ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

3. Контент, Созданный Потребителем / / Цифровой Маркетинг. - Хобокен, Нью-Джерси, США: John Wiley & Sons, Inc., 2015-10-23 — - С. 221-249.

4. Дженнифер Роули. Понимание маркетинга цифрового контента / / журнал управления маркетингом — - 2008-07-07 — - Т. 24, вып. 5-6. — С. 517-540.

5. Руководство по поисковая оптимизация – инструменты для веб-мастеров. support.google.com. https://support.google.com/webmasters/answer/7451184

6. Кристоф Майнель, Харальд СЭК. Все о / / WWW. - Берлин, Гейдельберг: Springer Berlin Heidelberg, 2004 — - с. 1-52.

7. Введение в поисковую оптимизацию.

https://cdn1.hubspot.net/hub/53/Introduction-to-SEO-eBook.pdf

9. SEO и рынок поисковых систем в России, 8 мая 2012 г.-Владимир Карев. Доступно по адресу: http://www.ginzametrics.com/blog/seo-and-the-search-engine-market-in-russia

10. Бела и Уайльд " академическая поисковая оптимизация (ASEO): оптимизация научной литературы для Google Scholar and Co."

ӘОЖ 004.056

КРИПТОГРАФИЯЛЫҚ КІЛТТЕРДІ ҮЛЕСТІРУ ПРОТОКОЛЫН САЛЫСТЫРМАЛЫ ЗЕРТТЕУ

Күзембай Шолпанай Бақытбекқызы
kuzembaysh@gmail.com
Л. Н. Гумилев атындағы ЕҰУ, Ақпараттық технологиялар факультеті, Ақпараттық қауіпсіздік кафедрасының магистранты, Астана, Қазақстан
Кургумбаев Адлет Муратканович
adlet.kurgumbaev@gmail.com
Л. Н. Гумилев атындағы ЕҰУ, Ақпараттық технологиялар факультеті, Ақпараттық қауіпсіздік кафедрасының студенті, Астана, Қазақстан
Ғылыми жетекші – Д.Ж.Сатыбалдина

Ақпараттық-телекоммуникациялық жүйелердегі ақпараттық қауіпсіздікті қамтамасыз етудің ең тиімді бағдарламалық құралдарының бірі ақпаратты қорғаудың криптографиялық құралдары мен әдістері болып табылады. Криптографиялық әдістердің негізінде ақпаратты криптографиялық түрлендіру ұғымы жатыр. Криптографияның негізгі міндеттері-құпиялылықты қамтамасыз ету (ақпаратты сыртқы қарсыластан қорғау), тұтастықты қамтамасыз ету (ақпараттың сенімді көзден және өзгеріссіз жеткізілуін қамтамасыз ету кепілдігі), хабарламалардың ««бақылауда болуын» қамтамасыз ету (ақпаратты жіберуші мен алушының құпиялылығына кепілдік).

Криптографиялық жүйелер қаншалықты күрделі және сенімді болса да, олардың практикалық іске асырудағы әлсіз тұсы - кілттерді үлестіру мәселесі. Екі пайдаланушы арасында құпия ақпарат алмасуға мүмкіндік беру үшін кілтті олардың біреуі жасауы керек, содан кейін қандай да бір жолмен екіншісіне құпия түрде берілуі керек.

Симметриялы криптографиялық жүйелерде кілттерді тарату схемалары бар, мұнда міндетті компонент құпия кілт берілетін қорғалған байланыс арнасының болуы болып табылады. Алайда, ең тиімдісі – құпия кілтті ашық байланыс арналары арқылы жіберуге мүмкіндік беретін екі кілтті криптография әдістері (ашық кілт жүйелері).

Криптожүйедегі кілттерді үлестіру мәселесі ең маңызды және қымбат процедуралардың бірі болып табылады, өйткені құпиялылық пен шынайылықтың негізгі талабы әрбір ақпарат алмасу сеансынан кейін кілттерді ауыстыру болып табылады. Егер ұзақ мерзімді құпия кілтті бұзу белгілі бір уақытта осы кілт арқылы жүзеге асырылатын құпиялылықты бұзбаса, онда криптожүйе прогрессивті құпиялылыққа ие болып саналады.

Кілттерді үлестіру протоколдары қазіргі криптографияда өте маңызды рөл атқарады, өйткені олар пайдаланушыларға тиімдірек симметриялық криптографияны (AES (ағылш.

