Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN: 2616-7263. eISSN: 2663-1261
ТЕХНИКАЛЫҚ ҒЫЛЫМДАР ЖӘНЕ ТЕХНОЛОГИЯЛАР СЕРИЯСЫ /
TECHNICAL SCIENCES AND TECHNOLOGY SERIES/
СЕРИЯ ТЕХНИЧЕСКИЕ НАУКИ И ТЕХНОЛОГИИ

ХҒТАР 81.93.29
Шолу мақала

DOI: https://doi.org/10.32523/2616-7263-2024-148-3-176-188

Ақпараттық қауіпсіздіктің криптографиялық әдістеріне салыстырмалы талдау жүргізу

З.А. Исағалиева[1], Ә.С. Әбдіраман*[2], Н.К. Меделбаева[3], Л.С. Алдашева[3], А.Ж. Алибек[3]

[1]О. Тұрмағанбетұлы атындағы Маңғыстау индустриалды техникалық колледжі
[2]Әл-Фараби атындағы №21 мамандандырылған гимназия
[3]Astana IT University

(E-mail: aliya.abdiraman@astanait.edu.kz)

Аңдатпа. Бұл мақалада шифрлау алгоритмдерінің криптографиялық тұрақтылығын талдау әдістерін зерттеуге арналған. Шифрлау жүйелерінің тез дамуы, сондай-ақ оларды бұзудың ілеспе дамуы жоғары криптотұрақтылығы бар жаңа жүйелердің пайда болуына әкеледі. Жұмыс барысында әртүрлі параметрлер бойынша шифрлаудың танымал әдістері зерттелді (өнімділік, жад көлемі, бұзылуға төзімділік және т.б.) зерттеу нәтижелері бойынша DES және AES алгоритмдері таңдалды және Cryptool 2 бағдарламалық өнімінің көмегімен оның алгоритмі модельденді, сондай-ақ әртүрлі әдістер бойынша шабуыл жасалды. Зерттеу нәтижелері бойынша объектіге бағытталған C# бағдарламалау тілін қолдана отырып шифрлау алгоритмдерінің бағдарламалық құралы жобаланды.

Түйін сөздер: криптография, ақпараттық қауіпсіздік, тұтастық, шифрлау, AES, DES, 3DES.

Түсті 30.05.2024 Жөнделді 14.08.2024 Мақұлданды 09.09.2024 Онлайн қолжетімді 30.09.2024

[1]*хат-хабар үшін автор

Кіріспе

Компьютерлік жүйелердің адам қызметінің кез-келген салаласына кеңінен енуі, цифрландыру үрдісінің қарқынды дамуы деректерді өңдеу жүйелерін киберқауіпке осал, сонымен қатар, қоғам пайдаланылатын мәліметтер ақпараттық технологиялардың қауіпсіздік деңгейіне тәуелді етеді. Сол себепті, айналымдағы және жіберілетін ақпараттың қауіпсіздігі қолданылатын ақпаратты қорғаудың криптографиялық алгоритмдеріне тікелей байланысты.

Кез-келген мемлекеттің даму стратегиясының басымдықтарының бірі ұлттық қауіпсіздік болып табылады, ал оның аса маңызды элементтерінің бірі ақпараттық қауіпсіздік болып табылады. Сондықтан ақпаратты қорғаудың жаңа технологияларын құру, оған қолжетімділікті шектеу, ақпаратты қорғаудың қажетті деңгейін қамтамасыз ету және қазіргі заманғы талаптарға жауап беретін ақпаратты қорғау құралдарын әзірлеу өзекті міндеттердің біріне айналады. Қорғалған ақпарат алмасу жүйелерінде ақпараттың құпиялылығын, тұтастығын, авторлығын теріске шығармауды қамтамасыз ететін криптографиялық құралдар пайдаланылуы тиіс [1]. Әр елде деректерді шифрлау және дешифрлау үшін ақпаратты криптографиялық қорғаудың әртүрлі стандарттары қолданылады. Бұл ретте, криптографиялық алгоритмдерге талдау жасау, зерттеу жүргізу оларды қолдану тиімділігін арттыруға, жетілдіру бойынша ұсыныстар енгізуге, артықшылықтары мен әлсіз тұстарын анықтауға үлкен мүмкіндік берері сөзсіз.

Әдіснама

Зерттеу мәселесі – ақпаратты қорғаудың криптографиялық әдістерін зерттеп, оларға салыстырмалы талдау жүргізу; зерттеу нәтижесіне алынған мәліметтерге сүйене отырып, объектілі-бағытталған бағдарламалау тілдерін қолданып, симметриялық алгоритмнің жұмысын модельдейтін бағдарламалық жасақтама құру [2].

Аталған мақсатқа жету үшін келесідей міндеттер қойылды:

– ақпаратты криптографиялық қорғау әдістеріне шолу және талдау;

– ақпаратты криптографиялық қорғау жүйелеріне қойылатын талаптар мен өнімділік критерийлерін бағалау;

– ақпаратты криптографиялық қорғау әдістерін және олардың жұмыс принципін зерттеу.

– ақпаратты криптографиялық қорғаудың қолданыстағы әдістеріне және олардың мүмкіндіктеріне салыстырмалы талдау жүргізу;

– заманауи объектілі-бағытталған бағдарламалау тілдерін қолдана отырып, симметриялық алгоритмді модельдеу әдістерін зерттеу;

– ақпаратты шифрлаудың симметриялық алгоритмінің жұмысын визуалды модельдеу үшін объектілі-бағытталған бағдарламалау тілінде пайдаланушы интерфейсі бар бағдарламалық жасақтаманы әзірлеу;

– объектілі-бағытталған бағдарламалау тілдерін қолдана отырып, модельдеудің ыңғайлы және тиімді әдісін таңдау. Бағдарламалық жасақтаманы модельдеу процесін және функционалдығын сипаттау.

