ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ
Факултет по телекомуникации
катедра Радиокомуникации и видеотехнологии

маг. инж. Иван Динков Иванов

МЕТОДИ И АЛГОРИТМИ ЗА ПОВИШАВАНЕ НА СИГУРНОСТТА И СЪХРАНЕНИЕТО НА ДАННИТЕ ПРИ ПРЕДАВАНЕТО НА ИНФОРМАЦИЯ В ТЕЛЕМЕТРИЧНИ СИСТЕМИ

АВТОРЕФЕРАТ

за получаване на образователна и научна степен „***Доктор***“

Научна специалност:

„Автоматизирани системи за обработка на информация и управление“ (в комуникациите)

Научни ръководители:

проф. д-р инж. Румен Арнаудов

доц. д-р инж. Добрин Диков

Рецензенти:

проф. д-р инж. Георги Димитров Ненов

доц. д-р инж. Иво Николаев Дочев

София, 2016

Дисертационният труд е обсъден на заседание на катедрен съвет на катедра “Радиокомуникации и видеотехнологии” при Факултета по телекомуникации на Технически университет - София, състояло се на 17.10.2016 г. от 15:30 ч. в зала 1259 и е насрочено за официална защита пред научно жури в състав: проф. д-р инж. Румен Иванов Арнаудов, доц. д-р инж. Иво Николаев Дочев, проф. д-р инж. Георги Димитров Ненов, доц. д-р инж. Кирил Методиев Алексиев, доц. д-р инж. Емил Иванов Йончев.

Резервни членове: проф. д-р инж. Лидия Тоткова Йорданова, доц. д-р инж. Красимир Костадинов Марков.

Дата на защита на дисертацията: 16.02.2017 г. (четвъртък) от 13:00 часа.

Място на защита на дисертацията: ТУ - София, конферентна зала на БИЦ.

Данни за дисертационния труд: брой страници 145; брой фигури 46; таблици 66; математически изрази 18; литературни източници 117; публикации по темата на дисертационния труд 6, заявка за патент 1, проект с внедряване 1.

Номерацията на фигурите, таблиците и формулите в автореферата отговаря на тези в дисертацията.

Материалите по защитата са на разположение на интересуващите се в секретариата на катедрата по Радиокомуникации и видеотехнологии (каб. 1254) и на Интернет страницата на Технически Университет – София: www.tu-sofia.bg.

Автор: маг. инж. Иван Динков Иванов.

Тема: Методи и алгоритми за повишаване на сигурността и съхранението на данните при предаването на информация в телеметрични системи.

Тираж: 30 бр.

Проект, оформление и предпечатна подготовка: авторът.

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Актуалност на проблема

През последните десетилетия телеметричните системи навлязоха масово в ежедневието на хората, индустрията, бизнеса, медицината и т.н., използвайки множество технологии, работещи в една обща или множество отделни мрежи. След като информацията от различните устройства за отдалечен контрол се преобразуват в цифров вид, тя се предава по определена преносна среда в дадена мрежа. Това действие води до факта, че тази информация може да бъде прихваната от хора, за които тя не е предназначена (нарушители) или може да бъде записана с цел, по-късна манипулация.

Поради спецификата на тези системи, факторът сигурност, за съжаление, в повечето случаи се пренебрегва изцяло или частично. Повечето производители на отделните компоненти не залагат възможност за активиране, въвеждане или използване на допълнителен модул за сигурност. Разчита се на евентуално осигурената защита на предаваната информация в съответната мрежа, осигурена с известни методи и алгоритми, които не са проектирани и оптимизирани за работа в една телеметрична система.

Все по-бързото развитие на информационните, комуникационните и компютърни технологии, водят и до усъвършенстване на прилаганите атаки и анализи, целящи да придобият достъп, възползване от съдържанието на предаваната или съхранена информация, контролиране и промяна на нейното съдържание, независимо от преносната среда и съоръжения.