Advanced Encryption Standard, қаз. Кеңейтілген шифрлау стандарты) сияқты алгоритмдер) пайдалануға мүмкіндік береді, өйткені қарапайым асимметриялық алгоритмдер (мысалы, RSA) үлкен хабарламалар үшін тиімділікті қамтамасыз етпейді [2]. Олар баптау рөлін атқаратындықтан, оларды бұзу кейіннен жіберілетін әрбір хабарламаның бұзылуын білдіруі мүмкін.

Пайдаланудың қарапайымдылығына және симметриялық кілттердің аз өлшеміне байланысты (AES үшін максимум 256-бит) орнату процесінде әдетте асимметриялық криптография қолданылады. Қазіргі уақытта 2048-биттік RSA пайдаланушыларға заңды веб-сайттарды анықтауға көмектесетін PKI-де сертификаттарға қол қою үшін қолданылатын ең көп таралған алгоритм болып табылады [3].

PKI (Public Keys Infrastructure, ашық кілттік инфрақұрылым) кілттерді ортақ пайдалану және аутентификация мәселесін шешеді. PKI енгізудің көптеген жолдары бар, олардың негізгі құрамдас бөліктері ретінде ашық кілт сертификаты, сертификаттау орталығы және тіркеу орталығы ұғымдарын пайдаланады [4].

Сертификаттау орталығы – бұл барлық әртүрлі нысандар үшін ашық кілт сертификатын (цифрлық сертификат) шығару арқылы хабар алмасуға қатысатын нысандарды аутентификациялау үшін пайдаланылатын сенімді үшінші тарап. Бұл сертификатта әдетте аталған нысанның ашық кілті, жұптастырылған жабық кілттің иесі туралы қосымша ақпарат, сертификаттың жарамдылық мерзімін көрсететін уақыт терезесі және куәлік беруші орталықтың жеке ЭЦҚ болады. Әрбір пайдаланушы онымен сенімді қарым-қатынас орнатуы керек, себебі әрбір жарамды сертификат сертификаттау орталығының жеке кілтімен қол қойылады. Тіркеу орталығының рөлі жаңа пайдаланушыларды қадағалау және сертификаттау орталығы үшін олардың жеке басын тексеру болып табылады. Жоғарыда сипатталған СО сертификатын пайдалану арқылы пайдаланушының дұрыс тараппен байланысып тұрғанына көз жеткізуге болады.

Кілттерді үлестіру мәселесі Диффи-Хеллманның жұмысында қарастырылды, онда ашық кілтті шифрлау схемасы жасалған [5]. Оның беріктігі соңғы абелев тобының (А) дискретті логарифмдеудің шешілмейтін мәселесіне негізделген. Ашық кілтті криптожүйелердің негізінде жатқан алгоритмдердің келесі кемшіліктері бар:

- кілттерді құру үлкен жай сандарды құруға негізделген;
- шифрлау және дешифрлау процедуралары көп таңбалы сандарды модуль дәрежесіне шығарумен байланысты.

Диффи-Хеллман протоколы – сеанс кілті арқылы жалпыға ортақ арна арқылы әртүрлі пайдаланушылар бір-біріне ақпаратты жіберетін схема.

Негізгі протокол келесідей [5]:

1) Орнату кезеңі:

Екі пайдаланушы да g және p екі жай сандарын таңдайды, мұнда p - үлкен сан және g – p-ның жай түбір модулі. Бұл нөмірлер басқа пайдаланушылардан құпия болуы керек. А мен Б құпия кілттер ретінде үлкен бүтін **a** және **b** сандарын таңдайды (А үшін a және Б үшін b), яғни әр қайсысы өзінің жеке кілтін ғана біледі. Мұндағы, А және Б – пайдаланушылар.

Ескерту: p кемінде 512 бит, **a** және $\mathbf{b} \leq p - 2$

2) А → В:

Пайдаланушы А $\boldsymbol{A = g^a \ (\mathrm{mod}\ p)}$ деп есептейді, содан кейін ол Б-ға жібереді.

