ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

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 имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

©Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2024

ҚОРҒАНЫС ТҮРЛЕНДІРУЛЕРІНІҢ АЛГЕБРАЛЫҚ АЛГОРИТМДЕРІН ҚҰРУ ЖӘНЕ ӘЗІРЛЕУ ТӘСІЛДЕРІ

Ануарбеков Алмас Маратович
almasanuarbekov01@gmail.com
Л Л.Н.Гумилев атындағы ЕҰУ механика-математика факультетінің криптология мамандығының 2-курс магистранты
Ғылыми жетекшісі – Қозыбаев Д.Х

Аннотация. Қорғаныс түрлендірулерінің алгебралық алгоритмдері криптографияның маңызды саласы болып табылады, өйткені олар құпиялылық пен тұтастықты қамтамасыз ету үшін деректерді өңдеу құралдарын ұсынады. Бұл жұмыс осындай алгоритмдерді құру және дамыту тәсілдеріне шолу жасайды. Даму тәсілдері криптографияның математикалық негіздерін талдауды, есептеулердің күрделілігін және жүйеге сәтті шабуыл жасау ықтималдығын зерттеуді, алгебралық теория әдістерін деректерді түрлендіруді құру және талдау үшін қолдануды қамтиды. Сандар теориясы мен алгебраға негізделген классикалық әдістер де, Машиналық оқыту алгоритмдері мен жасанды интеллект технологияларын қолдануды қамтитын заманауи тәсілдер де қарастырылады.

Кіріспе. Ақпараттық технологиялардың дамуымен және интернет кеңістігінің кеңеюімен деректердің қауіпсіздігін қамтамасыз ету барған сайын өзекті міндетке айналуда. Криптографиялық әдістер цифрлық ортадағы ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қорғауда шешуші рөл атқарады. Криптографиядағы маңызды бағыттардың бірі-деректерді сенімді және тиімді шифрлауды қамтамасыз ететін қорғаныс түрлендіру алгоритмдерін жасау.

Қорғаныс түрлендірулерінің алгебралық алгоритмдері алгебралық амалдарды қолдана отырып, математикалық деректерді түрлендіруге негізделген шифрлау тәсілі болып табылады. Бұл алгоритмдер бірқатар артықшылықтарға ие, соның ішінде деректерді қорғаудың жоғары дәрежесі, тәжірибеде қолдану мүмкіндігі және қазіргі есептеу қуаты жағдайында тиімділік.

Негізгі бөлім. Ақпараттық технологиялар өмірдің барлық салаларында шешуші рөл атқаратын қазіргі әлемде ақпараттық қауіпсіздік мәселелері өзекті бола түсуде. Ақпаратты қорғауды қамтамасыз ету бағыттарының бірі Қорғаныс түрлендірулерінің алгебралық алгоритмдерін жасау болып табылады. Бұл алгоритмдер деректерді рұқсатсыз кіруден, модификациядан және басқа қауіптерден қорғауға арналған.

Қазіргі цифрлық әлемде деректердің қауіпсіздігін қамтамасыз ету ең өзекті мәселелердің бірі болып табылады. Бұл тұрғыда криптография ақпараттың құпиялылығын, тұтастығын және қол жетімділігін қорғау құралдарын қамтамасыз етуде шешуші рөл атқарады. Деректерді сенімді және тиімді шифрлауды қамтамасыз ететін қорғаныс түрлендірулерінің алгебралық алгоритмдеріне ерекше назар аударылады.

Сандар теориясы, Алгебралық құрылымдар және операциялар сияқты криптографияның математикалық негіздері криптографиялық алгоритмдерді дамытуда шешуші рөл атқарады. Осы кезде біз қорғаныс түрлендіру алгоритмдерінің негізінде жатқан негізгі математикалық ұғымдарды анықтаймыз.

Криптографияның алгебралық әдістері көпмүшелік алгебраға негізделген Алгоритмдер, эллиптикалық қисықтар және басқалары сияқты қорғаныс түрлендірулерін жасау үшін алгебралық құрылымдар мен операцияларды қолдануды қарастырады. Бұл әдістер деректерді қорғаудың жоғары деңгейін қамтамасыз етеді және қазіргі заманғы ақпараттық жүйелерде тиімді қолданылады.

Есептеулердің күрделілігі мен шабуылдардың ықтималдығын талдау криптографиялық әдістердің беріктігін бағалауға және ықтимал қауіптерден қорғау шараларын жасауға мүмкіндік береді.

