КОМПЬЮТЕРНЫЕ НАУКИ, ПРИБОСТРОЕНИЕ И АВТОМАТИЗАЦИЯ
КОМПЬЮТЕРЛІК ҒЫЛЫМДАР, АСПАП ЖАСАУ ЖӘНЕ АВТОМАТТАНДЫРУ
COMPUTER SCIENCE, INSTRUMENTATION AND AUTOMATION

ӘОЖ 004.056
ҒТАХА 81.93.29
https://doi.org/10.53364/24138614_2025_38_3_7

А.Хомпыш[1,2], Қ.С.Сақан[2*], К.Алғазы[2], А.Ж.Абишева[3]
[1]Нұр-Мүбарак Египет ислам мәдениеті университеті,Алматы, Қазақстан
[2]Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан
[3]Абай атындағы Қазақ Ұлттық Педагогикалық университеті, Алматы, Қазақстан

[*]*E-mail:* kairat_sks@mail.ru

«EM CHIPER» БЛОКТЫ ШИФРЛАУ АЛГОРИТМІНІҢ КРИПТОБЕРІКТІЛІГІН ЗЕРТТЕУ

Аңдатпа. *Криптографиялық алгоритмдерінің ішінде блокты шифрлау алгоритмдері құпия ақпараттарды рұқсат етілмеген пайдаланушылардан сенім қорғау үшін қолданылады. Көптеген мемлекеттерде блокты шифрлау алгоритмдерінің өзіндік стандартары бекітіліген. Ол өз кезегінде ақпараттарды сенімді қорғауға мүмкіндік береді. Ал Қазақстанда мұндай ақпараттарды қорғау алгоритмдерінің стандарттары бекітілмегенін ескерсек, онда блокты шифрлау алгоритмдерін құру, олардың криптоберіктілігін зерттеу әрқашанда өзекті мәселелердің бірі. Бұл мақалада блокты шифрлау «EM Chiper» алгоритміне дифференциальдық және статистикалық талдау жүргізіліп нәтижелері ұсынылды. Блокты шифрлау алгоритмдерінің қауіпсіздігін зерттеудің негізгі әдістерінің бірі статистикалық қауіпсіздігін талдау болып табылады. Әдетте блокты шифрлауда қолданылатын түрлендірулер барысында жақсы араластыру мен шашырау сәтті түрде орындалса, онда алгоритмнің криптографиялық беріктігін жоғарғы деңгейде қорғауға мүмкіндік алуға болады. Статистикалық талдау жүргізу үшін алгоритм бағдарламалық жүзеге асырылып әртүрлі ұзындықтағы шифрмәтін алынды. Жүргізілген зерттеулерге сай ұсынылған алгоритмнің статистикалық талдаулары жоғары нәтиже көрсетті, яғни NIST ұсынған талаптарға сай А бағанадағы мәндері С мәнінен үлкен, ал В мәндері D мәндерінен үлкен екендігі анықталды. Дифференциалды талдаулар нәтижесі көрсеткендей ұсынылған алгоритм криптобекітілігі жағынан жоғары екендігі анықталды. Яғни 16 раундттан бастап кілтті табу ықтималдығы* 2^{-126} *тең. Сонымен қатар мақалада белгілі алгоритмдердің дифференциалды талдауларына нәтижелерімен салыстырмалы талдау жүргізіліп, танымал Camellia 128, AES 128 алгоритмдерімен шамалас нәтиже көрсеткендігі анықталды. Алдағы жұмыстарда басқада алгоримнің криптобекітілігі жан жақты зерттелініп нәтижелері мақала ретінде ұсынылатын болады.*

Түйін сөздер*. Блокты шифр, шифр, криптография, кілт, дифференциалды криптоталдау, статистикалық талдау, EM Chiper, S-блок.*

Кіріспе.

Ақпараттық қауіпсіздік саласы қазіргі уақытта кез-келген ұйымда немесе жеке тұлға үшін маңызды бағыттың бір бөлігіне айналды. Әрбір интернет желісіне қосылған жеке тұлға немесе ұйымның жеке мәліметтерін (жеке сәйкестендіру нөмері (ЖСН), құпия сөздер, бұлттық технологияда сақталған құжаттар және ЭСҚ т.б) құпия ақпараттарын

шабуылдаушылардан қорғау маңызды болып саналады. Соңғы жылдары елімізде кибершабуылдаушылар пайданушылардың құпия ақпараттарына рұқсатсыз кіру арқылы әртүрлі іс-әрекеттер жүргізіп, құпия ақпараттарын ұрлауда. Осы тұрғыда құпия ақпараттарды рұқсат етілмеген шабуылдаушылардан қорғаудың ең сенімді әдістерінің бірі криптографиялық әдістер болып табылады [1-2]. Криптографиялық әдістер симметриялы және ассиметриялы деп екі топқа жіктеледі. Бұл екі алгоритмнің өз ерекешеліктері және кемшіліктері бар. Симметриялы шифрлар жылдамдығы жағынан жоғары болғанымен өз кезегінде ақпараттарды шифрлау және кері шифрлау үшін бір кілт қолданғандықтан кілт алмасу үлкен қиындықтар туғызуы мүмкін [3]. Ал ассиметриялық алгоритмдерде үлкен жай сандарды қолданғандықтан жылдамдығы төмен, бірақ кілт алмасуда өте тиімді құрастырылған. Онда құпия ақпараттарды шифрлау үшін бір кілт, ал кері шифрлау үшін басқа кілт қолданылады [4].

Ұсынылып отырған мақалада симметриялы блокты шифрлау алгоритмі болғандықтан осы бағытқа тоқталсақ. Блокты шифрлар құпия ақпараттарды белгілі бір биттік ұзындықтағы блоктарға бөліп әрбір блокпен жеке шифрлау жүргізіледі. Қазіргі қолданыстағы блокты шифрлау алгоримінің ұзындықтары 64, 128, 256 тең [5]. Блокты шифрлау алгоритмдеріне DES [6], AES [7], SM4[8], GOS T[9], Present т.б. жатқызуға болады. Блокты шифлау алгоритмдері VPN, қауіпсіз байланыс TLS, дискідегі деректерді шифрлау (itlocker,VeraCrypt), қауіпсіз хабар алмасу (Signal, Whatsapp) сияқты әртүрлі салада ақпараттарды сенімді қорғау үшін қолданылады. Блокты шифрлау алгоритмдері құпия ақпараттың мазмұнын криптографиялық түрлендірулер арқылы шабуылдаушыға түсініксіз етіп түрлендіреді.

