Институт информационных и вычислительных технологий МОН РК

Казахский Национальный Университет имени аль-Фараби

Университет Туран

Люблинский технический университет, Польша

«Ғылым ордасы»

МАТЕРИАЛЫ

IV международной научно-практической конференции "Информатика и прикладная математика", посвященной 70-летнему юбилею профессоров Биярова Т.Н., Вальдемара Вуйцика и 60-летию профессора Амиргалиева Е.Н. 25-29 сентябрь 2019, Алматы, Казахстан

Часть 2

Алматы 2019

УДК 378 (063)
ББК 74.58
И74

И 74 **Информатика и прикладная математика:** Мат. IV Межд. науч. конф. (25-29 сентября 2018 г.). Часть 2. – Алматы, 2019. – 647 с.

ISBN 978-601-332-384-8

В сборнике опубликованы доклады, представленные по 4 секциям от Республики Казахстан, Российской Федерации, США, Латвии, Польши, Республики Беларусь, Украины, Азербайджана, Узбекистана, Японии, Кореи, Ирана, Португалии, Испании, Великобритании, Греции, Кыргызской Республики и других.

Рассмотрены актуальные вопросы в области математики, информатики и управления: математического моделирования сложных систем и бизнес-процессов, исследования и разработки защищенных и интеллектуальных информационных и телекоммуникационных технологий, математической теории управления, технологий искусственного интеллекта.

Материалы сборника предназначены для научных работников, докторантов и магистрантов, а также студентов старших курсов.

УДК 378 (063)
ББК 74.58

ISBN 978-601-332-384-8

Графикалық және бағалау статистикалық тесттерінен алынған тізбектің статистикалық сипаттамаларын талдау нәтижелері алынды. Зерттелген генератордың сапасын бағалау нәтижесінде алынған псевдокездейсоқ тізбектер жақсы статистикалық қасиеттерге ие екендігі анықталды.

Пайдаланылған әдебиеттер тізімі

1. Нысанбаева С.Е., Капалова Н.А, Алгазы К.Т. и др. / Отчет по НИР «Разработка системы управления криптографическими ключами» ПГФ 2018-2020, № госрегистрации 0118РК00117.
2. Объект авторского права под названием «Генератор псевдослучайной последовательности PSG1.1/ Бияшев Р. Г., Нысанбаева С. Е., Капалова Н. А., Дюсенбаев Д.С., Алғазы К.Т.; опубл. 16.04.2019, Бюл. № 3619. - 2 с.
3. Нысанбаева С.Е., Капалова Н.А., Дюсенбаев Д.С., Алгазы К.Т. Исследования статистических свойств разработанного генератора псевдослучайных последовательностей // Материалы научной конференции Института информационных и вычислительных технологий МОН РК «Современные проблемы информатики и вычислительных технологий». – Алматы, 2018. – С. 210-217.
4. Капалова Н.А., Алгазы К.Т., Самрат С.М. Криптоалгоритмдердің статистикалық қауіпсіздігін зерттеу // Материалы научной конференции Института информационных и вычислительных технологий МОН РК «Современные проблемы информатики и вычислительных технологий (29-30 июня 2017 г.)». – Алматы, 2017. – С. 108-113.
5. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: «КУДИЦ-ОБРАЗ», 2003. – 240 с.

ЕМ ТҮРЛЕНДІРУ ӘДІСІ НЕГІЗІНДЕ ЖАСАЛҒАН БЛОКТЫ ШИФРЛЕУ АЛГОРИТМІНЕ ЖҮРГІЗІЛГЕН БАҒАЛАУ ТЕСТТЕРІ

Капалова Н.А., Хомпыш А., Алгазы К.Т.
E-mail: nkapalova@mail.ru, ardabek@mail.ru, kunbolat@mail.ru
ҚР БжҒМ Ақпараттық және есептеуіш технологиялар институты

Аңдатпа. *Мақалада ақпаратты криптографиялық қорғаудың жаңа блоктық шифрлеу алгоритімі ұсынылады. Осы алгоритмнің құрама бөлігі болып табылатын жаңа ЕМ (exponentiation modul) түрлендіру әдісі сипатталған. Шифрлеу алгоритмінің жылдамдығын арттыру үшін позициялық емес полинимиалды санау жүйесі және жұмыс негіздерінің индекс кестесі қолданылады. Алгорим бойынша алынған шифрмәтіндер статистикалық қауіпсіздікке тексерілді, тестілеу нәтижелері сарапталды.*