НАУЧНА ОПРЕДЕЛЕНОСТ НА ИЗСЛЕДВАНЕТО

Обект на изследването

Обект на изследване на дисертационния труд са методи и алгоритми за повишаване на сигурността и съхранението на данните при предаването на информация в телеметрични системи.

Предмет на изследването са функционалността, основните параметри, криптографската устойчивост и бързодействието на разработения IDA алгоритъм, както и свойството „лавинен ефект“, определящо високата чувствителност на резултата към изменението на началните данни.

Цел на дисертацията:

Целта на дисертационния труд е да се анализират методите и алгоритмите за повишаване на сигурността и съхранението на данните, въз основа на което да се създаде нов метод и криптографски алгоритъм за предаването на информация в телеметрични системи със специално предназначение и повишена степен на защита с универсална приложимост, както и изследване на основните параметри и криптографката устойчивост на алгоритъма на външни атаки.

Задачи:

1. Критичен анализ на методите и алгоритмите за повишаване на сигурността и съхранението на данни;
2. Избор на схема, криптографски процедури, функции и генератор на ключове;
3. Създаване на нов метод за повишаване на сигурността на данните;
4. Създаване на нов криптографски алгоритъм;
5. Изследване бързодействието на алгоритъма;
6. Изследване на основните параметри и криптографската устойчивост на предложения криптографски алгоритъм;
7. Сравнение на криптографската устойчивост на новия алгоритъм с утвърдени блокови криптографски алгоритми;
8. Имплементиране на разработения алгоритъм в мобилна система с предаване на телеметрични данни.

Методи на изследване

За решаване на поставените задачи в дисертационната работа се използват методите на функционалния анализ, синтез, основи на криптографията, информационната и мрежова сигурност, имитационно моделиране, компютърна симулация и програмиране.

Апробация на изследването

Основните резултати от проведените изследвания в дисертацията са докладвани и обсъдени на научни форуми, национални и международни конференции: First International Scientific Conference “Telecommunications, Informatics, Energy and Management TIEM `15”; DCCN, Eighteenth International Scientific Conference, 2015 г., Moscow, Russia; International

conference Robotics, Automation and Mechatronics' 14 – RAM 2014; International scientific conference on information, communication and energy systems and technologies - ICEST 2015; Национален форум Електроника 2015; Известия на Съюза на учените – Русе, Серия 1 „Технически науки“, Том 11, 2014, както и заявка за патент №111513/25.06.2013 и участие в работа по проекта HeERO2 в консорциума на българската пилотна реализация на системата „eCall" 2014, завършил с внедряване на резултата от дисертационния труд.

Публикуване на резултатите от дисертационните изследвания

Основните резултати са публикувани в шест статии и доклади от конференции, научни списания и заявка за патент.

Структура на дисертацията

В структурно отношение дисертацията се състои от въведение, четири глави, заключение и изводи, приноси на дисертационното изследване, използвана литература и приложения.

II. СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

ГЛАВА 1

ОБЗОР НА ТЕЛЕМЕТРИЧНИ СИСТЕМИ, МЕТОДИ И АЛГОРИТМИ ЗА ПОВИШАВАНЕ НА СИГУРНОСТТА И СЪХРАНЕНИЕТО НА ДАННИ

В настоящата глава са представени и анализирани съществуващите криптографски методи и алгоритми [A1] за повишаване на сигурността и съхранението на данни при предаване на информация в телеметрични системи.