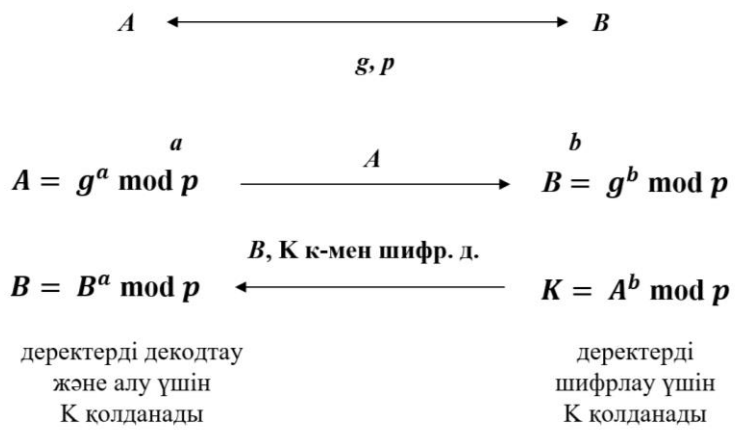
3) В → А:

Пайдаланушы В $\boldsymbol{B = g^b \ (\mathrm{mod}\ p)}$ есептейді және оны А-ға жібереді.

4) Нәтижесінде, пайдаланушы А $\boldsymbol{B^a \ (\mathrm{mod}\ p) = (g^b)^a \ (\mathrm{mod}\ p) = g^{ab} \ (\mathrm{mod}\ p)}$ есептейді.

5) Дәл солай Б-да $\boldsymbol{A^b \ (\mathrm{mod}\ p) = (g^a)^b \ (\mathrm{mod}\ p) = g^{ab} \ (\mathrm{mod}\ p)}$ есептейді.

Нәтижесінде екі нәтиже тең және ортақ кілтті білдіретінін атап өтуге болады. Енді ортақ құпия кілтті симметриялы криптожүйеге негізделген шифрланған деректерді үлестіру үшін пайдаланылуға болады.



Сурет 1. Диффи-Хеллман протоколының жалпы схемасы

Python тіліндегі код арқылы криптографиялық қауіпсіз кездейсоқ жай сандарды қолдана отырып, екі пайдаланушы арасында ортақ құпия кілт құру үшін Диффи-Хеллман протоколын жүзеге асырдық.

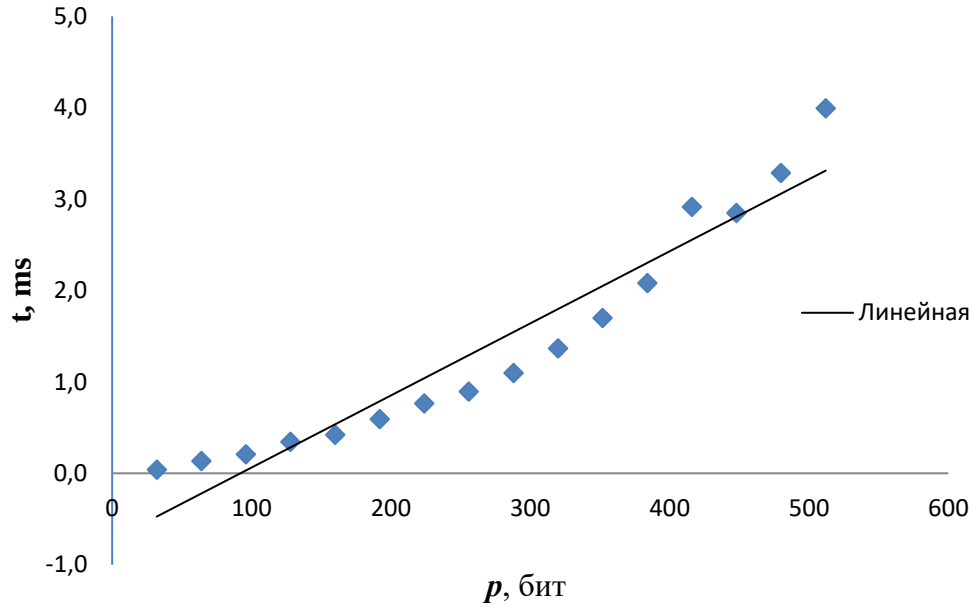
Нақтырақ айтсақ, код берілген ұзындықтың кездейсоқ жай санын биттерде жасайды (generate_prime_number функциясы), кездейсоқ G генераторын таңдайды (p модулінің дәрежесіне көтерілгенде p-ге бөлінудің барлық мүмкін қалдықтарын беретін сан) және екі кездейсоқ құпия a және b сандары. Содан кейін пайдаланушылардың әрқайсысы өздерінің жалпыға ортақ кілтін есептейді (generate_key функциясы), содан кейін олар өзара алмасады. Алынған ортақ кілттерді қолдана отырып, пайдаланушылардың әрқайсысы ортақ құпия кілтті (generate_key функциялары) өзінің құпия саны мен басқа мүшенің жалпыға ортақ кілті негізінде есептейді. Алынған жалпы құпия кілттер екі пайдаланушыға да сәйкес келуі керек.

is_prime функциясы санның жай екенін тексеру үшін қолданылады. Ол Миллер-Рабин тестін k=5 кездейсоқ негіздермен қолданады, бұл санның жай болуына ықтималды кепілдік береді.