Қазіргі блокты шифрлау алгоритмдері Киркхоффс [10] принципіне негізделген, яғни шифрдың сенімділігі шифрлау алгоритмінің құпиялылығында емес кілттің құпиялылығына тәуелді болу керек.

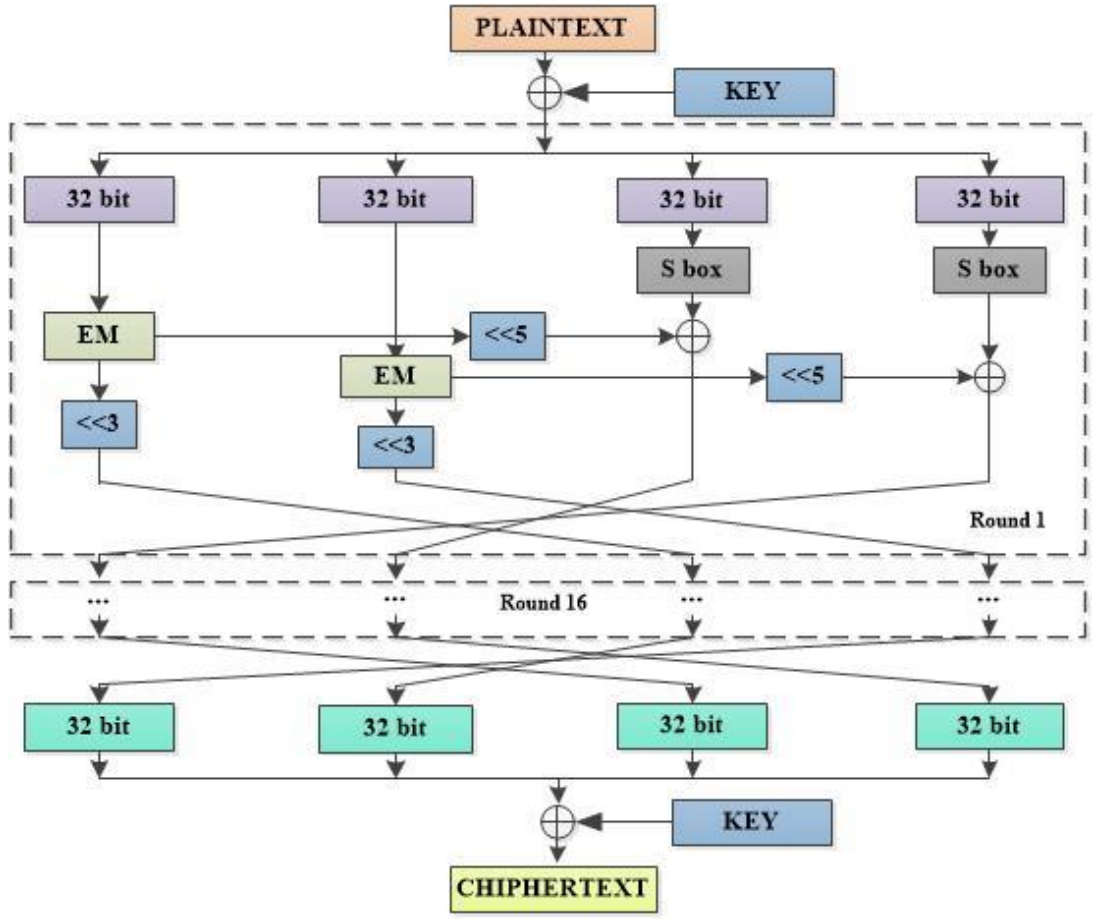
Қазіргі уақытта танымал блокты шифрлау алгоритмдерін қолдану саласын кеңейту шекті құрылғыларға негіздеп модификациясын жасаумен айналысуда, солардың бірі AES-ті сенсорлық желілерде тиімді қолдану тиімділігін арттыру және шифрлау жылдамдығын арттыру сияқты жұмыстарды қарастырған [11].

Chadi R. т.б. авторлар [12] AES, DES, 3DES, E-DES блокты шифрлау алгоритмдеріне салыстырмалы талдаулар жүргізіп, E-DES алгоритмі жоғары өнімділікке ие болатындығы дәлелдеген.

Блокты шифрлау алгоритмдері бойынша ауқымды талдау жұмыстарын жүргізген келесі [13] жұмысты атап айтуға болады, онда AES, Blowfish, IDEA сияқты шифрлау алгоритміне салыстырмалы талдау жүргізіп нәтижесін ұсынған.

Материалдар және тәсілдер.

Зерттеліп отырған «EM Chiper» блокты шифрлау алгоритмдерінің шифлау схемасы 1-суретте көрсетілген. Онда EM түрлендіру, S-блок, цикльдік жылжыту, биттік қосу операциясы және 4 байттық орын ауыстыру сияқты қарапайым түрлендіру әдістері қолданылған. Бұл әдістер алгоритмнің криптоберіктілігін арттыру мақсатында жақсы араластыру және шашырату сияқты маңызды рөлді атқарады. Алгоритмнің толық құрылымы [3] жұмыста көрсетілген.