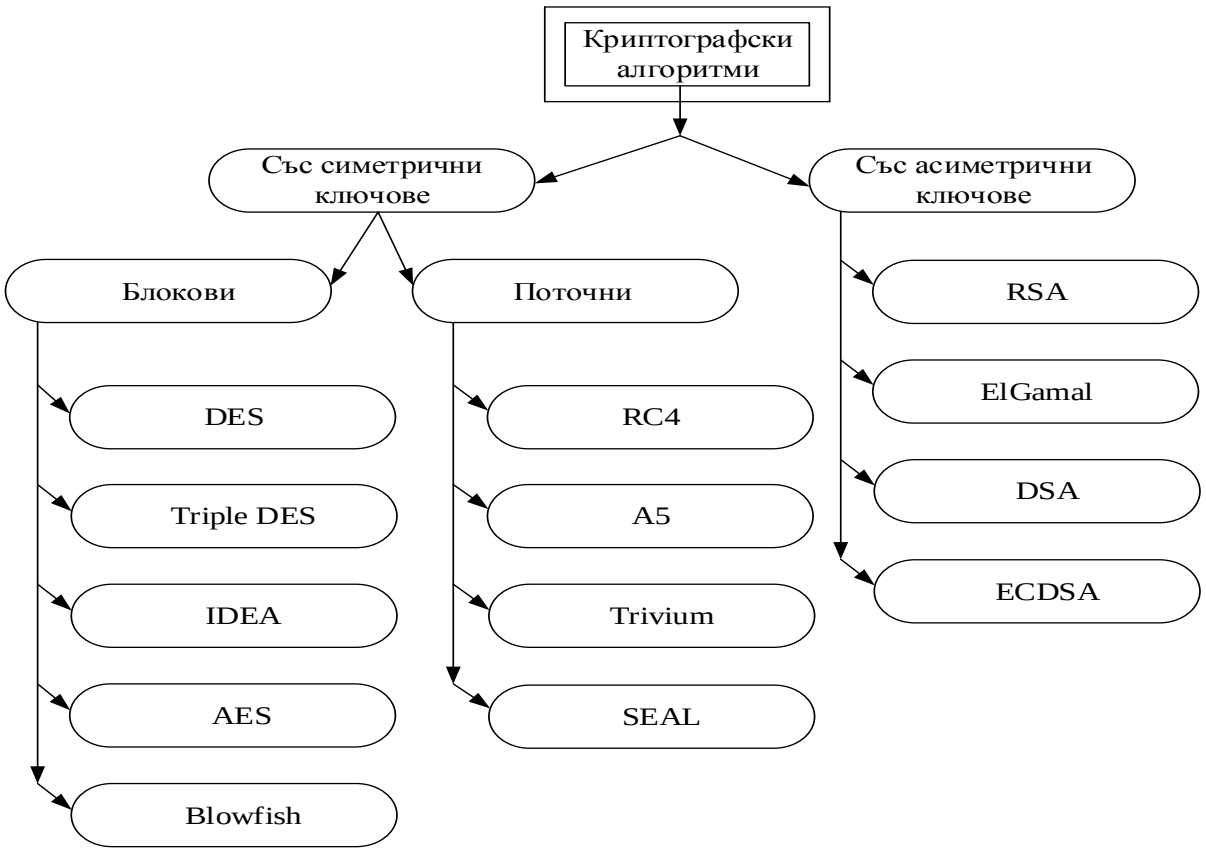
На базата на направения критичен обзор на широкото приложение и все по-голямата необходимост от използването на телеметрични системи в различни области и направления (в голямата си степен със специално предназначение), изискват реализирането на нов криптографски алгоритъм [A2], позволяващ лесна софтуерна и хардуерна реализация, както и универсална приложимост.

Анализ на криптографски методи и алгоритми

Основната цел е да се анализират използващите се криптографски методи и алгоритми, като са поставени следните задачи:

- да се извърши критичен анализ на криптографските методи и алгоритми;
- да се направи предложение за реализиране на нов криптографски алгоритъм.

За целта е направена обща класификация на криптографските алгоритми, в която са отчетени критериите: използвани ключове и начин на обработка (фиг. 1.1.).



Фиг. 1.1. Обща класификация на криптографските алгоритми

Всички криптографски алгоритми от тази класификация са обект на критичния анализ, на базата на които са определени техните предимства и недостатъци.

