УДК 004

МИХАЛЕВИЧ В. М.
ВАСИЛИНА А. В.

Демонстрація ефективності застосування Китайської теореми про лишки під час операції розшифровування даних в методі RSA

Вінницький національний технічний університет

Анотація

Досліджено тривалість обчислень операції розшифровування в методі RSA без та з використанням китайської теореми про лишки. Наведено приклади застосування цього методу на великих числах. На прикладі даних обсягом 1 Гб, з урахуванням отриманих результатів показано, що застосування Китайської теореми про лишки може зменшити тривалість операції розшифрування від декількох днів до декількох хвилин.

Ключові слова: шифрування, розшифрування, криптографія, метод RSA, Китайська теорема про лишки, Maple.

Abstract

The duration of calculations of the decryption operation in the RSA method without and using the Chinese leftovers theorem is investigated. Examples of the use of this method on large numbers are given. Using the example of 1 GB data, taking into account the results obtained, it is shown that the application of the Chinese leftovers theorem can reduce the duration of the decryption operation from several days to several minutes.

Keywords: encryption, decryption, cryptography, RSA method, Chinese residue theorem, Maple.

Вступ

Протягом історії криптографія використовувалася в різних областях для вирішення багатьох проблем. Діапазон сфер, де криптографія знаходить застосування, розширювався впродовж всієї історії існування нашої цивілізації.

Криптографія є сучасним інструментом, що забезпечує безпеку, конфіденційність, довіру та інші важливі елементи, що мають вирішальне значення для сучасної людини.

Сучасні криптосистеми з кожним днем розвиваються та вдосконалюються, шляхом застосування різних методів, що сприяють підвищенню ефективності їх роботи. Метод RSA став першим методом шифрування за допомогою відкритого ключа. Цей метод й досі є найбільш широко застосовуваним [1-3]. Проте, основною його вадою на сьогодні є повільність цього методу в порівнянні з альтернативними. Для покращення швидкості цього методу на етапі розшифровування даних застосовується Китайська теорема про лишки [5-7].

Метою цією роботи є розробка алгоритму та його програмна реалізація для унаочнення ефективності вказаного застосування Китайської теореми про лишки.

Результати дослідження

RSA (Rivest, Shamir та Adleman) — криптографічний алгоритм з відкритим ключем. Він став першим алгоритмом такого типу, придатним і для шифрування, і для цифрового підпису. Криптосистема RSA використовується у різних продуктах, на різних платформах і у багатьох галузях.

Китайська теорема про лишки (КТЛ) — це один з основних результатів елементарної теорії чисел.

Формулювання КТЛ:

Нехай $b_1, b_2, \dots, b_n$, - довільні цілі числа, а $m_1, m_2, \dots, m_n$ - попарно взаємно прості числа. Тоді така система:

$$\begin{cases} x \equiv b_1 (mod\ m_1) \\ x \equiv b_2 (mod\ m_2) \\ \dots \\ x \equiv b_n (mod\ m_n) \end{cases} \quad (1)$$

має розв'язок і всі її розв'язки рівні за модулем M

де

$$M = m_1 \cdot m_2 \cdot \ldots \cdot m_n.$$

У випадку n=2 розв'язок системи можна записати у вигляді

$$x \equiv \left(m_1 \cdot (m_1)_{m_2}^{-1} \cdot b_2 + m_2 \cdot (m_2)_{m_1}^{-1} \cdot b_1\right)(mod\, M),$$

де

$b_1 \equiv \left(C^v(mod\, m_1)\right)^{v(mod\,(m_1-1))}(mod\, m_1);$

$b_2 \equiv \left(C^v(mod\, m_2)\right)^{v(mod\,(m_2-1))}(mod\, m_2);$

$(m_1)_{m_2}^{-1}$ – число, обернене до m_1 за модулем m_2;

$(m_2)_{m_1}^{-1}$ – число, обернене до m_2 за модулем m_1.

КТЛ застосовується до оптимізації операцій з великими експонентами, що дозволяє зменшити кількість обчислень, тобто скорочує тривалість операції розшифрування і тим самим підвищує ефективність самого методу RSA.

Досвід авторів показує, що система комп'ютерної математики Maple є ефективним засобом для створення методичних матеріалів [8-15], унаочнення покрокового розв'язування типових математичних задач та розробки навчальних Maple-тренажерів [16-19], розробка електронних освітніх ресурсів [20-23], комбіноване використання систем комп'ютерної математики разом з сервісами штучного інтелекту [24-26]. Не менш ефективним є використання системи Maple під час розв'язування широкого кола наукових задач [27-31].