Машиналық оқыту, жасанды интеллект және кванттық криптография сияқты заманауи әдістер мен технологиялар деректерді қорғаудың тиімді және тұрақты алгоритмдерін жасау үшін белсенді қолданылады.

Қорғаныс түрлендіру алгоритмдерін сәтті жүзеге асырудың мысалдары және оларды криптографиялық деректерді қорғау және жеке ақпаратты өңдеу сияқты әртүрлі салаларда қолдану криптографиядағы алгебралық алгоритмдердің маңыздылығы мен даму перспективаларын көрсетеді.

Классикалық алгебралық құрылымдарды қолдану: дәстүрлі тәсілдердің бірі-криптографиялық алгоритмдерді құру үшін ақырлы өрістер мен топтар сияқты алгебралық құрылымдарды қолдану. Мысалы, RSA алгоритмі бүтін сандар мен топ теориясының қасиеттеріне негізделген.

Жаңа алгебралық құрылымдарды дамыту: тиімді және қауіпсіз алгоритмдерді құру үшін жаңа алгебралық құрылымдар жасалуда. Мысалы, соңғы жылдары эллиптикалық қисықтарға негізделген Алгоритмдер белсенді түрде зерттелуде.

Әр түрлі алгебралық тәсілдердің тіркесімі: кейде қауіпсіздік пен тиімділік деңгейін жақсарту үшін әр түрлі алгебралық тәсілдердің тіркесімі қолданылады. Мысалы, шегерім өрістерінің қасиеттерін эллиптикалық қисықтармен біріктіруге болады.

Қолданыстағы алгоритмдерді нақты есептерге бейімдеу: кейбір жағдайларда алгебралық Алгоритмдер ақпаратты қорғау саласындағы нақты есептерді шешу үшін өзгертіледі немесе бейімделеді.

Қорғаныс түрлендірулерінің алгебралық алгоритмдері қауіпсіздік пен ақпаратты қорғауды қажет ететін әртүрлі салаларда кеңінен қолданылады.

RSA және эллиптикалық қисық негізіндегі алгоритмдер сияқты шифрлау алгоритмдері интернет-банкинг пен электрондық коммерциядағы транзакцияларды қорғау үшін қолданылады. Олар төлем деректері мен клиенттердің жеке ақпаратын қауіпсіз тасымалдауды қамтамасыз етеді.

Қорытынды. Қорытындылай келе, қорғаныс түрлендірулерінің алгебралық алгоритмдері қазіргі цифрлық әлемде деректердің қауіпсіздігін қамтамасыз етудің негізгі элементі болып табылатынын атап өткім келеді. Оларды әзірлеу және қолдану ақпараттың құпиялылығын, тұтастығын және қол жетімділігін қорғауда маңызды рөл атқарады.

Осы алгоритмдерге негізделген криптографияның математикалық негіздері криптографиялық әдістердің сенімділігі мен тиімділігін қамтамасыз етеді. Алгебралық әдістер күрделі және сенімді шифрларды жасауға мүмкіндік береді, оларға шабуыл жасау қиын.

Есептеулердің күрделілігі мен шабуылдардың ықтималдығын талдау криптографиялық алгоритмдердің беріктігін түсінуге және тиімді қорғаныс шараларын жасауға мүмкіндік береді. Машиналық оқыту және кванттық криптография сияқты заманауи әдістер мен технологияларды пайдалану бізге бар алгоритмдерді жақсартуға және деректерді қорғаудың жаңа, сенімді әдістерін жасауға мүмкіндік береді.

Әр түрлі салаларда қорғаныс түрлендіру алгоритмдерін сәтті жүзеге асырудың мысалдары олардың маңыздылығы мен тиімділігін растайды. Сонымен қатар, алгоритмдерді қазіргі цифрлық әлемде кездесетін жаңа сын-қатерлер мен қауіптерге бейімдеу үшін осы саладағы зерттеулер мен дамуды жалғастыру қажет.

Қолданылған әдебиеттер тізімі:

1. Menezes, A. J., Oorschot, P. C. van, & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
2. Коблиц, Н. (1994). A Course in Number Theory and Cryptography. Springer-Verlag.
3. Washington, L. C. (2008). Elliptic Curves: Number Theory and Cryptography. Chapman and Hall/CRC.
4. Stinson, D. R. (2005). Cryptography: Theory and Practice. Chapman and Hall/CRC.
5. Hoffstein, J., Pipher, J., & Silverman, J. H. (2008). An Introduction to Mathematical Cryptography. Springer.