Предимства и недостатъци при режимите на работа на криптографските алгоритми:

- Режим „електронна кодова книга”;
- Режим „свързване на блоковете”;
- Режим „обратна връзка по шифротекст”;

- Режим „обратна връзка по изход”;
- Режим „брояч”.

На базата на този критичен анализ са определени следните **изисквания за реализиране на нов криптографски алгоритъм**:

1. Да осигурява индивидуална криптографска защита “от край до край“;
2. Да се използва блокова обработка на информацията, симетрична схема и ключове;
3. Да се използва схемата на Фейстел;
4. Дължината на основния ключ да бъде минимум 256-бита;
5. Да се използват по възможност по-голям брой вътрешни цикли (над 12);
6. Да се използват по възможност по-голям брой под-ключове (над 16);
7. Възможност за работа от 8 битови смарт карти до високо-производителни компютри;
8. Да притежава универсална приложимост.

1.2. Приноси към Глава 1

1.2.1. Предложена е класификация на криптографските алгоритми, като са описани техните предимства и недостатъци;

1.2.2. Представено е сравнение на разликите между различните режими на работа на криптографските алгоритми и тяхното въздействие върху сигурността, сложността и разпространението на грешки;

1.2.3. Определени са основните изисквания за реализиране на нов блоков криптографски алгоритъм.

1.3. Публикации на автора, свързани с настоящата глава

A1. IvanovI. Analysis of cryptographic algorithms - advantages and disadvantages, FirstInternationalScientificConference “Telecommunications, Informatics, Energy and Management „TIEM `15” October 15-18, 2015, pp. 114-117, Bitola, Macedonia.

ГЛАВА 2

РАЗРАБОТВАНЕ НА МЕТОД И НОВ КРИПТОГРАФСКИ АЛГОРИТЪМ ЗА ПРЕДАВАНЕ НА ИНФОРМАЦИЯ В ТЕЛЕМЕТРИЧНИ СИСТЕМИ СЪС СПЕЦИАЛНО

ПРЕДНАЗНАЧЕНИЕ И ПОВИШЕНА СТЕПЕН НА ЗАЩИТА С УНИВЕРСАЛНА ПРИЛОЖИМОСТ

2.2. Параметри за разработване на алгоритъма

Почти всички симетрични блокови криптографски алгоритми са построени на базата на схемата на Фейстел, поради изпитаната си във времето конструкция, бързодействие и сигурност. Затова на нейна база е изграден предложеният алгоритъм. На базата на използваните критерии за построяването на тази схема и DES алгоритъма, може да се въведат три основни параметъра, касаещи структурата на този блоков алгоритъм:

- Броят на вътрешните цикли;
- Видът на функцията за шифриране F;
- Получаването на под-ключовете.

2.2.1. Брой на вътрешните цикли

Колкото по-голям е броят на вътрешните цикли, толкова по-затруднен е криптоанализът на шифъра, дори при относително слаба функция F. В общия случай, броят на циклите трябва да се избира така, че за всички известни методи за крипто-анализ да е необходимо повече време в сравнение с анализа, използващ проверката на всички възможни ключове.

Този критерий е основен при настоящата разработка, при което основавайки се на схемата на Фейстел, броят на вътрешните цикли да бъде равен на 16.

2.2.2. Вид на функцията за шифриране F

Съгласно [A2], при разработването на алгоритъма, са дефинирани определени критерии за структурата на S матрицата и функцията P, на входа на която постъпват данните, получени от S матрицата.

2.2.2.1. Критерии за разработването на S матрицата

1. Никой бит от изходните данни на S матрицата не трябва да бъде зависим с помощта на линейна функция от входните битове;
2. Всеки ред на S матрицата, трябва да съдържа всички 16 възможни изходни комбинации от битове;
3. Ако входните значения на S матрицата се различават само с един бит, изходните значения трябва да се различават минимум с два бита;

4. Ако входните значения на S матрицата се различават по двата средни бита, изходните значения трябва да се различават минимум с два бита;
5. Ако входните значения на S матрицата се различават по първите два бита и съвпадат по двата последни, изходните значения не трябва да са еднакви.