Сурет 1 – «EM Chiper» блокты шифрлеу алгоритмінің схемасы

«EM Chiper» блокты шифрлау алгоритмінің ерекшелігі басқада блокты шифрлау алгоритмдерінде кездеспейтін EM түрлендіру операциясы қолданылды (2-сурет). EM түрлендіруі сызықты емес функция болғандықтан өз кезегінде ұсынылған алгоримнің криптоберіктілін жоғары деңгейде арттыруға мүмкіндік береді. EM түрлендіру барысында 32 биттік кіріс мәндер (ашықмәтін блоктары) таңдап алынған $p_1(x), p_2(x), \ldots, p_n(x)$ жұмыс негіздері деп аталатын келтірілмейтін көпмүшеліктердің дәрежесі бойынша бөліктерге бөлінеді. Алынған бөліктерді келесі формуладағы позициялық емес полиномиальды санау жүйесі (ПЕПСЖ) қалдықтардың тізбегі ретінде өрнектейміз:

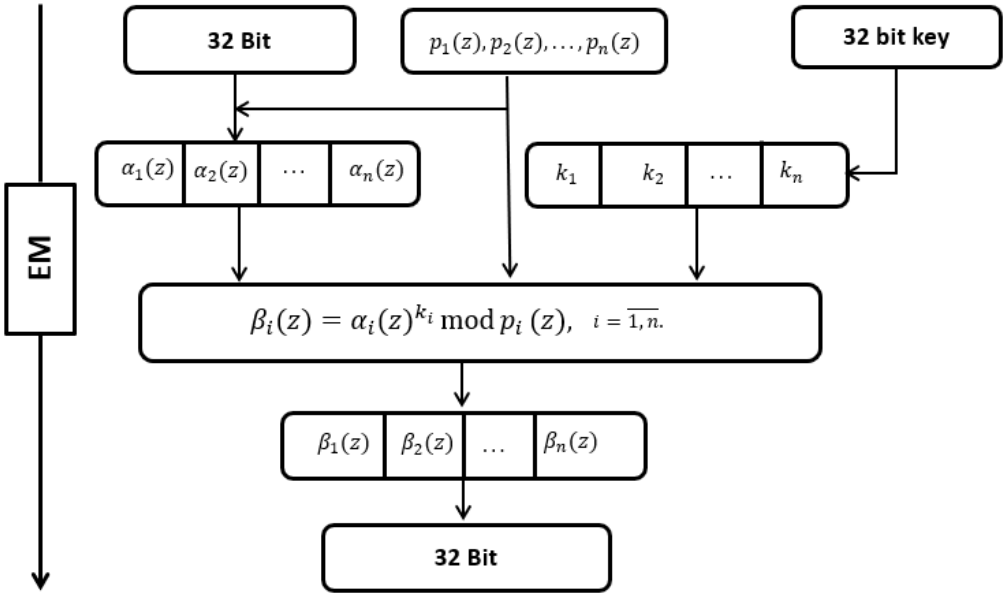
$$A(x) = a_1(x), a_2(x), \ldots, a_s(x),$$

мұндағы $a_i(x)$ - алынған бөліктер, $i = \overline{1,S}$.

Қалдықтардың тізбегіндегі әр бір бөліктерді раундтық кілттерді қолдану арқылы түрлендіру процессін төмендегідей формуламен өрнектеп аламыз:

$$b_i(x) = a_i^{k_i}(x) \bmod p_i\,(x), i = \overline{1,S}.$$

мұндағы $b_i(x)$ - шығыс мәндер (шифрмәтін) бөлігі.



Сурет 2 – EM түрлендіру операциясы

EM түрлендіру операциясы модуль бойынша дәрежеге негізделгендіктен, алгоритмнің шифрлау және керішифрлау жылдамдығына әсер ететіндігі белгілі. Бұл мәселені оңтайлы шешу үшін индекс кестесі қолданылды [3]. Сонымен қатар «EM Chiper» блокты шифрлау алгоритміне қолданылған S-блок жаңа әдіс арқылы алынды [14].

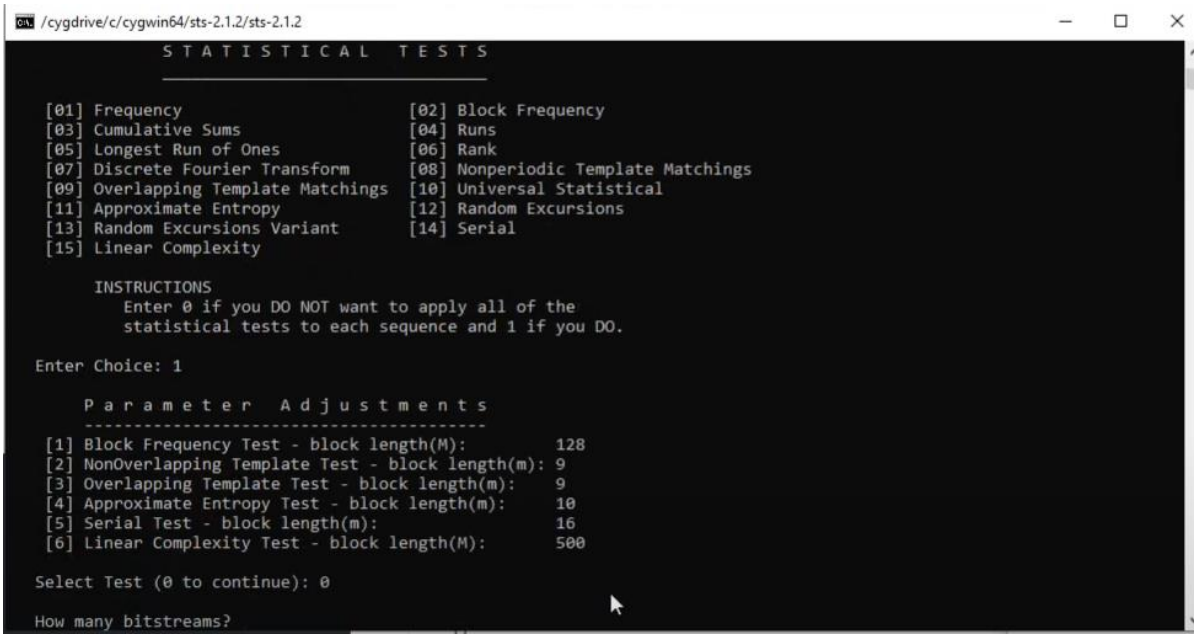
«EM Chiper» блокты шифрлау алгоритмінің криптобериктілігін анықтау үшін қолданылған әдістерге тоқталсақ.