Саме тому нами було обране середовище системи Maple для розв'язування поставленої в цій роботі задачі: дослідити швидкість розшифрування повідомлення за допомогою метода RSA без та із застосуванням китайської теореми про лишки.

Метод RSA:

1) Спершу згенерували два простих числа p=m_1 і q=m_2:

p=98939766841718438302949284375673289857473925757473663212109298378377266523729384746563622274398393449434477677128784378439374637293746582010100129288374656389459607984726153748595082372864452001273646583993239347387777919280183546723747428774834766128374657328282827365595092998373761829383837261622237873266611092011018181717162383933992028478781928929495495848594873763827372663473728829298733651019929288272762633545637281182376464664653525525711109337772822928334479198982828383264457814361402020018177736553255698682986829868298682986829868298682986829868298682986829868298682986829868298682986829868298682986829868298682986829868298682986823739292929292918181818102936366170820031309199906111956250419552503200582338273437273373277777777287364536278174673829098765434567654323434543567876769230910298392389238920293847484722875758238475674832929293838747447739437971714456427291813425687989929288272762633545637281182376464664653525525711109337772822928334479198982828383264457814361402020018177736553255698682986755443325784742579875432563744624542938474656362227439839344943447767712878437843937463729374658201010012928837465638945960798472615374859508237286445200127364658399323934738777791928018354672374742877483476612837465732828282736559509299837376182982481827366437838384478822020018177736551263622873218198018982387636281929839283276447198222833338923

q=789886863732777770298392389238920293847484722875758238475674832929293838747447739437971714456948737638273726634737288292987336510199292882727626335456372811823764646646535255257111093377728229283344791989828283832644578142729181342568798992928827276263354563728118237772873645362781746738290987654345676543234345435678767692309102983923892302938474847228757582384756748329292938389384839810928734657474737882919911010010209933848884848289101030393939998682986755443325784742579868298682986829868298682986829868298682986823739292929292918181818102936366170820031309199906111956250419552503200582338273437273373277777777287364536278174673829098765434567654323434543567876769230917646466465352552571110933777282292833447919898282838326445781436140202001817773655325569868298675544332578474257987543256374462454293847465636222743983934494344776771287843784393746372665237293847465636222743983934494344776771287843784393746372937465820101001292883746563894596079847261537485950823728644520937463476634766347746573282828273655950929983737618293838372616222378732666110920110181817171623839339920284787819289294954958485436140202001663476634545637281182376464664653525525711109337772822928334479198982828383264457814361402

0200181777365512636228732181980189823876362819298392832764471982228333325564287748347661283746573282828273655950929983737618298248182736643783838455309

2) Визначили $n = p \cdot q$

n=781512221290572565004929074897553173039026494079756086326223753005473958692570072312563978585887738622062187007094197567217761437757310458190322340653610753614666623020265638915735250119404060721351419569736217827015118051883625756193319459778632016537567459669699028146032443078971774980753671790542648686414946996532951046896874056343548826586114017721347341927304799183132043891272376133686944708701637727620901715216254777843494469110366503510310504775034081059786274507676751317073261225993911653217995164697184837641596859178724227880707602404513423727249959426558490141062471167999255046581134794545758263469822043549713178013126107856679194629031158628853049860663315971284562852103802972777814149974134314418200370681703454762721606815359623890341375432902451111625639347650937602760102839013442590311381566915115557649657367623531910883872293054892465916422668117457658910561072625275712975286541106807621866948151176075695461875697133036554288025818837145544506986332551382774616473653830769155554146371226732935699628370889279068430849873352061609763157528638606229146734603169159902605839892023130802650672515890285511303871906919886993233553520185416218584359800903263988251311750508419389648116941117057319073327029486816260173535651949845833554603464689653246940681981925769135630817322959286040950575948414802742582701429850389373561720450794675367235452602989839860039018216052615917896111600636814560178581654808718127427045497951920690761043320039797002966380614206138033704060536979847712064025272563979960736861823094623349275589324887608912781224231031739939705132767509971552718329756179921858209942256507556199638051752243687420108452185164332369755275053469425327909390382915290310801904799291849812927654231353093310115819653805238596817902500444954908437300009321609387260721679792071578850937905809697056991673192909219272409658944929254509160175869735674844963061430825981287386010402420443568194767703647456220689579482537081267442060361053082715188341995980770390468557079401819046969107454446229375039408354107988226698331204419216784064584445869159168588624664125543087173054271890078262383307853298549284354353149697415667151545573019308708296965955392755999574092153908674558445171452762414073478619709532116202862098361949407595422698643960074850774763065764588173202415788996683064708135995023849556881354142430143848021850798866249619554192031821450903075175960772809673661184787008461370373346672591923146278413476333871429413354460256642355571376442849743722602716399960565829269517141163348568822243222760502771255741911998644618283596036207497084327979741904005845390442000857097557497713787666904373535179480449579366196014993672702705994414347855891759111528548375686984375118569220 7