Ақпараттық қауіпсіздікті қаматамасыз ету әлі де болса толық шешімін таппаған мәселе. Бұл ретте қауіпсіздіктің салыстырмалы түрде жоғары деңгейін көрсете алатын алгоритмдерді таңдай білу қажет. Бұл жұмыста алгоритмдердің басты параметрлері сипатталды (кілт ұзындығы, өңделетін блок ұзындығы, математикалық моделінің күрделілігі, криптоаналитикалық шабуылдарға төзімділігі) және қазіргі кездегі ең танымал симметриялық криптожүйелерге салыстырмалы талдау жүргізілді. Алгоритмдердің тұрақтылығын сандық бағалау келесі критерийлер бойынша анықталды: крипто тұрақтылығы, крипто-тұрақтылық қоры, кілттің кеңею жылдамдығы, жұмыс уақытында шабуылдардан қорғау, көшкін әсерін жүзеге асыру, кілтті тез кеңейту мүмкіндігі және параллель есептеу мүмкіндігі. Әр шифрлау алгоритмінің артықшылықтары мен кемшіліктері анықталды [3]. Зерттеулер мен талдау нәтижесінде шифрлаудың ең берік симметриялық алгоритмдері таңдалды. Объектілі-бағытталған программалау тілдерін қолданып, таңдалған алгоритмнің жұмысын модельдейтін қолданушы интерфейсіне ие бағдарламалық жасақтама әзірленді.

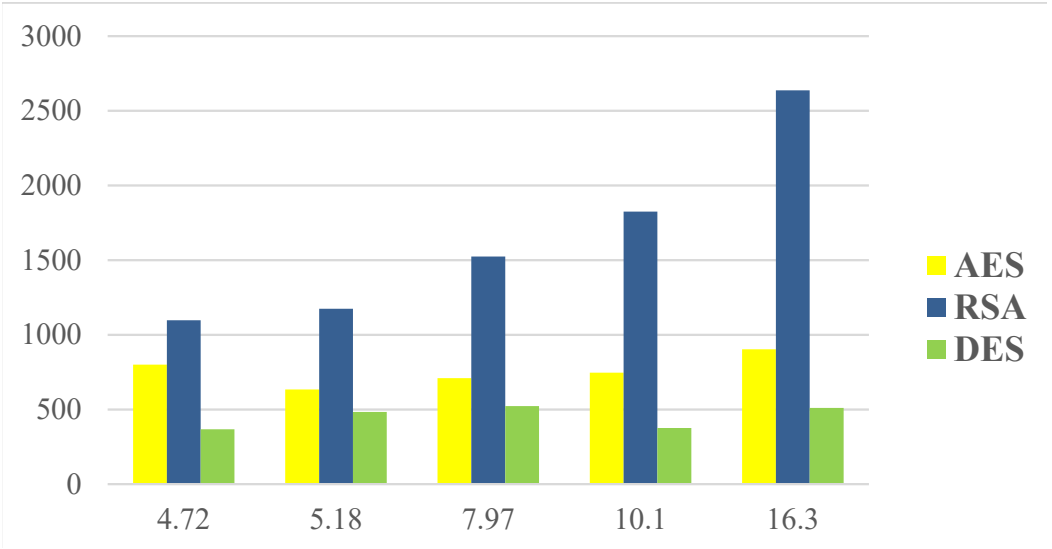
Зерттеу жұмысының теориялық және тәжірибелік маңызы ақпаратты қорғаудың криптографиялық алгроритмдеріне жүргізілген талдау нәтижелері және ақпаратты түрлендіру мақсатында симмериялық алгоритмдерді модельдейтін бағдарламалық жасақтаманың әзірленуімен негізделеді.

Криптографиялық алгоритмдерді уақыт, жады, қауіпсіздік деңгейі параметрлері бойынша салыстыру.

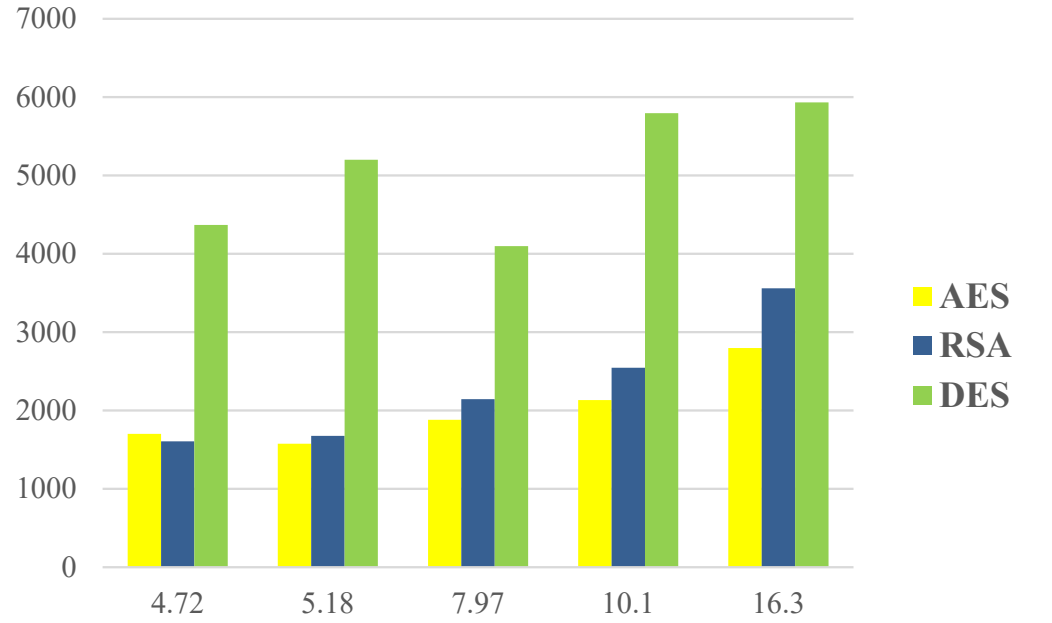
Ақпаратты криптографиялық қорғау құралдарын құру, оның ішінде шифрлау алгоритмдері бойынша өте көп зерттеулер жүргізілген. Осы зерттеулер нәтижесін, яғни басқа ғалымдардың ғылыми еңбектеріне шолу жасап келесідей нәтижелерге қол жеткізіп қорытынды шығарылды:

Бұл [4] ғылыми мақалада авторлар AES, DES және RSA криптографиялық алгоритмдеріне есептеу уақыты, жадты пайдалану және қауіпсіздік деңгейі бойынша салыстырмалы талдау жүргізілген. Зерттеу жұмыстары әріптер, сандар және арнайы таңбалардан құралған әртүрлі өлшемдегі мәтіндік файлдарды қамтыған.

Есептеу уақыты деп қарапайым мәтінді шифрланған мәтінге айналдыру үшін қажет уақыт болып саналады. Бұл параметр әр алгоритмнің күрделілігін көрсетеді. Сурет 1-де үш алгоритмнің әртүрлі көлемдегі файлды шифрлауға кеткен уақыт көлемі *(ms)* көрсетілген. Ақпаратты шифрлауда DES алгоритмі AES және RSA алгоритмімен салыстырғанда көп уақыт алады. AES және RSA алгоритмі шифрлау процесіне кететін уақыттың аз көлемін көрсетті. Ал сурет 2-де үш алгоритмнің әртүрлі көлемдегі файлды кері шифрлауға, яғни дешифрлауға кеткен уақыт көлемі көрсетілген. Ақпаратты кері шифрлауда RSA алгоритмі AES және DES алгоритмімен салыстырғанда көп уақыт алады. AES алгоритмі шифрлау процесіне кететін уақыттың ең аз көлемін көрсетті.

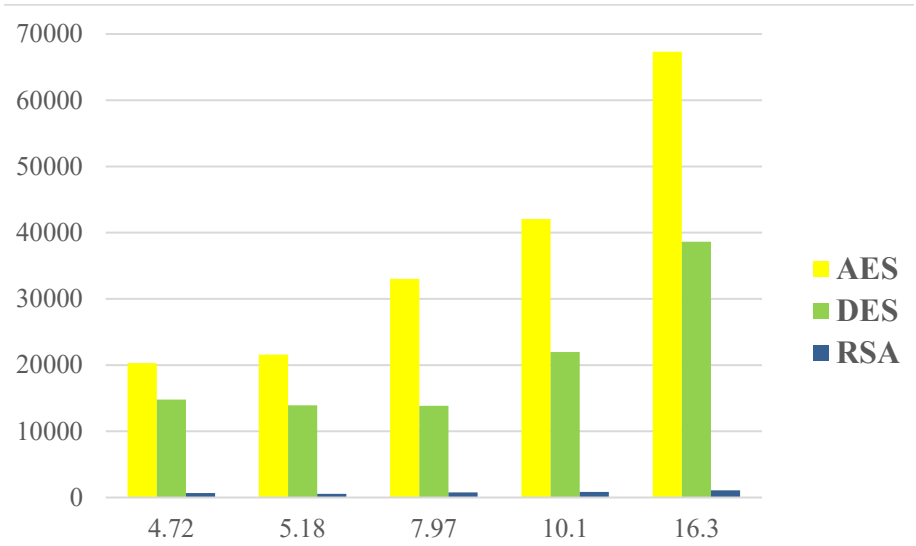


1-сурет. AES, DES және RSA алгоритмдерінің шифрлау уақытының салыстырмалы талдау нәтижесі



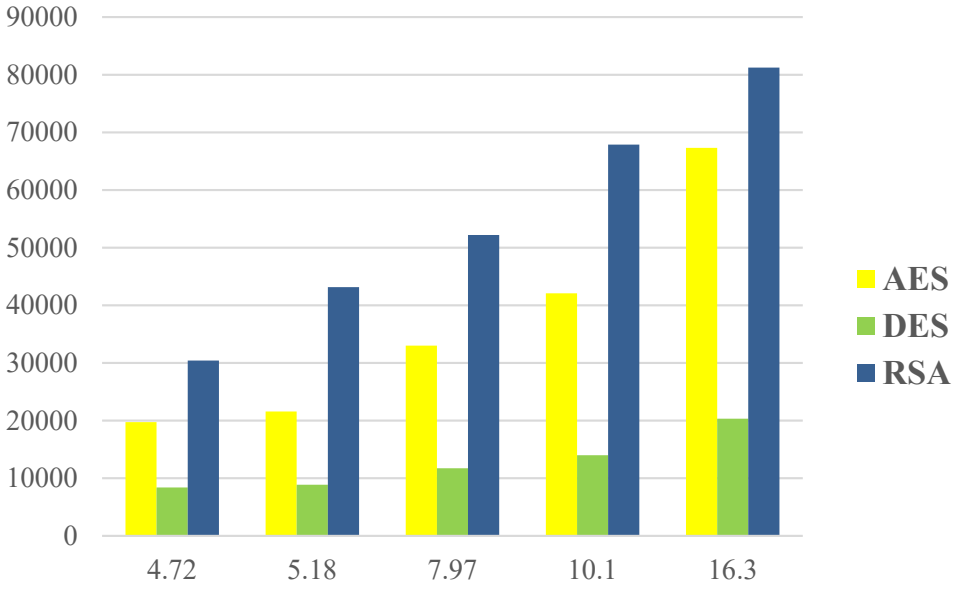
2-сурет. AES, DES және RSA алгоритмдерінің дешифрлау уақытының салыстырмалы талдау нәтижесі