Статистикалық талдау. Блокты шифрлау алгоритмдерінің қауіпсіздігін зерттеудің негізгі әдістерінің бірі статистикалық қауіпсіздігін талдау болып табылады [3]. Шифрлау алгоритмдерін статистикалық тұрғыдан талдау үшін National Institute of Standards and Technology (NIST) сынақтары, Д.Кнут сынақтары, Diehard сынақтары және Crypt-X сынақтары қолданылады. Бұл сынақтар шифрлау алгоритмінен алынған шифрмәтінді әртүрлі критерийлер арқылы зерттеп, осал жерлерін анықтап, статистикалық тұрғыда бағалайды [15].

Дифференциалдық криптоталдау әдісі – блокты шифрлау алгоритмдеріне қарсы пайдаланылатын криптоаналитикалық шабуылдардың бір түрі. Бұл әдіс алғаш рет DES алгоритміне қолданылып, 1990 жылдардан бастап кеңінен танымал бола бастаған және көптеген шифрлау алгоритмдерінің беріктілігін осы әдіс арқылы тексереді. Диференциалдық криптоталдау әдісі шифрлау алгоритмінің жұмыс істеу құрылымын біле отырып шабуылдаушылар кілтті анықтау ықтималдығын табады. Алгоритмге дифференциалды криптоталдау жүргізу барысында алдын ала таңдалған жұп шифрленген мәтін таңдап алынады. Шабуылдаушы $\Delta X = X_1 \oplus X_2$ ашықмәтін айырымдарын есептейді және оның нәтижесінде $\Delta Y = Y_1 \oplus Y_2$ шифрмәтіндердің айырымдары қандай болу керектігін табуға тырысады[16].

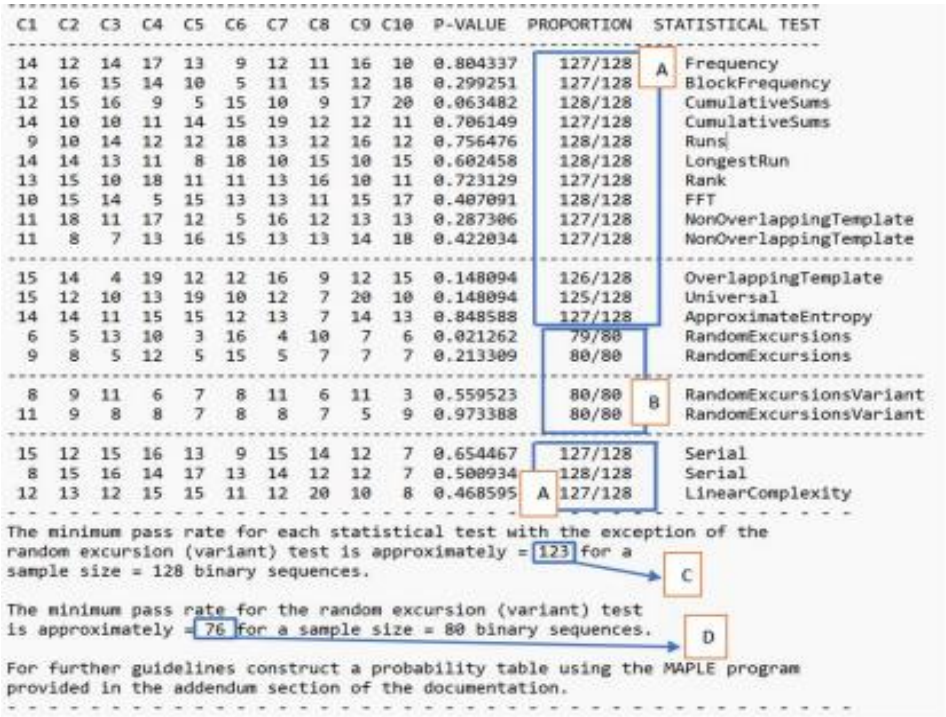
Нәтижелер мен талқылау.

Статистикалық талдау. Шифрлау алгоритмінінің статистикалық қауіпсіздігін бағалау барысында NIST сынақтары жүргізілді. Статистикалық талдау жүргізу үшін NIST ұсынған арнайы Statistical Test Suite бағдарламалық жабдықтама қолданылды (3-сурет). Бұл бағдарламаны қолдану барысында NIST ұсынған 15 статистикалық сынақтар бойынша зерттелетін шифрмәтінді кездейсоқтыққа χ^2 (хи-квадрат) критерийлері бойынша зерттеліп P – мәні анықталынады, егер P – мәні < 1 болса шифрмәтін кездейсоқ алынған деп болжаймыз.



Сурет 3 – Statistical Test Suite бағдарламасы

EM Chiper шифрлау алгоритмі арқылы алынған 1000000 бит ұзындықтағы шифрмәтін және 128 блок ұзындық таңдап алынып кездейсоқтыққа тексерілді. Statistical Test Suite бағдарламасымен тексерудің ерекшелігі әрбір 15 статистикалық сынақтар бойынша P – мәндерін есептеп қана қоймай, C1-C10 аралық интервалға бөлу арқылы әрбір интервалға қандай мән түсетіндігін анықтайды. Бұл өз кезегінде шифрмәтіннің бір қалыпты үлестірілгендігін көрсетеді. Мысалы: C1 бағанасында 0.0-0.1 аралықтағы P – мәндері 14 рет, C2 бағанасында 0.1-0.2 аралықтағы P – мәндері 12 рет кездесетіндігі, ал proportion бөлімінде 128 блок ұзындықтықтың 127-і сәтті өткендігі көрсетілген. NIST талаптарына сай алынған зерттеулерге сәйкес A бағанадағы мәндері C мәнінен үлкен болса, ал B мәндері D мәндерінен үлкен болса сынақ сәтті өтті деп есептейміз. Зерттеу нәтижесі 4-суретте көрсетілген.