Първият критерий определя нелинейният характер на S матрицата, необходим на всеки блоков алгоритъм, тъй като ако алгоритъмът няма нелинеен елемент в своята структура, той е много уязвим на крипто-анализ. Останалите критерии решават задачата по противодействие на диференциалния крипто-анализ на алгоритъма и помагат за получаването на добри показатели, свързани със свойството „confusion“.

За настоящата разработка се използват 8 S матрици (кутии) като в глава 4 са направени изследвания относно това, доколко и в каква степен покриват тези критерии.

2.2.2.2. Критерии за създаването на функцията P

1. Четирите изходни бита, получени като резултат от S матрицата на i–тия цикъл, трябва да се разпределят така, че два от тях да влияят на средните битове на i+1 цикъл, а другите два на крайните битове.
2. Четирите изходни бита на S матрицата в следващия цикъл трябва да влияят на резултатите на шест различни S матрици, и нито една двойка от тези четири изходни бита не трябва да попада на входа на една S матрица.
3. За две S матрици S_i и S_k, ако някой от изходните битове на S_i матрицата в следващия цикъл влияят на средните битове на S_k, то никой изходен бит на S_k не трябва да влияе на средните битове на S_i.

Тези критерии обезпечават изискването към алгоритъма за свойството „diffusion“.

За тази разработка се използва функцията P, като в глава 4 са направени изследвания на тази функция относно това, доколко и в каква степен покриват тези критерии.

2.3. Описание на алгоритъма

Алгоритъмът IDA (Ivanov, Dikov, Arnaudov) [A2,A3] е построен на базата на DES алгоритъма и в съответствие със схемата на Фейстел. Той е 64-битов, симетричен блоков криптографски алгоритъм, използващ 256-битов криптографски ключ. Състои се от 16 вътрешни цикъла, съдържащи

транспозиции, субституции и нелинейни процедури.

Алгоритъмът работи върху 64-битови блокове данни, като използва 256-битов ключ за криптиране и декриптиране. В процеса на манипулиране на данните участват побитови и логически операции, както и таблични пермутации. Простотата на операциите позволява прилагането на алгоритъма върху много широк спектър изчислителни системи – вградени микро-контролери, процесори с общо предназначение и програмируеми логически устройства.

Решението на поставената по-горе задача и съответните изисквания, са постигнати с разработената схема, показана на фиг.2.1. На базата на тази схема се постигат следните резултати:

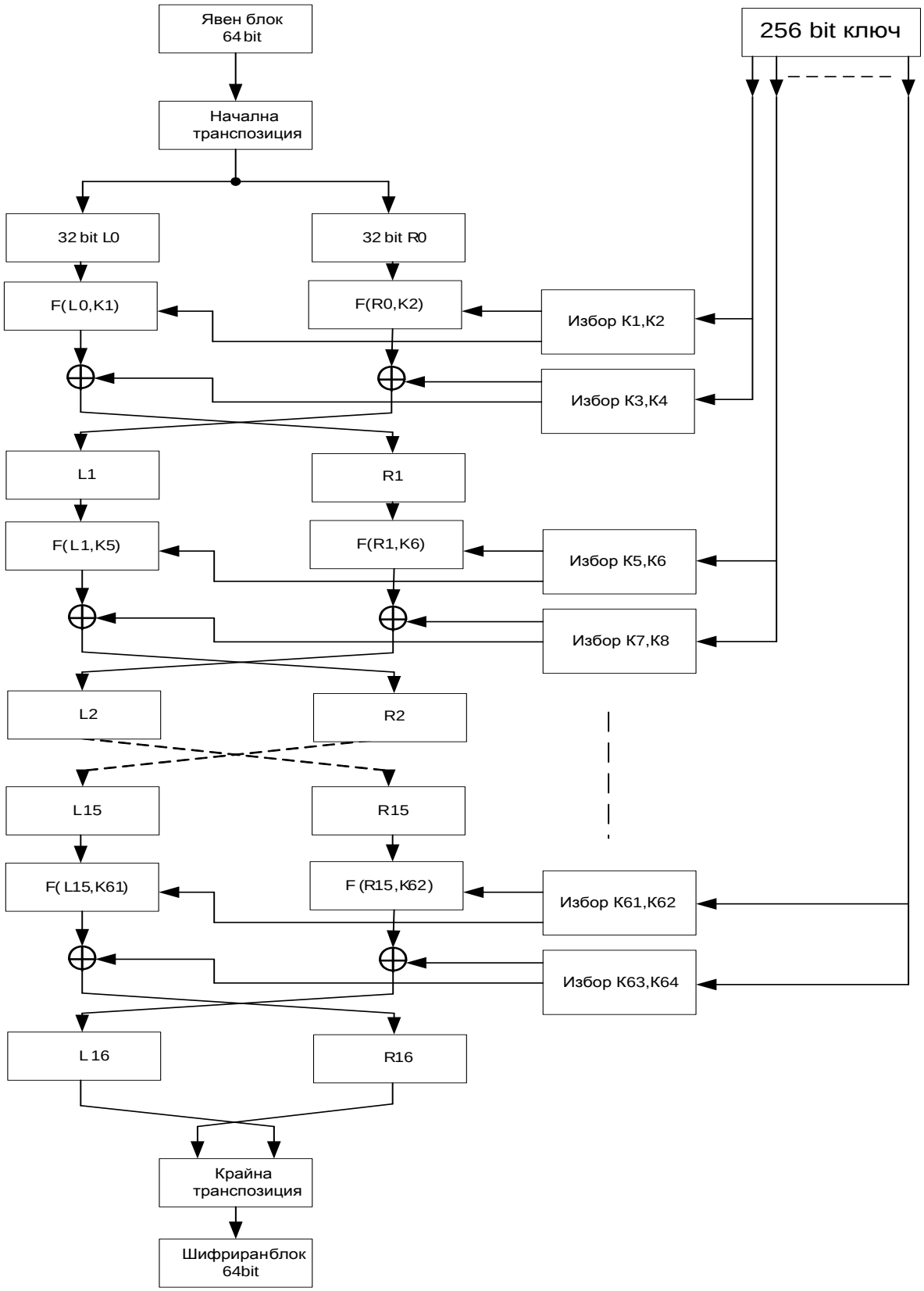
- Въвежда се реалното използване на 256-битов основен ключ;
- Използват се по два 48-битови и два 32-битови под-ключа на всеки цикъл;
- Общо използваните под-ключове са 64;
- Въвежда се допълнителен блок на функцията за шифриране във всеки цикъл в схемата;
- Въвежда се допълнителен суматор XOR във всеки цикъл.

Информационният поток се разделя на блокове от явна информация с дължина 64 бита (фиг. 2.1). Във фазите на първоначалното и крайното разместване се подават 64-битови блокове и се генерират блокове със същия размер. Разместването е процес на смяна на позициите на битовете без да се променят стойностите, използвайки таблични функции.

2.3.1. Начално и крайно разместване

Прилагането на табличните функции се извършва по следния начин. Записаните в таблиците числа показват поредния номер на бита от входната последователност и съответната му позиция в изходната последователност.