Жадты пайдалануға негізделген криптографиялық алгоритмнің тиімділігін бағалау үшін алгоритмнің тиімділігіне негізделген күрделілікті тексерудің «Big-O Analysis» әдісі қолданылады, яғни ол жадыдан алатын орынды және уақытты тексереді. Сурет 3-те AES, DES және RSA алгоритмдері арасында жадты пайдаланудың (шифрлаудың) салыстырмалы талдау нәтижесі көрсетілген.



3-сурет. AES, DES және RSA арасында жадты пайдаланудың (шифрлаудың) салыстырмалы талдау нәтижесі

Сурет 4-те AES, DES және RSA алгоритмдері арасында жадты пайдаланудың (дешифрлаудың) салыстырмалы талдау нәтижесі көрсетілген.



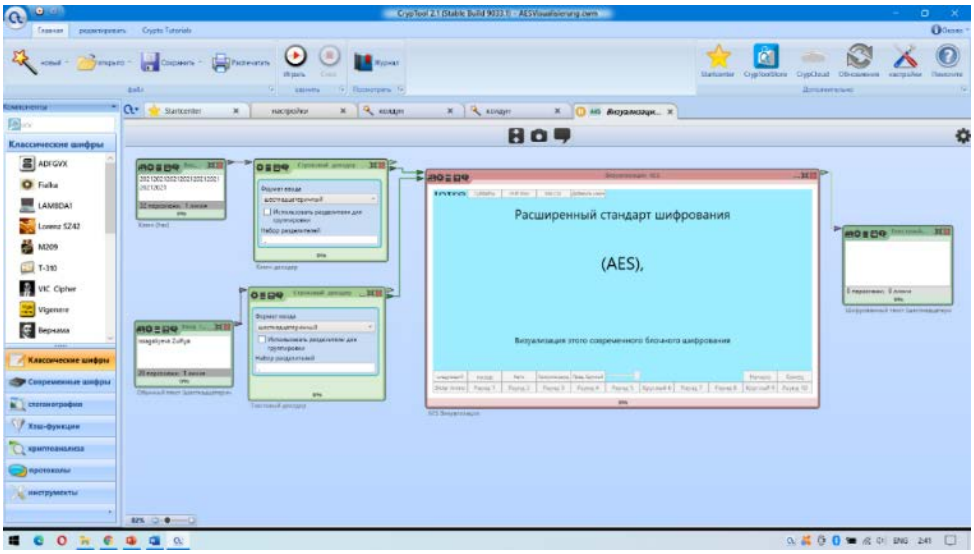
4-сурет. AES, DES және RSA арасында жадты пайдаланудың (дешифрлаудың) салыстырмалы талдау нәтижесі

Жоғарыда келтірілген графиктерде AES, DES және RSA алгоритмдері арасында уақыт, жады, қауіпсіздік деңгейі параметрлері бойынша салыстыру нәтижелері келтірілген.

Нәтижелер мен талқылау

CrypTool 2 (CT2) – бұл криптография мен криптоанализді визуализациялайтын Windows үшін заманауи электронды оқыту бағдарламасы [5]. Ол шифрлауды және криптоталдауды ғана емес, сонымен қатар олардың негіздерін және заманауи криптографияның барлық спектрін қамтиды. CT құрамында жұмыс процестері бар 200-ден астам дайын шаблондар бар. Сондай-ақ, CT2-де жұмыс процестерін құру үшін криптографиялық функцияларды оңай біріктіруге және орындауға болады (визуалды бағдарламалау) [6]. Мұндай тәсілмен күрделі процестерді оңай көруге болады, сондықтан оларды жақсы түсінуге болады. Векторлық графиканың көмегімен ағымдағы көріністі еркін масштабтауға болады.

Жұмыс процесінде қолданылатын компонентті іске асырылған алгоритмнің ішкі процесін визуализациялау үшін де бірдей қолдануға болады. Бұл пайдаланушыға криптографиялық процесті егжей-тегжейлі түсінуді жеңілдетеді сонымен қатар жалпы бейнені, яғни процесті қолданатын нақты сценарийді естен шығармайды. Сурет 5-те AES шифрын визуализациялау үдерісі бейнеленген.