Сурет 4 – NIST сынақтар нәтижесі

Диференциалдық талдау. Ұсынылып отырған «EM Chiper» алгоритмге диффересиядық талдау жүргізу үшін құрылымындағы түрлендірулерді сызықты және сызықты емес функцияларға бөліп, оларға жеке-жеке талдаулар жүргізсек. Онда сызықты функцияларға қатыстын дифференциалды талдаудың ықтималдылығын келесідей анықтаймыз:

- «XOR» операциясы үшін $\Delta y = y_1 \oplus y_2 = x_1 \oplus k \oplus x_2 \oplus k = x_1 \oplus x_2 = \Delta x$, яғни XOR операциясының кіріс мәніне бірдей мәндерді қосқаннан кіріс міндерінің айырымдары мен шығыс мәндерінің айырымдары өзгермейді;
- «XOR» опеарциясы үшін $\Delta y = y_1 \oplus y_2 = x_1 \cdot k \oplus x_2 \cdot k = (x_1 \oplus x_2) \cdot k = \Delta x \cdot k$, яғни XOR операциясының кірісіне бірдей мәндерді еселегенмен кіріс айырымдары мен шығыс айырымдарының мәндері сондай мәнге еселенеді;
- 3 қадам негізінде солға циклді жылжыту операциясы үшін: $\Delta y = y_1 \oplus y_2 = \left((x_{1,1} \oplus k_{1,1}) \cdot 2^3 \oplus (x_{1,2} \oplus k_{1,2}) \cdot 2^{29}\right) mod 2^{32} \oplus \left(\left(x_{2,1} \oplus k_{2,1}\right) \cdot 2^3 \oplus \left(x_{2,2} \oplus k_{2,2}\right) \cdot 2^{29}\right) mod 2^{32} = \left(\left(x_{1,1} \oplus x_{2,1}\right) \cdot 2^3 \oplus \left(x_{1,2} \oplus x_{2,2}\right) \cdot 2^{29}\right) mod 2^{32} = (\Delta x_1 \cdot 2^3 \oplus \Delta x_2 \cdot 2^{29}) mod 2^{32}$ теңдеу орындалады;
- 5 қадам бойынша солға циклді жылжыту операциясы үшін: $\Delta y = y_1 \oplus y_2 = \left((x_{1,1} \oplus k_{1,1}) \cdot 2^5 \oplus (x_{1,2} \oplus k_{1,2}) \cdot 2^{27}\right) mod 2^{32} \oplus \left(\left(x_{2,1} \oplus k_{2,1}\right) \cdot 2^5 \oplus \left(x_{2,2} \oplus k_{2,2}\right) \cdot 2^{27}\right) mod 2^{32} = \left(\left(x_{1,1} \oplus x_{2,1}\right) \cdot 2^5 \oplus \left(x_{1,2} \oplus x_{2,2}\right) \cdot 2^{27}\right) mod 2^{32} = (\Delta x_1 \cdot 2^5 \oplus \Delta x_2 \cdot 2^{27}) mod 2^{32}$ теңдеу орындалады;

Қорытындылай келе XOR, 3 және 5 қадам бойынша солға циклді жылжыту сызықтық функциялар үшін дифференциалдық зерттеулердің ықтималдылығы 1-ге тең болады.
Келесі сызықты емес функциялар үшін талдауларды қарастырайық.

- EM сызықты емес функциясы үшін: $\triangle \beta_i(x) = \beta_{i,1}(x) \oplus \beta_{i,2}(x) = \left(\left(\alpha_{i,1}(x)^{k_i(x)}\right) \oplus \left(\alpha_{i,2}(x)^{k_i(x)}\right)\right) mod P_i(x)$ айырымдарының кіріс мәнімен мен шығыс мәндерінің кездесулерінің үлкен ауытқуларына сәйкес келтірілмейтін көпмүшеліктерге қарай 8-ші дәреже үшін 2^{-5}, 7-ші дәреже үшін 2^{-4} және 5-ші дәреже үшін 2^{-2} тең ықтималдықты аламыз, мұндағы, $\alpha_{i,j}(x), \beta_{i,j}(x) \in \frac{GF\left(2^{\deg(k_i(x))}\right)}{P_i(x)}, i = \overline{1,4}, j = 1,2$;
- «S-блок» функциясы үшін келесі ықтималдықтарды аламыз: Таңдалған S-блок ауыстыруының зерттеу нәтижесіне сай айырымдардың кездесуі 0-ден 8-ге дейінгі аралықта болады. Әрбір кіріс мәндерінің айырымдары сәйкес шығыс мәндерінің айырымдары 8 рет кездесетін ең үлкен ауытқуы болғандықтан, $\frac{8}{256} = 0{,}03125$ ықтималдылықты таңдап аламыз.

Алгоритм құрамындағы түрлендірулердің жоғарыдағы зерттеулерін ескере отырып, ұсынылып отырған алгоритмнің 1-ші раундыдағы дифференциалды талдауды қарастырайық.

Мысалы: Ашықмәтін жұбын 0x00000000000000000000000000000001B-ге тең таңдап алайық. Сонда «EM Chiper» алгоритм негізінде 1-ші раундтан кейінгі алынған нәтижелердің айырымы 0x0000003C00000000000000000000000 тең, ал кілтті анықтаудығы жоғары ықтималдылық S-блок ауыстыруына қатысты болғандақтан $0{,}03125 = 2^{-5}$ ықтималдыққа тең.

2 - ші раундтағы айырымның нөлден өзгеше мәні 4-ші байтқа тең болғандықтан, ол EM фукциясына қатысты және кірісі 0x0000003C үшін $0{,}01887 \approx 2^{-4}$ ықтималдық болса, онда 2-раундтан кейін кілті анықтау ықтималдылығы 2^{-9} және айырымның мәні: 00000000 0000$x_{13}x_{14}$00 0000$x_{21}x_{22}x_{23}$0 00000000 тең болады.

3 - раундтағы айырымның нөлден өзгеше мәні 7-ші, 11-ші және 12-ші байт болғандықтан, оған EM фукциясыда және S-блок алмастыруы ықпал етеді. Дегенмен, екі

функциянында ауытқу міндетті түрде қатыса бермейді – тек қайсысының ауытқуы жоғары функцияны таңдаймыз. Біздің жағдайда ЕМ фукциясының ауытқуы жоғары болғандықтан дәл сол функцияны таңдаймыз. Сол себепті, 3-ші раундтан кейін анықтау ықтималдылығы 2^{-13} болады. Дәл осы тәртіппен зерттеу арқылы кілтті анықтау ықтималдықтар кестесін толтырамыз (Кесте 1).