Кілттік сөздер: *Қалдықтар классы, позициялық емес санау жүйесі, кілт, ашықмәтін, шифрлау, дешифрлау, индекс кестесі, мультипликативті топ.*

Кіріспе. Кез-келген мемлекеттің даму стратегиясында басым бағытарының бірі ұлттық қауіпсіздік екендігін ескерсек онда оның ең маңызды элементтерінің бірі ақпараттық қауіпсіздік болып табылады. Сондықтан ақпараттық жүйелерді қауіпсіз және тиімді өңдеуді дамыту әр бір мемлекеттің басым бағыттары бірі болып табылады [1]. Ақпараттық қауіпсіздіктің жаңа технологияларын құру мәселесін шешу, бір жағынан өңдеудің жоғары жылдамдығын және ақпараттың үлкен көлемін беруді, ал екінші жағынан оған қолжетімділікті шектеп, ақпаратты қорғаудың қажетті деңгейін қамтамасыз ету қажет.

Сондықтан заманауи талаптарға сай келетін ақпараттық қауіпсіздік құралдарын құру өзекті мәселелердің бірі. Бұл мәселелерді шешудің көптеген әдістер бар солардың ең тиімді әдістерінің бірі криптографиялық әдістер, яғни криптографиялық қорғау жүйелерін пайдалану. Ақпаратты криптографиялық қорғау әдістері функционалды міндеттеріне байланысты сан алуан. Мысалы, үлкен көлемді ақпаратты үлкен жылдамдықта шифрлеу [2]. Мақалада қазіргі таңдағы ақпараттық қорғау саласының өзекті болып саналатын шифрлеу алгоритмінің бір моделін құрастыру мәселелері қарастырылған. ЕМ түрлендіру әдісі негізінде жаңа блокты шифрлеу алгоритмі ұсынылды. Алгоритмнің статистикалық қауіпсіздігін бағалау үшін алгоритм жүзеге асырылып, алынған шифрмәтіндер статистикалық тестермен бағаланды.

ЕМ түрлендіру әдісі негізінде жасалынған блокты шифрлеу алгоритмі

Жасалынып отырған шифрлеу алгоритмін әзірлеу кезінде біз Галуа $GF(2^v)$ өрісінде дәрежеге шығару операциясына негізделген позициялық емес полиномальды санау жүйесінде жұмыс істейтін ЕМ (exponentiation modul) түрлендіру әдісі, S-box ауыстыру кестесі қолданылды. Барлық қолданылған әдістер төменде сипатталған. Ұсынылып отырған блокты шифрлеу/дешифрлеу алгоритмі 1,2-суретте көрсетілген. Шифрлеуден бұрын барлық кіріс деректері 128 битке бөлінеді де оған 128 биттегі кілт модуль екі бойынша қосылады, егер кіріс деректерінің соңғы блогі 128-биттен кем болса, онда блок нольдермен толтырлады, кейін ол дешифрлеу барысында алынып тастасталады. 128 биттік кіріс деректері 32 биттен 4 ішкі блокқа бөлінеді, осы ішкі блоктар бойынша шифрлеу процессі жүргізіледі.

ЕМ (exponentiation modul) түрлендіру әдісі. Кеңейтілген Галуа $GF(2^v)$ өрісінде дәрежеге шығару операциясына негізделген позициялық емес полиномиальды санау жүйесінде (ПЕПСЖ) жұмыс істейтін ЕМ (exponentiation modul) түрлендіру әдісі үш кезеңнен тұрады:

- жұмыс негіздер жүйесін құру және олардың орналасу ретін таңдау;
- раундық кілттерді жасау;
- кіріс деректерін түрлендіру және кері түрлендіру.