3) Обрали відкриту експоненту

$$u = 65537$$

4) Обчислили секретну експоненту

v=208158404181580400304042631359563119895162221045458630131232156376757456443497614817402639885793618343633634990857627183626855725124610698661370932121540951143592483199440880615729656927908163082715265880484541837257974895306171646552490722643633374745255009780647057926318603634382582420068603914974937447091861311495478790219751186772860953612267975240609719710744046485813402477471513767637201990251244154803400527042967230755695858107489779594366238481361596029412838668324845064480077634938274895380827984115141958372701142466451166850567342227645243520192796309718250818657956523926865680350340860484775870838293080125788382675391448170441003119525884691475942419819931391347533899115369710130300804155644728817066781674776317291576794308084251562167921167535059380266676235601183557284897922666869918618116127257431026356598852697504814629733963220260354990876513948736452598421564669527333349048657423446813972404091229833183392320401744881305089518572617318653965148746830293387150848590891708597881397974520253446535128444119249514297708399670927681462771836060782616475966236369087008253162963748047229672858681925947539333817355191625301034299864936701794583343526322037569295434608188885192573622981279877818053069207115398395373441542036353645582329952234960206884607850168549461091773306522686377631463963189172477753385662442107464560376461984403510991808485369993303201633515536158844524026215317726633063849905868564241524482579342278805257029844929502579 1

4194108589277360404439825036779920385410644246229514848415250645892421527846252999253821867254050617299274982099597532567844907987536250714247000411865700636236705645456862322401135382614420662290464990936203721968283506165846616420823102883093784495255433309367681659633368208423858983902237603797795744292085196357277210075243264686450047733356425160864353835556537754488210869165129002759104378615614745217484471972786043151876580837588169539721742014821202677366481247980179556761965706858105693664472384069817472502461038743628779978292483837636204040937099668054744430371634879125869479595775190376519913638611413867892992508203356700963321657138908123246384533851450847536201606755476657896078331444897403640146251424782007004194389986246650429095099267797943225827125163524300320093346893350711728412331300324296369426440071357238231279080099418089533100428230348574520644676283070035966612230766459200416739047392972410175474233617310756651155836781689550347760620237638502856222264583245706829148213531471324498833258185359446074868214841935955486022542870750325620737411677472218800257767625108838771383736547715627166911557712314531617916186873587021072579880018148029340708560939891871389121322485834097644397883527798748082519316790856249615)

5) Опублікували відкритий ключ

u = 65537; n.

6) Зберігаємо в секреті секретний ключ v.

7) Обираємо текст для шифрування (довжина, нижче вказаного тексту, рівна 2701 символу)

m=432111069327034363307369747425614356355845871897674675383053803206222085722974121768604305613921745580037409259811952655310075487163797179490457039169594160088430571674960498834085812920457916453747019461644031395307920624947349951053530086146486307198155590763466429392673709525428510973272600608981219760099374675982933766845473509473676470788342281338779191792495900393751209539300628363443011313746086538005862664913074813656220643842443844131905754565672075358391135537108795991638155474452610874309742867231360502542308382199053675592825240788613991898567277116881793749340807728335795394301261629479870548736450984003401594705923178314906195914825136973281314862289454100745237769034410057080703111299605127114594552921209928891515242515620324828055912854227507525717981351447473570262981491527797413449568788992987500442157627511097882499376798339062890227065912603127119521589474574157513825150650905007553408748182082815984929359632269852681585809504709739738485231104248045693804710098188302655538010818866476054310788175542136407374106205605523687223946800025812242019121022573901665288968349097396414947780422731613987785640265674198272844134050365811754869582636140810856859347877704841433599229456898724880795485531802023255050614524952922474293642065329619154912668026856069438450681407641506962917791070874166946435905950292905549552888716084125842236067060541266621757734462223575905687273574099511410424381304659501247275887974857856234450269247606386273485070460241146322057229320612320193122698146898380788553867838568046682595985479921284810557140299651198106710223609305579059712272244885805483826208735338387863489794196134912196910897216131848825391035580908168898203852497310816425237383431947635435699351252190359871651634727025199361890194640455210548527110526558995883321331291488160256835061600677790317018326352763557737161973361521410145117835798495990372909367548324437166624532717042911333128098958777221437607297225555515035135066117032387230140041261632419464837902953662742185431052718860357364253378245826804185157478108114115222166109457168704413863620712302109852829506233631164040613602795565800564274523660249107288396054758186579329287449756784117455124422567276167745427311322693517877134632551690893087076757744996285622033187255241397468914452589093299562414832644270546876729112628260582194035065789638419316941663241940100060552583892017380342336889130773122708067638635548911905029265582934003271419871730357073102169468185294819331087273443411310785598722235833720520836681919512091018322292582289845447694366516647943197660018541267866007697159742120516996987132975876894061013393503102244327489140959856471291506898005561942369165356644636007530136