Кесте 1 - Әр раундтағы кілтті анықтаудың ықтималдық нәтижесі

Раундтар №		**Айырым ықтималдығы**	**Раундтар №**		**Айырым ықтималдығы**
1	кіріс	1	9	Кіріс	2^{-54}
	шығыс	2^{-5}		Шығыс	2^{-63}
2	Кіріс	2^{-5}	10	Кіріс	2^{-63}
	Шығыс	2^{-9}		Шығыс	2^{-72}
3	Кіріс	2^{-9}	11	Кіріс	2^{-72}
	Шығыс	2^{-13}		Шығыс	2^{-81}
4	Кіріс	2^{-13}	12	Кіріс	2^{-81}
	Шығыс	2^{-18}		Шығыс	2^{-90}
5	Кіріс	2^{-18}	13	Кіріс	2^{-90}
	Шығыс	2^{-27}		шығыс	2^{-99}
6	Кіріс	2^{-27}	14	Кіріс	2^{-99}
	Шығыс	2^{-36}		Шығыс	2^{-108}
7	Кіріс	2^{-36}	15	Кіріс	2^{-108}
	Шығыс	2^{-45}		Шығыс	2^{-117}
8	Кіріс	2^{-45}	16	Кіріс	2^{-117}
	шығыс	2^{-54}		шығыс	2^{-126}

Енді осы зерттеулерге негізінде басқада белгілі блокты шифрлау алгоритмдерімен салыстырмалы талдаулар жүргізіліп, нәтижесі 2-кестеде көрсетілді.

Кесте 2 - Блокты шифрлардың дифференциалды талдауға қарсы тұру тұрақтылығы

Алгоритмдер	**Блок өлшемі**	**Кілт ұзындығы**	**Раундтар саны**	**Дифференциалды талдауға қарсы тұрақтылығы**	**Кілтті табу ықтималдығы**
Camellia 128	128 бит	128/192/256 бит	18/24	Жоғары дифференциалға төзімді	Өте төмен $\approx 2^{-126}$
AES 128	128 бит	128 бит	10	Жоғары дифференциалға төзімді	Өте төмен $\approx 2^{-126}$ $- 2^{-254}$
3 DES	64 бит	112/168 бит	48	Жақсы	Орташа $\approx 2^{-90}$
IDEA	64 бит	128 бит	8,5	Төзімді	Төмен $\approx 2^{-112}$
EM Chiper	128 бит	128 бит	16	Жоғары дифференциалға төзімді	Өте төмен $\approx 2^{-126}$

AES NIST стандарты ретінде бекітілген ең қауіпсіз блокты шифрлау алгоритм болып табылады. AES-тің AES-128, AES-192, AES-256 нұсқасы бар олардың барлығы дифференциалды шабуылдарға өте жоғары деңгейде төзімді. Кілтті табу ықтималдығы 2^{-126} -ден бастап 2^{-254} -ке дейін төмендейді. Қазіргі зертеулерде AES-ке қарсы дифференциалды шабуыл жүргізілген жоқ. Ал ұсынылып отырған EM Chiper алгоритміне осы аралыққа дейін басқада талдаулар жүргізіліп нәтижелері Scopus, комитет ұсынған журналдарға нәтижелері жарияланған. Бұл мақалада статистикалық зертеулері NIST ұсынған жаңа бағдарлама көмегімен зерттеліп нәтижелері алынды. Сонымен қатар әр раундтар бойынша дифференциалға төзімділік ықтималдылығы талданып, нәтижелері ұсынылған. Зерттеулер негізінде өте жоғары нәтиже көрсетілді.

Қорытынды.

Блокты шифрлау ақпараттарды сенімді қорғауда, әсіресе деректерді шифрлау, электронды байланыс цифрлық жүйелерді қорғау саласында кең қолданыста. Блокты шифрлардың өзектілігі төзімділігі жоғары, шифрлау жылдамдығы жоғары және әртүрлі қосымшаларға оңтайлы енгізілумен тығыз байланысты. Ұсынылған EM Chiper алгоритміне жан жақты талдаулар жүргізіліп, нәтижелері зерттелеген. Бұл мақалада алгоритмге дифференциалды талдау жүргізіліп нәтижелері ұсынылды. Алынған нәтижелерге сай EM Chiper алгоритмі жоғары дифференциалға төзімді екендігі айқындалды. Ұсынылған EM Chiper алгоритмін TLS/SSL, IPSec, VPN, Disk Encryption, Messaging apps (WhatsApp, Signal) т.б. қауіпсіздік хаттамаларында және құпия ақпараттарды рұқсат етілмеген пайдаланушылардан сенімді қорғау мақсатында қолдануға болады.

Әдебиеттер тізімі

1. Kapalova, N., & Haumen, A. (2018). The model of encryption algorithm based on non-positional polynomial notations and constructed on an SP-network. Open Engineering, 8(1), 140–146. https://doi.org/10.1515/eng-2018-0013

2. Nyssanbayeva, B. S., Kapalova, N., & Haumen, A. (2016). Modified symmetric block encryption-decryption algorithm based on modular arithmetic. Proceedings of the International Conference on Wireless Communications, Network Security and Signal Processing (WCNSSP2016) (pp. 263–265).

3. Kapalova, N., Khompysh, A., Arici, M., & Algazy, K. (2020). A block encryption algorithm based on exponentiation transform. Cogent Engineering, 7(1). https://doi.org/10.1080/23311916.2020.1788292

4. Sabitha S, Binitha V Nair "Survey on Asymmetric Key Cryptographic Algorithms" International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Volume 7, Issue 2, pp.404-408, doi : https://doi.org/10.32628/IJSRSET207292

5. Hasan, S. H., Trigui, M. S., & Ali Alquraishee, A. G. (2014). Block Cipher Based Cryptographic Algorithm For Data Security. International journal of management & information technology, 8(3), 1424–1429. https://doi.org/10.24297/ijmit.v8i3.1978

6. G., Renuka, Usha Shree V., and Chandra Sekhar Reddy P. "Comparison of AES and DES Algorithms Implemented on Virtex-6 FPGA and Microblaze Soft Core Processor." International Journal of Electrical and Computer Engineering (IJECE) 8, no. 5 (2018): 3544–49. https://doi.org/10.11591/ijece.v8i5.pp3544-3549.