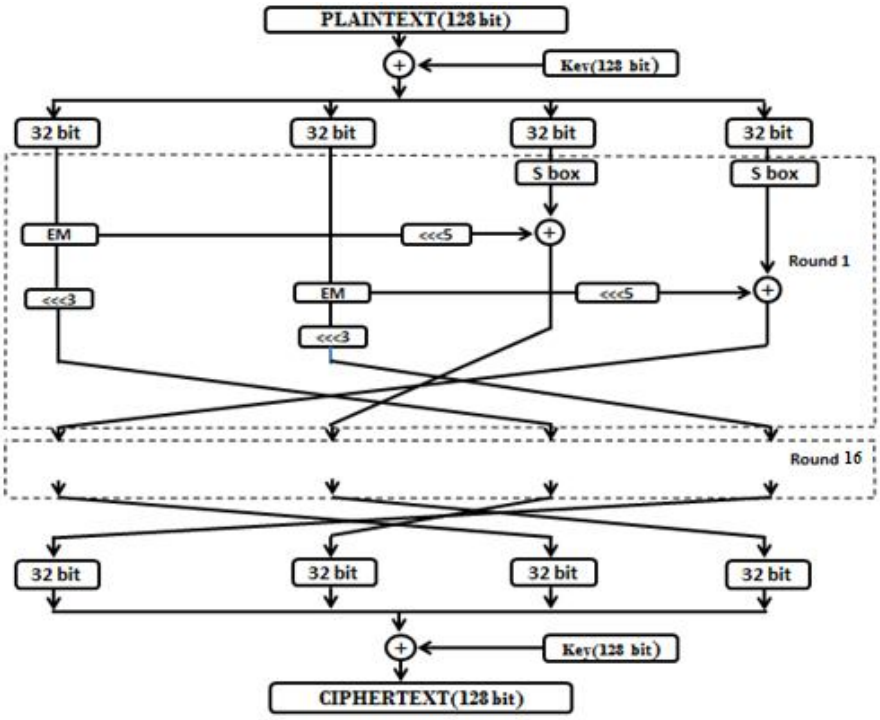
Бірінші кезең. Жұмыс негіздерін таңдап алу кезеңін қарастырайық. Ол үшін екілік тізбектегі келтірілмейтін көпмүшеліктердің сәйкесінше n_1 дәрежесінің саны m_1-ге, n_2 дәрежесінің саны m_2 -ге, n_S дәрежесінің саны m_S -ге тең болсын.

Онда жұмыс негіздерінің ең үлкен дәрежесі $H-$қа тең және m_i, $i=\overline{1,S}$-ке дейінгі дәрежелі жұмыс негіздерін таңдау кезеңдерінде (1) теңдікті қанағаттандыратындай алгебралық теңдеудің барлық ықтималды шешімдерін табамыз

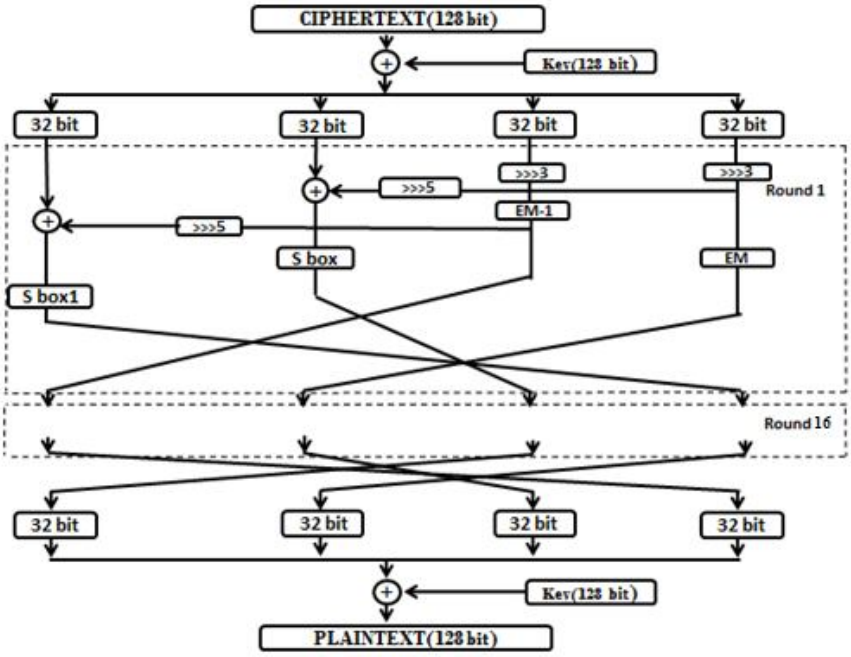
$$k_1m_1+k_2m_2+...+k_Sm_S=H. \tag{1}$$

мұндағы $0\le k_i\le n_i$, $i=\overline{1,S}$-белгісіз коэффициент, k_i - таңдап алынған m_i дәрежелі келтірілмейтін көпмүшеліктердің саны, n_i-барлық m_i дәрежелі келтірілмейтін көпмүшеліктердің саны, мұндағы $1\le m_i\le H,$ онда барлық жұмыс негіздерінің саны мынаған тең [3]:

$$S=k_1+k_2+...+k_S. \tag{2}$$



1-сурет. Модуль бойынша дәреже негізіндегі блокты шифрлеу алгоритм схемасы



2-сурет. Модуль бойынша дәреже негізіндегі блокты дешифрлеу алгоритм схемасы

Екінші кезең. Кеңейтілген Галуа өрісінде дәрежеге шығару операциясына негізінделген түрлендіру әдісін жүзеге асыру үшін k_i және k_i^{-1} мәнін псевдокездейсоқ тізбектер генераторының (ПКТГ) көмегімен аламыз:

- тізбекті түзу;
- алынған екілік тізбекті таңдалған жұмыс негіздерінің дәрежелеріне сәйкес бөлшектеу;
- екілік жүйедегі тізбектерді ондық жүйеге ауыстыру;
- алынған k_i мәнді ЕҮОБ(k_i, $p^{ord(p_i(x)}-1$)=1 болатындындай таңдаймыз.

Үшінші кезең. Модуль бойынша дәрежеге шығару операциясын пайдалану негізінде деректерді шифрлеу жылдамдығы көп уақытты талап ететіндігі белгілі. Алайда, бұл процедураның есептеу уақытын жылдамдату үшін ПЕПСЖ-ні қолдану орынды [4].

Ұсынылып отырған түрлендіру әдісінде кіріс деректері 128 ұзындықтағы биттер түрінде берілгендіктен. Оны 32 ұзындықтағы блоктарға бөліп, әр блокпен жұмыс жасаймыз. Әрбір 32 ұзындықтағы блок жұмыс негіздерінің дәрежесі бойынша бөліктерге бөлінеді. Алынған бөлікті (3) формуладағы ПЕПСЖ-дегі қалдықтардың тізбегі ретінде өрнектейміз.

$$A(x)=a_1(x),a_2(x),...,a_s(x), \tag{3}$$

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

(3) формула бойынша бөлініп алынған блоктарды түрлендіру формуласын төмендегідей өрнектейміз [5]:

$$b_i(x) = a_i^{k_i}(x) \bmod p_i(x), \qquad i = \overline{1,S}. \tag{4}$$

(4) формуласы бойынша алынған шифрмәтіндер жүйесі келесідей өрнектеледі:

$$B(x) = (b_1(x), b_2(x), ..., b_s(x)). \tag{5}$$

Онда керітүрлендіру мынадай түрде болады:

$$a_i(x) = b_i^{k_i^{-1}}(x) \bmod p_i(x). \tag{6}$$

Алынған ашық мәтіндердер жиыны келесі формуламен өрнектеледі:

$$A(x) = a_1(x), a_2(x), ..., a_s(x). \tag{7}$$

Ұсынылған алгоритмде әрбір қолданылатын кілттің керісін есептейміз:

$$k_i \cdot (k_i)^{-1} \equiv 1 \bmod (p^{\deg(p_i(x))} - 1), \ i = \overline{1,S}. \tag{8}$$

Қолданылып отырған ЕМ түрлендіру әдісінде дәрежеге шығару амалы шифрлеу кезінде көп уақыт алатыны белгілі. Бірақ ұсынылып отырған алгоритмде дәрежені есептеу индекс кестесін құру арқылы орындап отырғандықтан есептеу жылдамдығы артады [6]. ЕМ түрлендіруінде таңдап алған жұмыс негіздері $p_i(x)$ бойынша индекс кестесін келесі заңдылық бойынша толтырамыз.

$$a(x) = \alpha^j \bmod p_i(x), \ j = \overline{0, (2^{\deg(p_i(x))} - 2)} \tag{9}$$

Мұнда, α - $GF(2^v)$ өрісіндегі мультипликативті топты тудырушы элемент.

Мысалы: $GF(2^v)$ өрісіндегі жұмыс негіздерінің бірі $p(x) = x^3 + x + 1$, келтірілмейтін көпмүшеліктің индекс кестесін қарастырайық (1-кесте).