8) Обчислюємо шифротекст

C=421564311719291456604482882505908009179706741904070465384663459517991619644583540586064495798804417179279405300014915699537908997672883664544926510259537587172353006922801623333841647236511255624055323833482922062274723478774542195030496083591165391821007324732

836177130666891135162822398862402030292066146803369375255546738676093780488539333355135
787992006698607014437980794632733778966507833384016363311078445724602907762018362976556
716298094609635043073411096630286207614013603649574011114936701757828935537983121501430
456672785722787590925688092472296877493221764619294441723684944841801926779711757012472
231748071579993280407477006759495362620511583088043043817225612540899809936356044232124
606924184935327364390875047938404437579114396863450573504444286769209723023375397216397
080318783794196711784584868073457406381283632744183205951045256991077898449107322841243
197544307143857716566499031926804175971458610443191823792725224108308760653630402220179
985763586643066271122001631140032152195041241982726114583439081135114510984758335116146
291071401759239962061593589840774351995771351822748365415128305612338828548052094800970
505699387137883170561110986837264575062695090085315472584673271196518332601779226951390
249398485012388655502345035238433710128173868643231667106189008915751427652244785897338
063800009707812659760999871771130938331763359517852937084611029574145978997449894076256
938752875692664691150073304997516117312744738161570026929982273705292489146330797212879
508699474107520754776739509473738373222038168224029386727990960433067926626338315801923
984676978073157864211061782707054637591053774259938007571030729560534721941558432762672
141309088179930575246829457668266943008871083272243239228538304072853943407566469442579
582018713382223517302058362104855416837079624541993486243221932972870812614022925133654
269528453613780758467740250714769769999129312795131591787288856856623588875005524360419
262902879716332402697440117804187882317646824034706454045720583616953229457771098499376
812223041524638494177775253777506237299527228116674014716609947609685100974691647479174
658731242552535387414775350179659714049789294696130467830133228773130121108104284269328
682685696353412676055905251034530218801395157039999521508557398395885258201366265142542
424299477984417925480720325577662945831074012473923870127742984762087385114672682080035
530786764456778186494372145772463250483771187651874992376158040426412301318950760024952
695928622936234960327798449844131374106261345281847828885619906091362276129223790064194
209441752982200579499502746725263430139008357298456877253030665680636003768427049124789
388236444587333398714980073174865750680741328847613578701680432420504190611780464865941
180737525588889579358765862645 85

00981883026555380108188664760543107881755421364073741062056055236828
72239468000258122420191210225739016652889683490973964149477804227328
16139877856402656741982728441340503658117548695826361408108568593424
78777048414335992294568987248807954855318020232550506145249529224727
42936420653296191549126680268560694384506814076415069629177910708727
41669464359059502929055495528887160841258422360670605412666217577328
44622235759056872735740995114104243813046595012472758879748578562328
44502692476063862734850704602411463220572293206123201931226981468929
83807885538678385680466825959854799212848105571402996511981067102228
36093055790597122722448858054838262087353383878634897941961349121929
69108972161318488253910355809081688982038524973108164252373834319424
76354356993512521903598716516347270251993618901946404552105485271112
05265589958833213312914881602568350616006777903170183263527635577328
71619733615214101451178357984959903729093675483244371666245327170424
29113331280989587772214376072972255555150351350661170323872301400424
12616324194648379029536627421854310527188603573642533782458268041828
51574781081141152221661094571687044138636207123021098528295062336328
11640406136027955658005642745236602491072883960547581865793292874424
97567841174551244225672761677454273113226935178771346325516908930828
70767577449962856220331872552413974689144525890932995624148326442728
05468767291126282605821940350657896384193169416632419401000605525828
38920173803423368891307731227080676386355489119050292655829340032728
14198717303570731021694681852948193310872734434113107855987222358328
37205208366819195120910183222925822898454476943665166479431976600128
85412678660076971597421205169969871329758768940610133935031022443228
74891409598564712915068980055619423691653566446360075301366