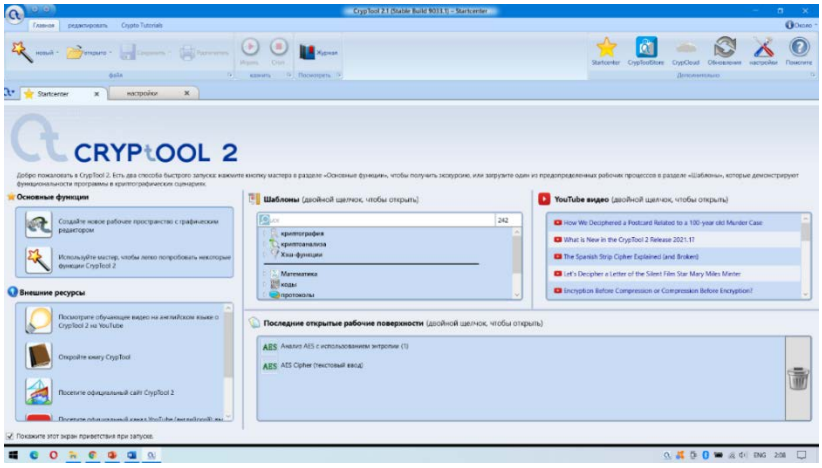
5-сурет. AES шифрын визуализациялау

CrypTool 2 (CT2) классикалық және заманауи шифрлауды талдау және бұзу үшін қолдануға болатын көптеген құралдарды ұсынады. Мысалы, жиіліктердің таралуын бағалауға, Виженер сияқты полиалфавиттік шифрлардың кілттерінің ұзындығын анықтауға, қазіргі заманғы Oracle толтыру шабуылын жасауға немесе блоктық шифрларға қарсы дифференциалды криптоанализді қолдануға мүмкіндік береді.

CrypTool-да әр түрлі кілттер мен хэш функциялары бар. Олар Startcenter шаблондарының тізімінде орналасқан. Заманауи хэш парольдері әр түрлі кілт енгізу функцияларын қолданады. Құпия сөздің (пароль) сенімділігі мамандандырылған «Құпия сөздің сенімділігін тексеру» шаблонымен тексеріледі. CrypTool талданған парольдің

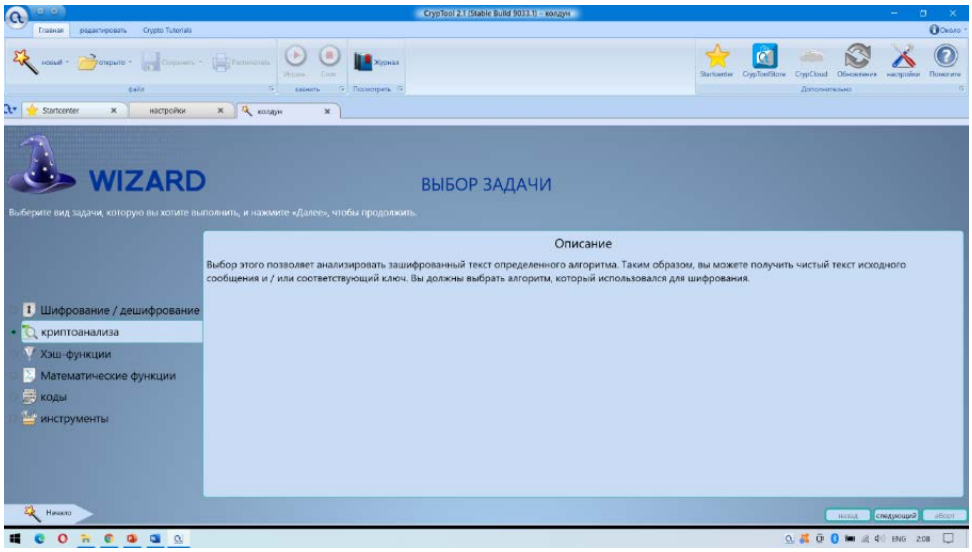
қауіпсіздік деңгейі туралы ақпарат береді. Егер қауіпсіздік деңгейі төмен болса, оны әріптер (бас әріптерді қоса), сандар мен таңбаларды қосу арқылы өзгерту қажеттігі туралы хабарлама береді. Құпия сөз сенімді болуы үшін қызметтік бағдарламамен алынған мәліметтерге сүйене отырып, оның ұзындығы таңбалар комбинациясының күрделілігіне қарағанда үлкен мәнге ие.

Сурет 6 келтірілген интерфейстің сол жақ терезесінде (негізгі терезеде), «Негізгі функциялар» бөлімінде, «Шебер көмегімен...» деп белгіленіп тұрған өрісті таңдауымыз қажет.



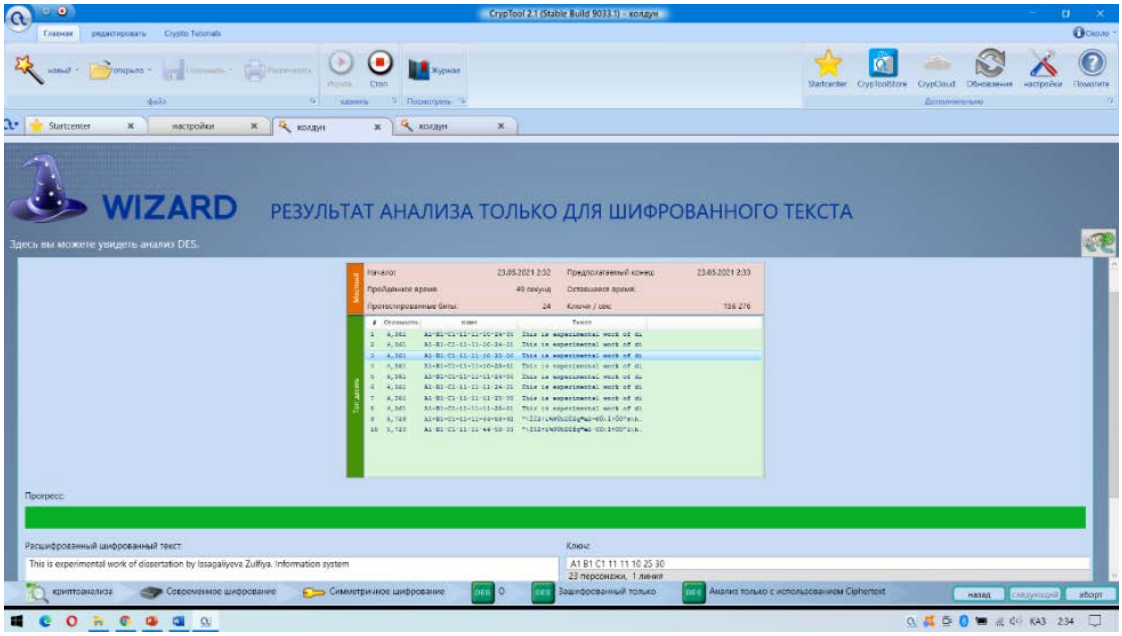
6-сурет. Cryptool 2 бағдарламасының басты беті