7. Gaur, Paavni. "AES Image Encryption (Advanced Encryption Standard)." International Journal for Research in Applied Science and Engineering Technology 9, no. 12 (2021): 1357–63. http://dx.doi.org/10.22214/ijraset.2021.39542.

8. Kongsheng L, Yonghua Zh, Chunzhi M, and Jianhao Ch. 2024. Research on New Encryption Technology Based on SM4 Symmetry. In Proceedings of the International Conference on Image Processing, Machine Learning and Pattern Recognition (IPMLP '24). Association for

Computing Machinery, New York, NY, USA, 459–463. https://doi.org/10.1145/3700906.3700979

9. Babenko, Ludmila & Evgeniya, Ishchukova & Maro, Ekaterina. (2012). Research about strength of GOST 28147-89 encryption algorithm. pp.138-142. Doi:10.1145/2388576.2388595.

10. R.Biyashev , S. Nyssanbayeva, N.Kapalova, The Key Exchange Algorithm on Basis of Modular Arithmetic, Proceedings of International Conference on Electrical, Control and Automation Engineering (ECAE2013), Hong Kong— Lancaster, U.S.A.: DEStech Publications, 2013, pp.16-21

11. Yang Z. Wireless sensor network security encryption based on AES module optimization design. *Journal of Computational Methods in Sciences and Engineering*. 2025;25(1):766-778. doi:10.1177/14727978251321651

12. Chadi RIMAN, Pierre E. ABI-CHAR. Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey. Information Security and Computer Fraud. Vol. 3, No. 1, 2015, pp 1-7. https://pubs.sciepub.com/iscf/3/1/1

13. Sharma, Mukta. (2016). Comparative Analysis of Block Key Encryption Algorithms. International Journal of Computer Applications. 145. 26-35. 10.5120/ijca2016910656.

14. Khompysh A., Algazy K., Kapalova N., Sakan K., & Dyusenbayev D. (2024). Statistical properties of the pseudorandom sequence generation algorithm. Scientific Journal of Astana IT University, 18, 107–119. https://doi.org/10.37943/18LYCW2723

15. Бабенко, Л. К., & Ищукова, Е. А. (2011). Дифференциальный криптоанализ алгоритма ГОСТ 28147-89. Известия Южного федерального университета. Технические науки, 125 (12), 120-130.

References

1. Kapalova, N., & Haumen, A. (2018). The model of encryption algorithm based on non-positional polynomial notations and constructed on an SP-network. Open Engineering, 8(1), 140–146. https://doi.org/10.1515/eng-2018-0013

2. Nyssanbayeva, B. S., Kapalova, N., & Haumen, A. (2016). Modified symmetric block encryption-decryption algorithm based on modular arithmetic. Proceedings of the International Conference on Wireless Communications, Network Security and Signal Processing (WCNSSP2016) (pp. 263–265).

3. Kapalova, N., Khompysh, A., Arici, M., & Algazy, K. (2020). A block encryption algorithm based on exponentiation transform. Cogent Engineering, 7(1). https://doi.org/10.1080/23311916.2020.1788292

4. Sabitha S, Binitha V Nair "Survey on Asymmetric Key Cryptographic Algorithms" International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Volume 7, Issue 2, pp.404-408, doi : https://doi.org/10.32628/IJSRSET207292

5. Hasan, S. H., Trigui, M. S., & Ali Alquraishee, A. G. (2014). Block Cipher Based Cryptographic Algorithm For Data Security. International journal of management & information technology, 8(3), 1424–1429. https://doi.org/10.24297/ijmit.v8i3.1978

6. G., Renuka, Usha Shree V., and Chandra Sekhar Reddy P. "Comparison of AES and DES Algorithms Implemented on Virtex-6 FPGA and Microblaze Soft Core Processor." International Journal of Electrical and Computer Engineering (IJECE) 8, no. 5 (2018): 3544–49. https://doi.org/10.11591/ijece.v8i5.pp3544-3549.

7. Gaur, Paavni. "AES Image Encryption (Advanced Encryption Standard)." International Journal for Research in Applied Science and Engineering Technology 9, no. 12 (2021): 1357–63. http://dx.doi.org/10.22214/ijraset.2021.39542.

8. Kongsheng L, Yonghua Zh, Chunzhi M, and Jianhao Ch. 2024. Research on New Encryption Technology Based on SM4 Symmetry. In Proceedings of the International Conference on Image Processing, Machine Learning and Pattern Recognition (IPMLP '24). Association for Computing Machinery, New York, NY, USA, 459–463. https://doi.org/10.1145/3700906.3700979

9. Babenko, Ludmila & Evgeniya, Ishchukova & Maro, Ekaterina. (2012). Research about strength of GOST 28147-89 encryption algorithm. pp.138-142. Doi:10.1145/2388576.2388595.

10. R.Biyashev , S. Nyssanbayeva, N.Kapalova, The Key Exchange Algorithm on Basis of Modular Arithmetic, Proceedings of International Conference on Electrical, Control and Automation Engineering (ECAE2013), Hong Kong— Lancaster, U.S.A.: DEStech Publications, 2013, pp.16-21

11. Yang Z. Wireless sensor network security encryption based on AES module optimization design. *Journal of Computational Methods in Sciences and Engineering*. 2025;25(1):766-778. doi:10.1177/14727978251321651

12. Chadi RIMAN, Pierre E. ABI-CHAR. Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey. Information Security and Computer Fraud. Vol. 3, No. 1, 2015, pp 1-7. https://pubs.sciepub.com/iscf/3/1/1

13. Sharma, Mukta. (2016). Comparative Analysis of Block Key Encryption Algorithms. International Journal of Computer Applications. 145. 26-35. 10.5120/ijca2016910656.