m_q =724920241704523377168716871018237780337220745983514922992574036133798498748768764407094142793530185644815703583040845404570785150680105906638473149755074547704011448982123341503943270724091451236144106866215415677407883064060293018703610750551524367300172894229462609539504091400099512853285546631439981286068866336086499578129523858913393659565507447485307976918275598488484728773410469472415248194420679717273304505159598977945172105236441556056503205898218960451087597743657286555960847926384804684063852973448592170513704376837280131888812440304911161989379732719747263185513092508222813666797233287493224546889500096909530578424066512837063623307129159904715317769304179521727082297322946020926831910319245308468272714881617249925153533815590141599443408221484196103611434161092475477299657032817530785635003919173760927410999987643407438743260692687777030216730308887263043327063068683278112170716929160817311313991452889688656655729589427811287001840076790702252441629773743103040346956744779902092291936104310266070896654352161530487911808291027973620152240913760554608933284366947989431016891242478831553432606312711266278118821428596892024332510119419404296839114730209133948522780449174702401088818867026830570209523364695344749588198354237631920764938331246203105066676363322855579699548860832666878042610704709610204079785327212235562308288474021680 4

Тепер знайдемо p_q^{-1} і q_p^{-1}

p_q^{-1} =583559493922627085972016478742187248177525533449367486448910400915687699428286008547543953346631651952820840111045268770089206848977249473226495738161406143170593633227948029716217857917504191294908656215460380490095489733830507673162193755263910618863791710819026125162056647860124713704863342893013160918516900678083332077023642562955794626747499419779485689565675088476247737324692673980443816480831803421742539573203537136241828523714342319929334061898724946061133066461902924649463916109114309652393212339761165427395937878951055831348040013142907023655429159734642642198236265628412323776200188065889871230051643695086150807860087492899125268765912877236647229955621234653960305417080088528532886009473837247223646612298869428732809493642021726303774818957192907427030822824930830854528492746416313586441254207527833484063622043191441711416812820337215154983387454537675715459467676787281059615946930716982980059838838342154886912233763789770749233220522508401303038898345536323829785945681685451161903810593267536814326063360076898006661609958535538191855130285410017021058875830547625184104181130505774520256759542843963159459503629569625647758307788392272310378439230375477969577096287805557081144438779271714024704246072878402574871674868453558963915120790277627635475517246418159350856438459096792315988908575904492664466759605171281088928979437590154591 5

q_p^{-1}=258441845274027309839893295302103648459846608877449753533357298156186413907167137422477663655047708903180589521376946286080175645865463705642778340511546178892565970055686544335134797099081990662216960751095876191617902006981411232278380422060242520349623972579398283337961901349966414880696114817461956162513370039149635659360426671444053432795703640819365566374068224893860670709299265535047425344558105817921610452630028723479417191949724991961656961282834663079762189810749391855608026326926614605436509909790668677468052675401321794414161494081198926584196483596390780499648809893578333084153357482745754933096744021377320207797006683390553564543508604448703132499230114135755526082216890218085445517386045523275851414370321486315081880441781075445301234041456455188563855004554630955793207190797717501051192972365981736577798427903613786254848371638971209327546866465101865568355715249394186320810582628652258378198996893026379071439760631709384811477720688905057180494388377796733775829010394018872943589120371581453197691075100304277018870798130477156019757881274253973121008097716992157087202198008958279310850700039127069272536710835768671013704003277159718644534816839593664751933976953659861641079370476648227362184628127384051519532649371300676872427014359014599884846648634548760823892687705845834217672247118476865981712103090199856312614554843053 9

```
> st:=time():
(p*a*(m['q'])+(q*f*(m['p']))) mod n;
time()-st;
```

де $a = p_q^{-1}$, $f = q_p^{-1}$

43211106932703436330736974742561435635584587189767467538305380320622212
208572297412176860430561392174558003740925981195265531007548716379
71794904570391695941600884305716749604988340858129204579164537470114
94616440313953079206249473499510535300861464863071981555907634664212
93926737095254285109732726006089812197600993746759829337668454735010
94736764707883422813387791917924959003937512095393006283634430113114
37460865380058626649130748136562206438424438441319057545656720753515
83911355371087959916381554744526108743097428672313605025423083821919
90536755928252407886139918985672771168817937493408077283357953943010
12616294798705487364509840034015947059231783149061959148251369732818
13148622894541007452377690344100570807031112996051271145945529212010
99288915152425156203248280559128542275075257179813514474735702629818
14915277974134495687889929875004421576275110978824993767983390628919
02270659126031271195215894745741575138251506509050075534087481820818
28159849293596322698526815858095047097397384852311042480456938047114
00981883026555380108188664760543107881755421364073741062056055236818
72239468000258122420191210225739016652889683490973964149477804227313
16139877856402656741982728441340503658117548695826361408108568593414
78777048414335992294568987248807954855318020232550506145249529224717
42936420653296191549126680268560694384506814076415069629177910708717
41669464359059502929055495528887160841258422360670605412666217577313
44622235759056872735740995114104243813046595012472758879748578562313
44502692476063862734850704602411463220572293206123201931226981468919
83807885538678385680466825959854799212848105571402965119810671022212
36093055790597122722448858054838262087353383878634897941961349121919
69108972161318488253910355809081688982038524973108164252373834319414
76354356993512521903598716516347270251993618901946404552105485271114
05265589958833213312914881602568350616006777903170183263527635577313
71619733615214101451178357984959903729093675483244371666245327170414
29113331280989587772214376072972255555150351350661170323872301400414
12616324194648379029536627421854310527188603573642533782458268041818
51574781081141152221661094571687044138636207123021098528295062336313
11640406136027955658005642745236602491072883960547581865793292874414
97567841174551244225672761677454273113226935178771346325516908930818
70767577449962856220331872552413974689144525890932995624148326442717
05468767291126282605821940350657896384193169416632419401000605525818
38920173803423368891307731227080676386355489119050292655829340032717
14198717303570731021694681852948193310872734434113107855987222358313
37205208366819195120910183222925822898454476943665166479431976600114
85412678660076971597421205169969871329758768940610133935031022443212
74891409598564712915068980055619423691653566446360075301366