Cryptool 2 бағдарламасын қолданып AES және DES алгоритмдеріне мүмкін болатын кілттерді (кілтті білместен) іріктеп алу арқылы хабарламаны ашып оқу мүмкіндігі сыналды. Ол үшін ашылған сурет 7 келтірілген терезеден «Криптоталдау» бөлімін таңдап, «Келесі» батырмасын басу қажет.

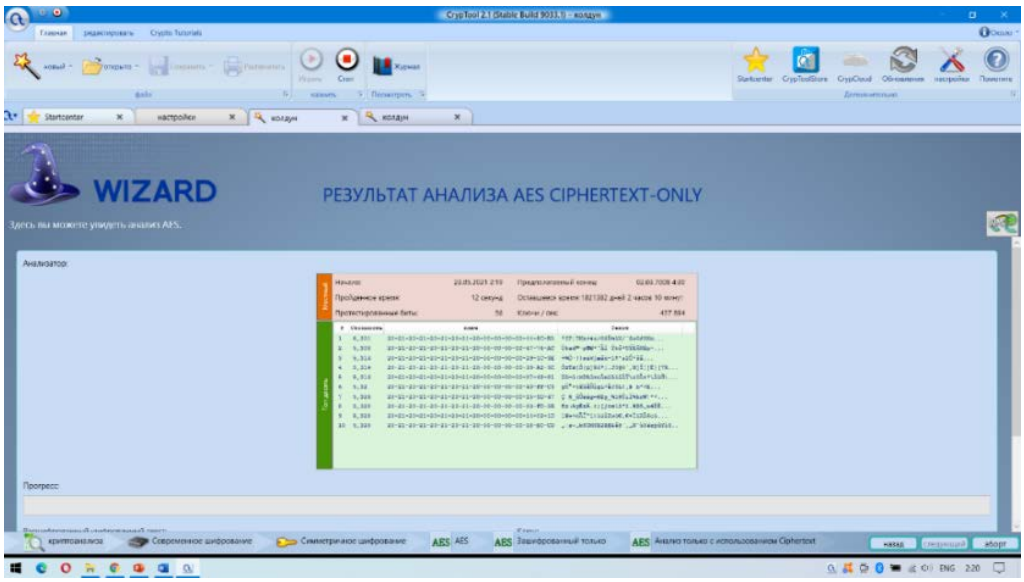


7-сурет. Cryptool 2 «Криптоталдау» беті

Сурет 13 DES криптографиялық алгоритмдерді шабуылдарға беріктілігіне талдау жүргізу нәтижесі кельтірілген. Ескере кететін жәйт, егер шабылдаушы кілт мәнін мүлдем білдем білмейтін болса, кілтті іріктеп табу үшін 40 жылға жуық уақыт кететіні сурет 14 көрсетілген. Яғни теориялық түрде алгоритмдерді бұзу мүмкін болғанымен, тәжірибе жүзінде оны ешкім көрсете және дәлелдей алмады. Себебі күрделі кілтті іріктеуге кететін уақыт өте көп уақыт және қаржыны талап етеді.



Сурет 13. Cryptool 2 «Кілттерді іріктеу»



Сурет 14. Cryptool 2 «Кілт мәнін білместен хабарламаны ашып оқу»

Нақты алгоритмнің деректерді шифрлаудағы жылдамдығы шифрлау алгоритмінің жұмыс жылдамдығын талдауда маңызды параметр болып табылады [7-9]. Алгоритм қауіпсіздіктің жоғары деңгейін қамтамасыз етсе ғана сенімді болып саналады. Авторлар криптографиялық алгоритмдердің (AES, DES) қауіпсіздік деңгейлерін талдау қорытындысы бойынша кесте 1 келтірілген нәтижелерге ие болды.

1-кесте. Криптографиялық алгоритмдердің салыстырмалы сипаттамасы

Алгоритм	DES	Triple DES	Blow Fish	Two Fish	AES	RSA
Шифр түрі	Симметриялық блоктық	Симметриялық блоктық	Симметриялық блоктық	Симметриялық блоктық	Симметриялық блоктық	Асимметриялық блоктық
Кілт ұзындығы (Bits)	54	56, 112 немесе 168	32 - 448	128, 192 немесе 256	128	1024 - 4096
Блок өлшемі (Bits)	64	6	6	128	128	Өзгермелі
Жылдамдығы	Баяу	Өте баяу	Жылдам	Жылдам	Жылдам	Баяу
Қауіпсіздігі	Жеткіліксіз емес	Жеткілікті емес	Қауіпі аз	Қауіпсіздігі жоғарылау	Қауіпсіз	Қауіпі аз
Ерекшелігі	Кең таралған, қуаты төмен	Модификацияланған DES, Жеткілікті қауіпсіздік	Жоғары қауіпсіздік	-	DES алмастырылымы, Жоғары қауіпсіздік	-
Математикалық амалдар	XOR, Fixed S-boxes	XOR, Fixed S-boxes	A Logical XOR addition, Modulo Arithmetic	XOR	Substitution byte, Shift row, Mixcolumn and Addround key	Exponentiation and Modulo Arithemetic
Икемділігі	Жоқ	Иә	Иә	Иә	Иә	Иә
Шабуыл түрі	Қатал күш шабуылы (Brute Force)	«Brute» шабуылы, «Force» шабуыл, Таңдалған ашық мәтін	Dictionary Attack	Мүмкін емес дифференциалды шабуыл	Бүйірлік арна шабуылы	Ашық кілт факторингі