14. Khompysh A., Kapalova N., Algazy K., Dyusenbayev D., Sakan K. Design of substitution nodes (S-Boxes) of a block cipher intended for preliminary encryption of confidential information. Cogent Engineering, 2022, vol. 9 (1), pp. 1-14, https://doi.org/10.1080/23311916.2022.2080623

15. Khompysh A., Algazy K., Kapalova N., Sakan K., & Dyusenbayev D. (2024). Statistical properties of the pseudorandom sequence generation algorithm. Scientific Journal of Astana IT University, 18, 107–119. https://doi.org/10.37943/18LYCW2723

16. Babenko, L. K., & Ishchukova, E. A. (2011). Differential cryptanalysis of the algorithm GOST 28147-89. Bulletin of the Southern Federal University. Technical sciences, 125 (12), 120-130.

ИССЛЕДОВАНИЕ КРИПТОСТОЙКОСТИ АЛГОРИТМА БЛОЧНОГО ШИФРОВАНИЯ «EM CHIPER»

Аннотация. *Среди криптографических алгоритмов для надежной защиты конфиденциальной информации от несанкционированных пользователей используются алгоритмы блочного шифрования. Во многих странах установлены собственные стандарты алгоритмов блочного шифрования. Это, в свою очередь, позволяет обеспечить надёжную защиту информации. И это при том, что в Казахстане не утверждены стандарты на подобные алгоритмы защиты информации. Создание алгоритмов блочного шифрования и исследование их криптографической стойкости всегда являются одними из самых актуальных вопросов. В данной статье представлены результаты дифференциального и статистического анализа алгоритма блочного шифрования «EM Chiper». Одним из основных методов исследования стойкости алгоритмов блочного шифрования является статистический анализ стойкости. Если в ходе преобразований, обычно используемых в блочных шифрах, успешно реализовано хорошее смешивание и рассеивание, то можно добиться высокого уровня криптографической стойкости защиты алгоритма. Для проведения статистического анализа алгоритм был реализован программно и получены шифртексты различной длины. Согласно проведенным исследованиям статистический анализ предложенного алгоритма показал высокие результаты, то есть согласно требованиям, рекомендуемым NIST, было определено, что значения в столбце A больше значений в C, а значения в B больше значений в D. Результаты дифференциального анализа показали, что предложенный алгоритм обладает высокой криптографической стойкостью. То есть вероятность нахождения ключа из раунда 16 составляет* 2^{-126}. *Кроме того, в статье проведён сравнительный анализ результатов дифференциального анализа алгоритмов подписи, и установлено, что они показали сопоставимые результаты с известными алгоритмами Camellia 128 и AES 128. В будущих*

работах будет проведено комплексное исследование криптографической стойкости других алгоритмов, а результаты будут представлены в виде статьи.

Ключевые слова. *Блочный шифр, шифр, криптография, ключ, дифференциальный криптоанализ, статистический анализ, EM Chiper, S-блок.*

STUDY OF CRYPTOCURRENCY OF THE BLOCK CIPHER ALGORITHM «EM CHIPER»

Abstract. *Among cryptographic algorithms, block encryption algorithms are used to reliably protect confidential information from unauthorized users. Many countries have established their own standards for block encryption algorithms. This, in turn, ensures reliable protection of information. And this is despite the fact that in Kazakhstan, standards for such information protection algorithms have not been approved. There, the creation of block encryption algorithms and the study of their cryptographic strength are always among the most pressing issues. This article presents the results of differential and statistical analysis of the block encryption algorithm «EM Chiper». One of the main methods for studying the strength of block encryption algorithms is statistical analysis of strength. If good mixing and diffusion is successfully implemented during the transformations commonly used in block ciphers, then a high level of cryptographic security of the algorithm can be achieved. To conduct statistical analysis, the algorithm was implemented in software and ciphertexts of various lengths were obtained. According to the conducted research, the statistical analysis of the proposed algorithm showed high results, that is, according to the requirements recommended by NIST, it was determined that the values in column A are greater than the values in C, and the values in B are greater than the values in D. The results of the differential analysis showed that the proposed algorithm has high cryptographic strength. That is, the probability of finding the key from round 16 is* 2^{-126}*. In addition, the article conducted a comparative analysis of the results of the differential analysis of signature algorithms, and found that they showed comparable results with the well-known Camellia 128 and AES 128 algorithms. In future works, a comprehensive study of the cryptographic strength of other algorithms will be conducted, and the results will be presented in the form of an article.*

Keywords. *Block cipher, cipher, cryptography, key, differential cryptanalysis, statistical analysis, EM Chiper, S-block.*

Авторлар туралы мәлімет

Хомпыш Ардабек	PhD, Нұр-Мүбарак Египет ислам мәдениеті университеті, Алматы, Қазақстан, Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан, E-mail: ardabek@mail.ru
Сақан Қайрат Сақанұлы	PhD, Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан, E-mail: kairat_sks@mail.ru
Алғазы Күнболат	PhD, Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан, E-mail: kunbolat@mail.ru
Абишева Ақмарал Жолсеитовна	Абай атындағы Қазақ Ұлттық Педагогикалық университеті, Алматы, Қазақстан, аға оқытушы, E-mail: ak_maral@mail.ru

Сведения об авторах

Хомпыш Ардабек	PhD, Египетский университет исламской культуры «Нур-Мубарак», Алматы, Казахстан, Институт информационных и вычислительных технологий, Алматы, Казахстан, E-mail: ardabek@mail.ru
Сакан Кайрат	PhD, Институт информационных и вычислительных технологий, Алматы, Казахстан, E-mail: kairat_sks@mail.ru
Алгазы Кунболат	PhD, Институт информационных и вычислительных технологий, Алматы, Казахстан, E-mail: kunbolat@mail.ru
Абишева Акмарал Жолсеитовна	Казахский национальный педагогический университет имени Абая, Алматы, Казахстан, старший преподаватель, E-mail: ak_maral@mail.ru

Information about the authors

Khompysh Ardabek	PhD, Egyptian University of Islamic Culture "Nur-Mubarak", Almaty, Kazakhstan, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, E-mail: ardabek@mail.ru
Sakan Kairat	PhD, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, E-mail: kairat_sks@mail.ru
Algazy Kunbolat	PhD, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, E-mail: kunbolat@mail.ru
Abisheva Akmaral Zh.	Kazakh National Pedagogical University named after Abaya, Almaty, Kazakhstan, senior lecturer, E-mail: ak_maral@mail.ru