Бағдарламалық код 32-ден басталып, 32-ден 2048-ге дейін өсетін биттердегі p санының ұзындығының әртүрлі мәндері үшін бірқатар нәтижелерді алдық. Әрбір эксперимент үшін код кілттерді құруға және жалпы құпия кілтті есептеуге кететін уақытты есептеп, сонымен қатар жай p, G генераторы және екі құпия a және b сандарын сақтауға қажетті жадты байттармен пайдалануды бағалайды.

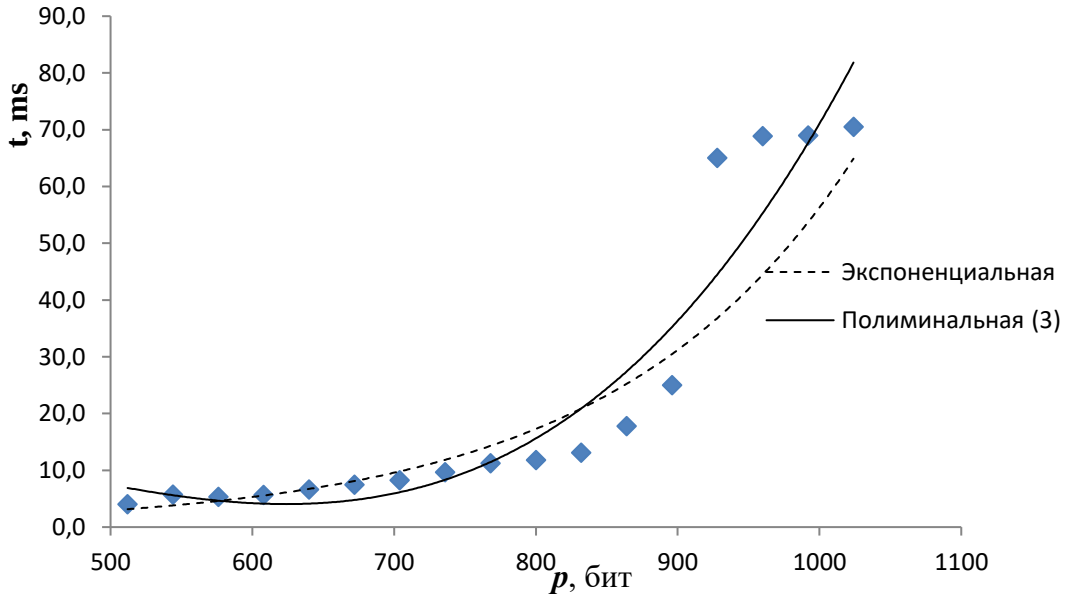
Есептеу Dell Inc., моделі OptiPlex 7470 AIO, процессоры Intel(R) Core(TM) i7-9700 CPU 3.00GHz ЭЕМ-нда орындалды.

Бағдарламалық есептеудің нәтижесі 2-4 суреттерде көрсетілген.