Таңдалған жұмыс негіздерінің индекс кестесіне сәйкес келесі математикалық теңдеуді енгізейік.

$$l = \underset{\alpha}{ind}\, a_i(x) \bmod p_i(x), \tag{10}$$

мұндағы l - $a(x)$-тің α-бойынша алынған дәрежесі немесе индексі (ind). Ондай болатын болса онда (4) формулаға келісідей өзгерту енгіземіз:

$$b_i(x) = (\alpha^l)^{k_i} \bmod p_i(x) = (\alpha(x)^{(lk_i) \bmod (2^{\deg(p_i(x))}-1)}) \bmod p_i(x). \quad (11)$$

1-кесте. $p(x) = x^3 + x + 1$ жұмыс негіздерінің индекс кестесі

Индексті берілуі ind	Көпмүшелік түрде берілуі $a(x)$
α^{∞}	0
α^0	1
α^1	x
α^2	x^2
α^3	$x+1$
α^4	$x^2 + x$
α^5	$x^2 + x + 1$
α^6	$x^2 + 1$

Кері түрлендіру процессіндеде k_i-дің орынына кері элементі $(k_i)^{-1}$-ді қолданамыз:

$$l = \underset{\alpha}{ind}\, b_i(x) \bmod p_i(x) \quad (12)$$

$$a_i(x) = (\alpha^l)^{k_i^{-1}} \bmod p_i(x) = (\alpha^{(lk_i^{-1}) \bmod (2^{\deg(p_i(x))}-1)}) \bmod p_i(x) \quad (13)$$

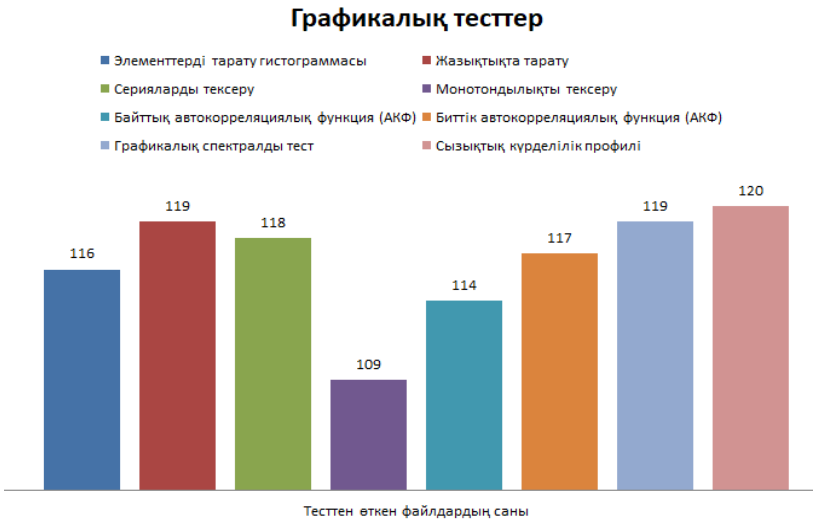
Шифрлеу алгоритмінің статистистикалық қауіпсіздігін бағалау үшін жүргізілген тестлеу. Шифрлеу алгоритмінің моделін іске асыру үшін с++ тілінде бағдарламасы әзірленді. Ұсынылған алгоритмнің статистикалық қауіпсіздігін зерттеу үшін шифрмәтінге бағалау тестері жасалынып талдау жүргізілді.

Ұсынылған алгоритмге тестілеу жүргізу үшін:

- әр түрлі өлшемдегі 10 файл;
- 12 толық кілт және әр түрлі жұмыс негіздері қолданылды.

Ұсынылған ЕМ алгоритмі бойынша алынған 120 шифрмәтіннің статистикалық қәуіпсіздігі тексеріліп нәтижелерлері ұсынылды.

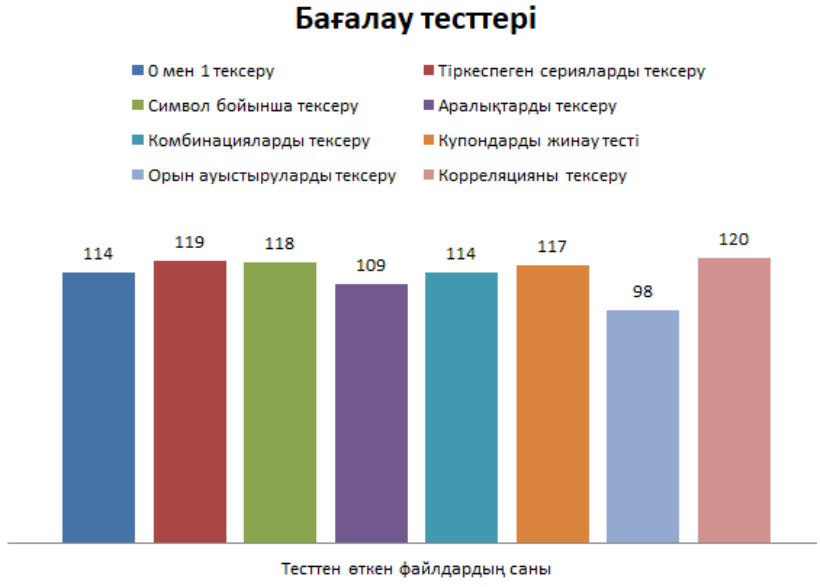
Графикалық тестердің нәтижелерін төмендегі суретте бейнеленген, әр баған аталмыш тесттен 120 файлдың шешеуі өткенін корсетеді (3-суретте).



