیا پورې اړه لري چې ایا برید کوونکی د Decryption میکانیزم ته لاسرسی پیدا کولای شي کنه. د *CCA* برید په *RSA* او Humami and Aldarish کې ممکن دی.

Timing Attack: دا یو له هغه بریدونو څخه دی چې په RSA الګوریتم کې د کوکر (*KoCher*) پوسیله واقع کیږي. ښیي چې برید کولای شي د هغه وخت په پام کې نیولو سره چې کمپیوټر د *Encrypted* پیغام

Decryption لپاره خومره وخت ته اړتیا لري تر څو د Private Key قیمت مشخص کړای شي. د بیلګې په توګه که د سمارټ کارډ قضیه په پام کې ونیسو چې د *RSA* الګوریتم پټه کیلي له لري ګورو چې سمارټ کارډ د لاسوهنې یا مداخلې په وړاندې مقاومت درلودونکي دی نو برید کوونکی نشي کولای چې د هغې منځپانګه وګوري او کیلي ښکاره کړي. (*KoChen*) ښیي چې هغه وخت معلوم کړي چې د سمارټ کارډ له خوا د*RSA* الګوریتم د *Decryption* لپاره کارول شي او بریدګر په چټکۍ سره کولای شي د Private key توان تشخیص او وپیژني. او (*Timing Attack (TC* په اصلي *RSA* الګوریتم او همدارنګه په Hamami and Aldariseh کې څېړنه د تطبیق وړ دی چې د Encryption او Decryption وخت په دقیقه توګه اندازه کوي. او د کیلي د تولید لپاره وخت کولای شي چې د پټې کیلي توان یعنې d مشخص کړي.

Small Private key Exponent: دا ثابته شوې چې RSA الګوریتم د پیغام د Decryption لپاره زیات وخت ته اړتیا لري، د ژوندانه په ډېرو اړخونو کې د Encryption پروسه د ځانګړو میکانیزمونو په وسیله ترسره کیږي چې د بیلګې په توګه د سمارټ کارډ یادونه کولای شو په داسې حالاتو کې د m د لومړنۍ پیغام یا Plaintext په لوړ توان پورته کول دوخت او انرژۍ د ضایع کیدو سبب ګرځي. ددې لپاره چې د Decryption او لاسلیک په پروسه لږ وخت مصرف شوی وی نو کولای شو چې د d لپاره کوچني قیمت وټاکو. که څه هم Michael Wiener یو برید توضیح کړ هغې وښودل چې د Decryption توان یعنې d کوچنی قیمت د *RSA* د ټول سیستم سقوط ته اشاره ده. *Wiener* په برید کې د d داسې په لاس راځي چې d د n د دریمې برخې په اندازه د منلو وړ وي او e د n تر اندازې کوچنی وي چې دا په داسې حال کې په سختۍ سره پېښیږي؛ کله چې e او d په تصادفي ډول ټاکل شوي وي. همدارنګه په هغه صورت کې نه پېښیږي کله چې e کوچنی قیمت ولري.

۴. موندنې

لومړني اعداد د عددونو تیوري هغه مهم مفهوم دی چې د معلوماتي تکنالوژۍ او د عددونو تیوري ترمنځ د ارتباطي پول حیثیت لري او د بریښنایي امنیت لپاره خدمات چمتو کوي.په دې مقاله کې په لومړنیو اعدادو او د *RSA* کریپټوګرافي په هغه مواردو بحث ترسره شوی چې د *RSA* کریپټوګرافي د استحکام او قوت لپاره بنسټونه بلل کیږي. دلته اصل دادی چې په کریپټوګرافي کې د لومړنیو اعدادو کارول د هیکرانو په مخنیوي کې اغیزمن رول لري یعنې لومړني عددونه په آسانه توګه په خپل ضربي فکټورونو د تجزیه کېدو وړ نه دي. له دې سره د لومړنیو اعدادو د لومړیتوب د معلومولو لپاره پراخ او منل شوي معیارونه داسې په پام کې نیول شوي چې لومړني عددونه د سلسلې په ډول په نښه کوي. د *RSA* کریپټوګرافي پروسه معمولا له دوه لومړنیو اعدادو پیلیږي او د اوښلر تابع په مرسته د لازمي الجبري عملیاتو په پام کې نیولو سره مخته ځي. په ځینو تګلارو کې کولای شو دا دوه لومړني اعداد درې یا څلور هم ونیسو دلته د لومړنیو اعدادو د ارقامو په زیاتیدو د کریپټوګرافي قوت رامنځته

کېږي، خو محاسبه يې پيچلې کېږي او زيات وخت ته اړتيا لري.سربيره پردې په *RSA* الګوريتم باندې د برید ډولونه د هغوی په اغېزو بحث ترسره شوی چې په ځينو کې په ګروپي شکل يو عنصر تر هغې شمارل کېږي ترڅو بل يې په لاس راشي آما د CMA په برید کې C_1 او C_2 په لاس راوړلو لپاره هڅه کېږي او د ځانګړې کيلي په پام کې نيولو سره د M د لاسته راوړلو هڅه کېږي.همدارنګه د Chosen Cipher text attack، Timing attack او Small Exponent Private key د بريدونو ډولونه او د هغوی اغيزې تر بحث لاندې نيول شوي دي. خو دلته د *RSA* کريپټوګرافي تګلاره داسې ټاکل کېږي چې د ممکنه بريدونو په مقابل کې د امکان ترکچې ځواکمنه پاته شي چې دا چاره د يو لړ قضيو،معيارونو او مثالونو په پايله کې واضح شوې ده.