Вхідне повідомлення, вказане в пункті 7, займає 2701 байт і при розшифруванні даних такого розміру, можна зекономити приблизно 1,1 секунди часу, за умови використання КТЛ. Порівняємо вхідне повідомлення з художнім фільмом низької якості, що займає близько 1 Гб пам'яті (1 073 741 824 байти):

$\frac{1\,073\,741\,824}{2\,701} \approx 397534 -$ кількість блоків інформації, розміром 2701 байт, що міститься в 1 Гб інформації.

$397534 \cdot 1{,}1 = 437\,287{,}4 -$ кількість секунд, зекономлених під час процесу розшифрування (з використанням КТЛ) даних, розміром 1 Гб,.

$$437\,287{,}4 \text{ секунд} \approx 5 \text{ діб.}$$

Звичайно, наведені результати не відображують істину картину, оскільки розрахунки здійснювалися з використанням системи комп'ютерної математики. Використання середовища однієї з професійних мов програмування із залученням відповідних алгоритмів та прийомів пришвидшення виконання арифметичних операцій з великими числами безумовно суттєво зменшує тривалість обчислень з розшифровування зашифрованих повідомлень, отже і сам ефект застосування Китайської теореми про лишки буде вимірюватися значно меншими числами в абсолютному вимірі. Але нашою задачею було унаочнити застосування вказаної теореми та проаналізувати отримані результати.