3-сурет. Графикалық тесттердің нәтижелері

Графикалық тестердің нәтижелері: Элементтерді тарату гистограммасы, жазықтықта тарату, сериялардың тексеру, монотондылықты тексеру, байттық автокорреляциялық функция (АКФ), биттік автокорреляциялық функция (АКФ), графикалық спектралды тест, сызықтық күрделілік профилі тестеріне сәйкес 116, 119, 118, 109, 114, 117, 119, 120 шифрмәтін тестілеуден өтті.

Ал бағалау тестердің нәтижелері нақты өткендігі немесе өтпегендігі туралы нәтижелер ұсынады (4-сурет) .



4-сурет. Бағалау тесттердің нәтижелері

Бағалау тестердің нәтижелері: 0 мен 1 тексеру, байланыссыз сериялардытексеру, тіркеспеген сериялардытексеру, символ бойынша тексеру, аралықтардытексеру, комбинацияларды тексеру, купондарды жинау тесті, орын ауыстыруларды тексеру, корреляцияны тексеру тестеріне сәйкес 114, 119, 118,109,114,117, 98, 120 шифрмәтін тестілеуден өтті.

Қортынды. Қарастырылған алгоритімнің бағдарламасы құрылып, осы алгоритм бойынша шифрленген файлдардың шифрмәтіндерінің статистикалық қауіпсіздігін бағалау және графикалық тестер арқылы сыналды. Алгоритмнің басқа да қасиеттерін зерттеу алдағы жұмыстарда жоспарланған.

Қолданылған әдебиеттер

1. Чипига А.А. Криптографическая защита данных в информационных технологиях на базе непозиционных полиномиальных систем [Текст] / А.А. Чипига, И.А. Калмыков, А.В. Барильская, О.А. Кихтенко // Известия ЮФУ. Технические науки. Таганрог, -2009, -С.210-220.

2. Амербаев В. М., Бияшев Р. Г., Нысанбаева С. Е. Применение непозиционных систем счисления при криптографической защите // Изв. Нац. акад. наук Респ. Казахстан. Сер. физ.-мат. 2005. No 3. С. 84–89

3. R. Biyashev, S. Nyssanbayeva, N. Kapalova, A. Haumen, Modied symmetric block encryption-decryption algorithm based on modular arithmetic // Proceedings of the International Conference on Wireless Communications, Network Security and Signal Processing (WCNSSP2016). – Chiang Mai, Thailand,2016. – pp. 263-265.

4. Червяков Н.И. Нейрокомпьютеры в остаточных классах [Текст] / Н.И. Червяков, П.А. Сахнюк, А.В. Шапошников, А.Н. Макоха; под ред. А.И. Галушкина. –М.: Радиотехника, 2003. – 272 с.

5. Чипига А.А. Применение расширенных полей Галуа гля повышения информационной скрытности передачи данных [Текст] / А.А. Чипита, И.А. Калмыков, А.Б. Хайватов, Сагдеев А-К. // Успехи современного естествознания, № 5. - 2007. С. 103-105.

6. Чипига А.А. Реализация процедуры обратной нелинейному шифрованию с использованием индексного представления для поля Галуа / А.А. Чипига, И.А. Калмыков, А.В. Барильская, О.А. Кихтенко, В.Р. Гахов // Материглы электронной заочной конференции Российской Академии Естествознания «Прикладные исследования и разработки по приоритетным направлениям науки и техники». 15-20 ноября 2009.

КРИПТОСТОЙКОСТЬ СИСТЕМЫ ШИФРОВАНИЯ RSA

Абдикаликов К.А.
e-mail: abdikalikov@mail.ru
Актюбинский университет имени С. Баишева (Актобе), Казахстан