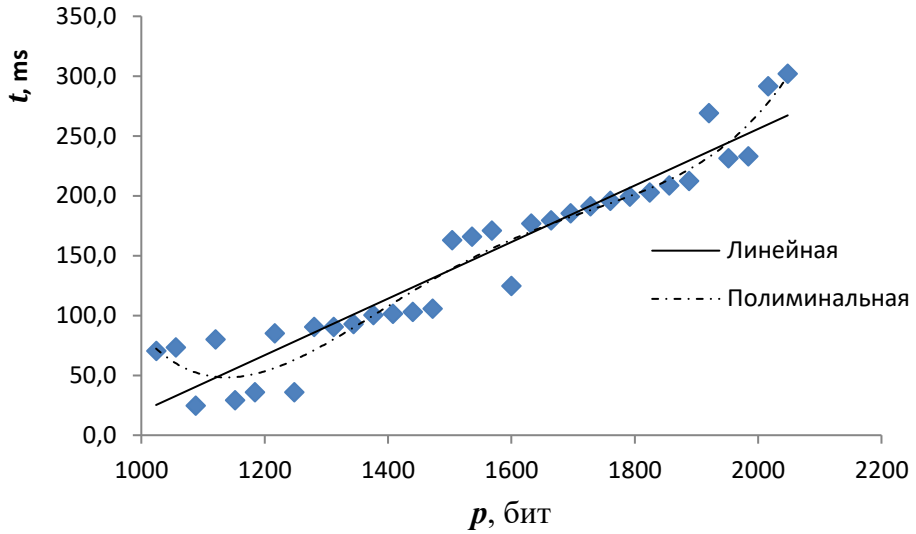


Сурет 2. 32-ден 512-ге дейін өсетін биттердегі p санының ұзындығының мәндері

Python тілінде Diffie-Hellman протоколын бағдарламалық қамтамасыз етуді енгізу есептеу экспериментін жүргізуге мүмкіндік берді. Компьютерлік бағдарламаның жұмыс уақытының кілт ұзындығына тәуелділігінің сызықтық сипаты p бастапқы параметрінің шағын мәндері үшін анықталады. p жай санның ұзындығы 512 биттен үлкен болғанда, программаның орындалу уақыты сызықты емес өседі.



Сурет 3. 512-ден 1024-ке дейін өсетін биттердегі p санының ұзындығының мәндері



Сурет 3. 1024-тен 2048-ге дейін өсетін биттердегі p санының ұзындығының мәндері

Қолданылған әдебиеттер тізімі

1. Subramani S., Svn S. K. Review of Security Methods Based on Classical Cryptography and Quantum Cryptography //Cybernetics and Systems. – 2023. – С. 1-19.

2. Oruganti R., Churi P. Systematic Survey on Cryptographic Methods Used for Key Management in Cloud Computing //International Conference on Innovative Computing and Communications: Proceedings of ICICC 2021, Volume 2. – Springer Singapore, 2022. – С. 445-460.

3. Imam R. et al. Systematic and critical review of rsa based public key cryptographic schemes: Past and present status //IEEE Access. – 2021. – Т. 9. – Pp. 155949 -155976.

4. Bojjagani S. et al. Systematic survey of mobile payments, protocols, and security infrastructure //Journal of Ambient Intelligence and Humanized Computing. – 2023. – Т. 14. – №. 1. – С. 609-654.

5. Diffie B.W. New Directions in Cryptography / B.W.Diffie, M.E.Hellman // IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976. – Pp. 644 – 654.

УДК 004.942

СЫЗЫҚТЫҚ ЕМЕС ФУНКЦИЯЛАР АРҚЫЛЫ АГРАРЛЫҚ ӨНІМДІ ӨНДІРУГЕ КЕТЕТІН ЕҢБЕК ШЫҒЫНДАРЫН БОЛЖАУ МОДЕЛЬДЕРІ

Қозан Ақдидар Райбекқызы, Асыл Камила Оразғалиқызы, Жақсан Мадина Сеилбекқызы,
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан akdidar.kozan@bk.ru
Ғылыми жетекші – А. Муханова, М. Самбетбаева.

Кіріспе. Аграрлық өнімді өндіруге жұмсалатын еңбек шығындары динамикада төмендейді, бұл, ең алдымен, кәсіпорынның техникамен жабдықталу деңгейіне және жаңа технологияларды пайдалануына байланысты. Кәсіпорын технологиясының деңгейі неғұрлым жоғары болса, оның әртүрлі өнім түрлерін өндіруге кететін шығыны соғұрлым төмен болады. 2011-2020 жылдардағы ауыл шаруашылығы өнімдерінің негізгі түрлерін өндіру бойынша деректер жүйеленді. Ақпарат көзі ретінде Қызылорда облысының агроөнеркәсіптік кешені тауар өндірушілерінің қаржылық-экономикалық жағдайы туралы жылдық статистикалық есептіліктің ресми нысандары пайдаланылды, олардың негізінде өндірілген өнімнің бірлігіне еңбек шығындары алынды. Көпжылдық кезеңдегі еңбек шығындарын талдау олардың шағын, орта және ірі шаруашылықтар үшін төмендеу тенденциялары бар екенін көрсетеді. Бұл жағдайда кәсіпорын көлемінің ұлғаюымен параметрдің шашырауын азайту үрдісі[1] байқалады.