Висновки

Отже, дослідження порівняння швидкості методу RSA та методу RSA з використанням китайської теореми про лишки (КТЛ) вказує на значне покращення продуктивності при використанні КТЛ. Застосування китайської теореми про лишки дозволяє оптимізувати операції з великими експонентами, що сприяє зменшенню часу виконання розшифрування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Методичні вказівки до виконання курсового проекту з дисципліни "Прикладна криптологія" / Укладачі: В. А. Лужецький, Ю. В. Баришев, А. В. Остапенко-Боженова. - Вінниця: ВНТУ, 2018. – 40 с.
2. Приймак А. В. Підвищення стійкості криптоалгоритму RSA за рахунок генетичної оптимізації вихідного повідомлення [Текст] / А. В. Приймак, Ю. Є. Яремчук // Реєстрація, зберігання і обробка даних. – 2018. – Т. 20, № 4. – С. 76-84.
3. Майданюк В. П. Кодування та захист інформації. Навчальний посібник. - Вінниця: ВНТУ, 2009. - 164 с. Режим доступу: https://pz.vntu.edu.ua/media/uploads/metod/kz/k_z_NP.pdf.
4. Методи підвищення ефективності криптографічних систем, які грунтуються на задачах факторизації [Електронний ресурс]. КПІ ім. Ігоря Сікорського. – 2022. – Режим доступу: https://ela.kpi.ua/bitstream/123456789/49778/1/Kyslyi_bakalavr.pdf . (дата звернення: 04.12.2023).
5. Quisquater J. J., Couvreur C. Fast decipherment algorithm for RSA public-key cryptosystem //Electronics letters. – 1982. – Vol. 18. – №. 21. – P. 905-907.
6. J. Grossschadl, "The Chinese Remainder Theorem and its application in a high-speed RSA crypto chip,"Proceedings 16th Annual Computer Security Applications Conference (ACSAC'00), 2000, pp. 384-393.
7. G.N. Shinde, H.S. Fadewar Faster RSA Algorithm for Decryption Using Chinese Remainder Theorem. Режим доступу: http://www.techscience.com/doi/10.3970/icces.2008.005.255.pdf (дата звернення: 12.12.2023).
8. Михалевич В. М. Ключові проблеми створення навчально-контролюючого комплексу з дисциплін математичного спрямування / В. М. Михалевич // Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми : [зб. наук. праць]. — Вип. 10 / редкол. : І. А. Зязюн (голова) та ін. — К.-Вінниця : ДОВ «Вінниця», 2006. — С. 391–397.
9. Михалевич В.М., Крупський Я.В., Шевчук О.І. Математичні моделі генерування завдань з інтегрування частинами невизначених інтегралів/ В.М. Михалевич, Я.В. Крупський, О.І. Шевчук // Вісник Вінницького політехнічного інституту. – 2008. - № 1. – С. 116-122.
10. Михалевич В. М. Комп`ютерна програма «Maple програма генерування індивідуальних завдань з теми «Порівняння першого степеня» / В. М. Михалевич, О. І. Тютюнник, А. А. Коломієць, Д. О. Пінчук, А. В. Фещук, Ю. В. Добранюк // Свідоцтво про реєстрацію авторського права на твір № 120820, Дата реєстрації авторського права 26.07.2023 бюлетень № 77 від 29.09.2023.
11. Михалевич В. М. Комп`ютерна програма «Maple програма генерування індивідуальних завдань з теми «Шифрувальні матриці» / В. М. Михалевич, О. І. Тютюнник, А. А. Коломієць, Д. О. Пінчук, А. Р. Магденко, Ю. В. Добранюк // Свідоцтво про реєстрацію авторського права на твір № 120822, Дата реєстрації авторського права 26.07.2023 бюлетень № 77 від 29.09.2023.
12. Михалевич В.М. Excel-VBA-Maple програма генерації задач з дисциплін математичного спрямування//Інформаційні технології та комп'ютерна інженерія. – 2005. - № 2. – С.74 83.
13. Михалевич В.М. Реалізації технології "живих сторінок" в Maple, MathCad, Excel / В.М. Михалевич // Вісник ВПІ. – 2004. - № 3. – С. 90-95.
14. Михалевич В. М. Математичні системи комп'ютерної алгебри як засіб підвищення ефективності і якості освітнього процесу з вищої математики / В. М. Михалевич, О. І. Шевчук, Н. Л. Буга // Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців : методологія, теорія, досвід, проблеми : зб. наук. прац. — Випуск 14 / редкол.: І. А. Зязюн (голова) та ін. — Київ-Вінниця : ДОВ «Вінниця», 2007, — С. 357–360.