۵. پایله

په دې مقاله کې د اعدادو تيوري بنسټيز مفاهيم، لومړني اعداد او د RSA کريپټوګرافي تخنيک او تګلاره داسې څېړل شوي چې د RSA کريپټوګرافي تخنيک آسانه کوي. ددې چارې د وضاحت او پرمختګ لپاره د لومړنيو اعدادو پر رول بحث شوی، پايله دا چې لومړني اعداد د خپل جوړښت له مخې د کريپټوګرافی په امنيت کې اغېزمن رول لري، همدارنګه هغه تګلارې او تخنيکونه څېړل شوي چې د *RSA* تخنيک په آسانه کيدو او استحکام کې مرسته کولای شي. د *RSA* کريپټوګرافي امينت د هغو لومړنيو اعدادو په فکټور نيونې پورې اړه لري چې د کيلي په توليدEncryption او، Decryptionپه پروسه کې کارول کېږي. دلته مهمه داده چې د کيلي د توليد الګوريتم پيچلی او وخت يې زيات شي. دا چاره د برید کوونکي د مخنيوي لپاره اغېزمنه تمامېدای شي. ځينې وختونه د امنيت د ډاډ لپاره دوه ځله د Encryption او همدارنګه د Decryption پروسې ترسره کېږي چې دا چاره د برید کوونکي د انحراف سبب ګرځي. له دې سره د هغو ممکنه بريدونو په نوعيت او تخنيکونو بحث شوی چې په *RSA* کريپټورګرافي کې پېښيدونکي دي.

وړاندیزونه

- د اعدادو تيوري او معلوماتي تکنالوژۍ ترمنځ د اړيکو د پراخ وصل لپاره د Symmetric Key Cryptography او Asymmetric Cryptography کې د لومړنيو اعدادو پر تطبيقاتو کار وشي.
- هغه بريدونه چې په RSA کريپټوګرافي کې رامنځته کېږي د هغې د څېړلو او مخنيوي لپاره د لومړنيو اعدادو پر تطبيقاتو کار ترسره شي.

اخخلیکونه

B.Persis Urbana Lvy, Purshotam Mandiwa. Nov(2012). A modified RSA Cryptosysten based on 'n' Prime Numbers . *international Journal of Engineering and Computer Science ISSN:2319-7242*, 1-10.

choi, S.-H. S. (2019). Development of Modofied RSA Algorithm using fixed mersenne Prime numbers for Medical Ultrasound Imaging instrumentation. *Tandfo online* , 50-62

David, M. (2006). Elementary number Theory, 2nd Edition. New York: USB Publishers

desai, T. (2013, 06). Application of Prime Numbers in Copmputer science and the Algorithms used to Test the Primality of Number. pp. 132-145

James S.Kraft, L. C. (2014). An Introduction to Number Theory and Cryptography. International Journal of Mathematics, 204-210.

Kanwar, D. (2017). Advanced Discrete Mathematics. CHANDIGARH, CHANDIGARH, India: Surinder Pahuja for Mohinder Capital Publisher.

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

Mangal, N. S. (2014, November 16). An Improved RSA Cryptographic System. International Journal of Computer Application, 1-5

Maymin, A. (2008). *The Application of Prime Number to RSA Encryption* . Summer I 2008: Boston University

M.Burton. (2014). Elementary Number Thoery,2nd Edition. New York: UBS Publishers.

M.Maurer, U. (1995). Fast generation of Prime numbers and secure Public Key Cryptgraphy Parameters . *Journal of Cryptology* , 123-132

Neil, K. (1994). A Course in Number Theory and Cryptography 2nd Edition. New York: Springer Verlag.

Pawanveer singh, A. S. (Jan2017). Importance of Number Theory in Cryptography. International Journal of Advance Research in Science and Engineering, 05-13.

Paillier, m. J. (2001). Fast Generation of Prime Numbers on Portable Devices . *International Association for Cryptologic Research 20016*, 1-09.

Paual Lavelle Schuler, B. (2012). *Application of Prime Numbers* . Texas : The Uniersity of Texas at Austin

Pooja Singh, Pintusen. (September2017). Enhancing Security of Caesar Cipher Using Divide and Conquer Approach. International Journal of Advance Research in Science and Engineering, 17-25.

Prachi, P. (2013). A Poly-alphabetic Approach to Caesar Cipher Algorithm. International Journal of Computer Science and Information Technologies, 954-959.

Rosen, K. H. (1984). Elementary number theory and its applications. Reading, Massachusetts, Addison-Wesley Publishing Company.

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

Sharma, P. (2015). Analytic Number Theory, Shimla, India: Surinder Pahuja for Mohinder Capital Publisher.

Rao, K. Z. (2018). Large Prime Numbers in Cipher Cryptography. *Regents of Louisiana Grant* , 1-9.