Қорытынды

Криптографиялық әдістер мен құралдар жаңа желілік қауіпсіздік технологияларын дамытуда маңызды рөл атқарады. Авторлардың жүргізген талдауы бойынша қарастырылған бес шифрлау алгоритмдерінің ішінде AES энергияны тұтыну, өнімділік және ресурстарды пайдалану тұрғысынан ең тиімдісі болып табылады. AES шифрлау алгоритмі жылдам, сонымен қатар, аппараттық және бағдарламалық ортада қолдануға жақсы бейімделген.

Көрсетілген нәтижелерге қарап, жұмыс өнімділігі жоғары алгоритм ретінде AES-ті ерекшелеуге болады. Келесі DES және 3DES. Жұмыс өнімділігінің салыстырмалы төмен деңгейін көрсеткен RSA шифры. Сонымен қатар аталған алгоритмдерге Cryptool 2 бағдарламасында алгоритмдерге жасалатын шабуылдарға төзімділігі талданды. Осы нәтижелерге сүйене отырып, жылдамдықтың, жадыдан алатын орын, қауіпсіздіктің жоғары деңгейін көрсеткен AES және DES алгоритмдері бағдарламалық жасақтаманы құруға негіз ретінде алынды.

Авторлардың қосқан үлесі.

Исағалиева З.А. зерттеу тұжырымдамасы мен әдістемесін әзірледі.

Әбдіраман Ә.С. хат-хабар авторы ретінде авторлар ұжымының жұмысын үйлестірді, криптографиялық алгоритмдерге салыстырмалы талдау жүргізді және мақаланың кіріспе, негізгі бөлім және қорытындыны қамтитын негізгі бөлімдерін жазып, редакциялады.

Меделбаева Н.К. криптографиялық беріктік әдістерін талдауға қатысты, алгоритмдерді сынау үшін мәліметтер дайындады, Cryptool 2 бағдарламалық құралын пайдалану арқылы эксперименттер жүргізді және нәтижелерге талдау жасады.

Л.С. Алдашева криптографиялық алгоритмдерді модельдеуге арналған бағдарламалық қамтамасыз етуді әзірледі, жұмыстың модельдеу және бағдарламалаудың техникалық аспектілеріне қатысты бөлімдерін жазды және әдебиеттерге шолу жасады.

А.Ж. Әлібек симметриялық және асимметриялық шифрлау алгоритмдерін қолдану бойынша зерттеулер жүргізді, мақалада келтірілген графиктер мен кестелерді дайындап, талдады, сонымен қатар мақаланың техникалық аспектілерін өңдеуге қатысты.

Әдебиеттер тізімі

1. Priya C. Trusted Cloud Computing Platform in IaaS for Closed Box Execution Environment to VM // Journal of Advanced Research in Dynamical and Control Systems, 10, 193-198 (2018)

2. R.Ranjani and Dr.C.Priya A Fusion of Image Processing and Neural Networks for Lung Cancer Detection Using SVM In Matlab // International Journal of Pure and Applied Mathematics, 119, 100-111 (2018)

3. Prachi V. Bhalerao Hardware Implementation of Cryptosystem by AES Algorithm Using FPGA // IJCMC, 6, 84-89 (2018)

4. GurupinderKaur, Dr.Amandeep Singh Sappal Implementation of AES Algorithm on FPGA For Low Area Consumption. // International Journal of Advanced Research in Computer Science, 8, 704-707 (2019)

5. R.Ranjani, C.Priya A Survey on Face Recognition Techniques: A Review / / International Journal of Pure and Applied Mathematics, 118, 253-274 (2017)

6. Kuzminykh E.S., Ilina S.P., Maslova M.A. Analysis of impenetrable encryption algorithms // Research result. Information technologies, 9(1), 10-18 (2024)

7. Kostikov V.A. The need to compress encrypted data using LZW and Huffman coding algorithms // Theory and practice of project education, 3(19), 62-64 (2021)

8. Vovchenko N.G., Kuznetsov N.G., Makarenko E.N. Implementation of ESG principles in the strategy for sustainable development of the Russian economy [study guide], (Rostov-on-Don, 2022, 508 p.) [in Russian]

9. Объяснение шифрования AES, - [Электронды ресурс]. Қолжетімді: https://blog.kraden.com/ru/aes-256-encryption (қолжеткізілді 08.06.2024)

З.А. Исағалиева[1], Ә.С.Әбдіраман*[2], Н.К.Меделбаева[3], Л.С.Алдашева[3], А.Ж.Алибек[3]

[1]Мангистауский индустриальный технический колледж имени О.Тұрмағанбетұлы

[2]Специализированная гимназия №21 имени Аль-Фараби атындағы

[3]Astana IT University

Сравнительный анализ криптографических методов защиты информации

Аннотация. Данная статья посвящена исследованию методов анализа криптографической устойчивости алгоритмов шифрования. Бурное развитие систем шифрования, а также сопутствующее развитие их взлома приводит к появлению новых систем с высокой криптостойкостью. В ходе работы были изучены популярные методы шифрования по различным параметрам (производительность, объем памяти, устойчивость к повреждениям и т.д.), по результатам исследования были выбраны алгоритмы DES и AES, а его алгоритм смоделирован с помощью программный продукт Cryptool 2, а также атаку различными методами. По результатам исследования было разработано программное обеспечение алгоритма шифрования с использованием объектно-ориентированного языка программирования C#.