15. Михалевич В. М. Навчально-контролюючий Maple — комплекс з вищої математики / В. М. Михалевич // Інформаційні технології та комп'ютерна інженерія. — 2004. — № 1. — С. 74–78.
16. Михалевич В. М. Розвиток системи Maple у навчанні вищої математики майбутніх інженерів-механіків : монографія / В. М. Михалевич, Я. В. Крупський. — Вінниця: ВНТУ, 2013. — 236 с. ISBN. — 978-966-641-539-7.
17. Михалевич В. М. Використання систем комп'ютерної математики у процесі навчання лінійного програмування студентів ВНЗ: монографія / В. М. Михалевич, О. І. Тютюнник. – Вінниця: ВНТУ, 2016. – 279 с. ISBN 978-966-641-670-7.
18. Михалевич В. М. Розвиток системи Maple у навчанні вищої математики [Електронний ресурс] / В. М. Михалевич, Я. В. Крупський // Інформаційні технології і засоби навчання. — 2011. — Т. 21 — № 1. — Режим доступу до журн. : http://journal.iitta.gov.ua.
19. Тютюнник О. І. Реалізація принципу наочності за допомогою засобів СКМ у процесі навчання лінійного програмування / О. І. Тютюнник, В. М. Михалевич // Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми // Зб. наук. пр. – Випуск 36 / Редкол.: І.А. Зязюн (голова) та ін. – Київ-Вінниця : ТОВ фірма "Планер", 2013, – С.434-440.
20. Михалевич В. М. Розробка електронних освітніх ресурсів в середовищі СКМ Maple [Текст] / В. М. Михалевич, Я. В. Крупський, Ю. В. Добранюк // Математика та інформатика у вищій школі: виклики сучасності : зб. наук. праць за матеріалами Всеукр. наук.-практ. конф., 18-19 травня 2017 р. / М-во освіти і науки України, Вінницький державний педагогічний університет імені Михайла Коцюбинського [та ін.]. - Вінниця : ФОП Рогальська І. О., 2017. - С. 69-72. Режим доступу: https://conferences.vntu.edu.ua/index.php/pmovc/index/pages/view/zbirn2018 Дата звернення: Черв. 2018
21. Михалевич В. М. Фрагменти електронних освітніх ресурсів з функції двох змінних в середовищі СКМ Maple [Текст] / В. М. Михалевич, Ю. В. Добранюк, Я. В. Крупський //http://ir.lib.vntu.edu.ua//handle/123456789/15474
22. Михалевич В. М. Курс математики для слухачів-іноземців в середовищі СКМ Maple. Алгебраїчні рівняння і системи рівнянь: Електронний освітній ресурс / В. М. Михалевич, Н. Б. Дубова, І. А. Клеопа – Вінниця : ВНТУ, 2019. – 64 с.
23. Михалевич В. М. Електронний освітній ресурс з курсу математики для слухачів-іноземців в середовищі СКМ Maple [Текст] / В. М. Михалевич, Н. Б. Дубова, І. А. Клєопа // Збірник наукових праць за матеріалами дистанційної всеукраїнської наукової конференції «Математика у технічному університеті XXI сторіччя», м. Краматорськ, 15–16 травня 2019 р. – Краматорськ : ДДМА, 2019. – С. 193-195.
24. Михалевич В. М. Використання штучного інтелекту у вивченні математики/ Михалевич В. М., Немировська Д. О. //LII Науково-технічна конференція підрозділів ВНТУ (2023) : Вінниця, ВНТУ, наук.-практ. конф., 21-23 червня 2023 р. Режим доступу : https://press.vntu.edu.ua/index.php/vntu/catalog/view/788/1373/2632-1
25. Mykhalevych V., Turzhanska I., Nemyrovska D. Joint use of ChatGPT, Maple and Maxima in teaching mathematics and computer science. Збірник тез : IV Міжнародної науково-практичної інтернет-конференції, «Математика та інформатика в науці й освіті, виклики сучасності», 25-26 травня 2023 р. Вінниця. 2023. С. 198-201. Режим доступу https://press.vntu.edu.ua/index.php/vntu/catalog/view/791/1378/2645-1.
26. Introducing ChatGPTL: https://openai.com/blog/chatgpt.
27. Volodymyr O. Kraievskyi, Volodymyr O. Kraievskyi, Volodymyr M. Mykhalevych, Volodymyr M. Mykhalevych, Daniel Sawicki, Daniel Sawicki, Olga Ostapenko, Olga Ostapenko, "Modeling of the materials superplasticity based on damage summation theory ", Proc. SPIE 10808, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2018, 108084S (1 October 2018); doi: 10.1117/12.2501489; https://doi.org/10.1117/12.2501489
28. Mikhalevich V. M. Maximum Accumulated Strain for Linear Two-Link Triangle-Like Deformation Trajectories / Volodymyr Markusovych Mikhalevich, Igor Vasilyevich Abramchuk // International Applied Mechanics. – 2021. – No. 57(6). – P. 720–736, https://doi.org/10.1007/s10778-022-01121-w.
29. Volodymyr Mykhalevych, Yurii Dobraniuk, Victor Matviichuk, Volodymyr Kraievskyi, Oksana Tiutiunnyk, Saule Smailova, Ainur Kozbakova. A comparative study of various models of equivalent plastic strain to fracture. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. 2023. № 1. P. 54-70. DOI: http://doi.org/10.35784/iapgos.3496
30. Andrii V. Titov, Andrii V. Titov, Volodymyr M. Mykhalevych, Volodymyr M. Mykhalevych, Peter Popiel, Peter Popiel, Kanat Mussabekov, Kanat Mussabekov, "Statement and solution of new problems of deformability theory", Proc. SPIE 10808, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2018, 108085E (1 October 2018); doi: 10.1117/12.2501635; https://doi.org/10.1117/12.2501635
31. Mikhalevich V. M. Variational problems for damage accumulation models heritable type [Text] / V. M. Mikhalevich, V. O. Kraevskiy // The nonlinear analysis and application 2009 : materials of the international scientific conference, Kyiv, April 02-04th 2009. - Kyiv : NTUU "KPI", 2009. - P. 109-110.

Василина Анастасія Василівна – студентка групи 2БС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: nstvsln@gmail.com.

Науковий керівник: ***Михалевич Володимир Маркусович*** — д-р техн. наук, професор, завідувач кафедри вищої математики, Вінницький національний технічний університет, м. Вінниця, e-mail: mykhalevych@vntu.edu.ua.

Vasylyna Anastasia Vasylivna- is a student of group 2BS-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Supervisor: ***Mykhalevych Volodymyr M***. — Dr. Sc. (Eng.), Professor, Head of the Chair for Higher Mathematics, Vinnytsia National Technical University, Vinnytsia, mykhalevych@vntu.edu.ua.