Ключевые слова: криптография, информационная безопасность, целостность, шифрование, AES, DES, 3DES.

Z.A. Issagalyeva[1], A.S.Abdiraman*[2], N.K.Medelbayeva[3], L.S.Aldasheva[3], A.Zh. Alibek[3]

[1]Mangistau Industrial Technical College named after O. Turmaganbetuly

[2]Specialized gymnasium No. 21 named after Al-Farabi Atyndagy

[3]Astana IT University

Comparative analysis of cryptographic methods of information protection

Abstract. This article is devoted to the study of methods for analyzing the cryptographic stability of encryption algorithms. The rapid development of encryption systems, as well as the concomitant

development of their hacking, leads to the emergence of new systems with high cryptographic strength. During the work, popular encryption methods were studied according to various parameters (performance, memory size, resistance to damage, etc.), based on the results of the study, the DES and AES algorithms were selected, and its algorithm was modeled using the Cryptool 2 software product, as well as attack by various methods. Based on the results of the study, software for an encryption algorithm was developed using the object-oriented programming language C#.

Keywords: cryptography, information security, integrity, encryption, AES, DES, 3DES.

References

1. Priya C. Trusted Cloud Computing Platform in IaaS for Closed Box Execution Environment to VM / / Journal of Advanced Research in Dynamical and Control Systems, 10, 193-198 (2018)

2. R.Ranjani and Dr.C.Priya A Fusion of Image Processing and Neural Networks for Lung Cancer Detection Using SVM In Matlab // International Journal of Pure and Applied Mathematics, 119, 100-111 (2018)

3. Prachi V. Bhalerao Hardware Implementation of Cryptosystem by AES Algorithm Using FPGA / / IJCMC, 6, 84-89 (2018)

4. GurupinderKaur, Dr.Amandeep Singh Sappal Implementation of AES Algorithm on FPGA For Low Area Consumption. // International Journal of Advanced Research in Computer Science, 8, 704-707 (2019)

5. R.Ranjani, C.Priya A Survey on Face Recognition Techniques: A Review / / International Journal of Pure and Applied Mathematics, 118, 253-274 (2017)

6. Kuzminykh E.S., Ilina S.P., Maslova M.A. Analysis of impenetrable encryption algorithms // Research result. Information technologies, 9(1), 10-18 (2024)

7. Kostikov V.A. The need to compress encrypted data using LZW and Huffman coding algorithms // Theory and practice of project education, 3(19), 62-64 (2021)

8. Vovchenko N.G., Kuznetsov N.G., Makarenko E.N. Implementation of ESG principles in the strategy for sustainable development of the Russian economy [study guide], (Rostov-on-Don, 2022, 508 p.) [in Russian]

9. AES encryption, - [electronic resource]. Available: https://blog.kraden.com/ru/aes-256-encryption (accessed 08.06.2024

Авторлар туралы мәлімет:

Исағалиева З.А. **–** магистр, О.Тұрмағанбетұлы атындағы Маңғыстау индустриалды техникалық колледжі, арнайы пәндер оқытушысы, Жаңаөзен, Қазақстан

Әбдіраман Ә.С. **–** хат хабар авторы, магистр, Astana IT University сеньор лектор, Астана, Қазақстан

Меделбаева Н.К. **–** Әл-Фараби атындағы №21 мамандандырылған гимназия, математика пәні мұғалімі, Ақтөбе, Казақстан

Алдашева Л.С. **–** техникалық ғылымдар кандидаты, Astana IT University асистент профессор, Астана, Қазақстан

Алибек А.Ж. **–** магистр, Astana IT University оқытушы, Астана, Қазақстан

Исағалиева З.А. **–** Магистр, Мангистауский индустриально-технический колледж имени О.Турмаганбетулы, преподаватель специальных предметов, Жанаозен, Казахстан

Әбдіраман Ә.С. **–** автор для корреспонденци, магистр, старший преподаватель Astana IT University, Астана, Казахстан

Меделбаева Н.К. **–** Учитель математики специализированной гимназии №21 имени Аль-Фараби, г. Актобе, Казахстан

Алдашева Л.С. **–** кандидат технических наук, доцент Astana IT University, Астана, Казахстан

Алибек А.Ж. **–** магистр, преподаватель Astana IT University, Астана, Казахстан

Isagalieva Z.A. **–** Master, Mangistau Industrial and Technical College named after O. Turmaganbetuly, teacher of special subjects, Zhanaozen, Kazakhstan

Abdiraman A.S. – corresponding author, master's degree, senior lecturer at Astana IT University, Astana, Kazakhstan

Medelbaeva N.K. **–** Mathematics teacher at specialized gymnasium No. 21 named after Al-Farabi, ***Aktobe, Kazakhstan***

Aldasheva L.S. **–** Candidate of Technical Sciences, Associate Professor Astana IT University, Astana, Kazakhstan

Alibek A.Zh. – Master, teacher at Astana IT University, Astana, Kazakhstan