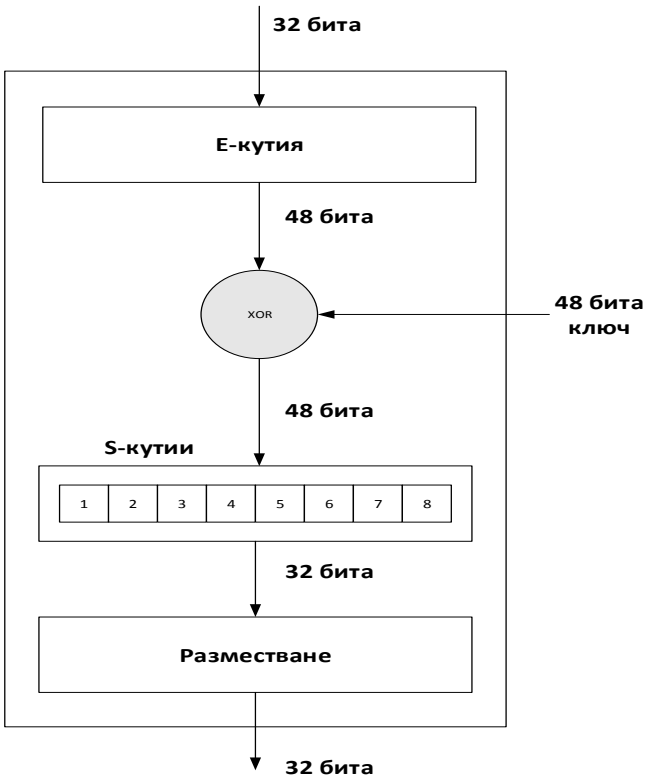
Получената последователност от 64 бита (фиг.2.1) се разделя на две последователности - лява L(0) и дясна R(0), всяка от които съдържа 32 бита. Това разделяне се реализира, като битовете от 1-ви до 32-ри се взимат като лява част, а от 33-ти до 64-ти като дясна част. След това се изпълнява процесът за шифриране с помощта на функцията F(.). Тази функция в този случай се осъществява и върху двете части. Изходните 32-битови последователности на двете функции F(.) се подават на първите входове на два суматора XOR. На вторите входове на тези суматори се подават първите два 32-битови под-ключа. Изходните 32-битови последователности на двата XOR суматора сменят местата си, т.е. левите стават десни и обратно.



Фиг. 2.1. Обща блокова схема на алгоритъма за криптиране

2.3.2. Реализация на функцията за криптиране F-функция

Използва се означението „F-функция“, за да се опише функция от 48-битов междинен ключ и 32-битовата лява и дясна част на входа на първия цикъл f (R_1, K_1) и f (L_1, K_2). В настоящия случай функцията за криптиране се прилага два пъти за всеки цикъл, т.е. върху лявата и дясната част. Блоковата диаграма на структурата на F-кутията е показана на фигура 2.2. Както се вижда на фигурата, междинният ключ се подава на входа на XOR операция заедно с изхода от функцията за разширяване (E-кутия), който приема за вход лявата или дясната част на съответната стъпка и я разширява от 32 на 48 бита. Резултатът от XOR операцията е 48-битова последователност, която се подава на входа на S-кутия. Изходната 32-битова последователност от S-кутия преминава през функция за 1-1 разместване (по същия начин, както първоначалното и крайното разместване, но по различна таблица).



Фиг.2.2. F-функция (кутия)

2.3.2.1. Функция за заместване (S-кутия)

S-кутията е най-важната част в процеса на разместване. 48-битовия входен блок на S-кутията се разделя на 8 под-блока от по 6 бита. Всеки под-блок е вход на една от осем S-кутии (фиг. 2.1). Всяка S-кутия генерира 4-битов изходен блок, като използва таблица с размер 4x16 за преобразуването. Четирите средни бита от входния 6-битов блок се

използват за определяне на индекс на колона в съответната таблица, а двата крайни бита определят индекс на ред. Стойността от кутията с тези индекси в таблицата е изходният блок от битове.

На изходите на осемте S-кутии се получава 32 битова последователност.

Нелинейният характер на тези S-кутии се определя от стойностите в колоните им, получени на базата на специални математически „бент“ функции.

2.3.2.2. Функция за разместване P

Функцията за разместване на битовете P(L), също се използва за определяне функцията за шифриране, задавайки значенията, представени в табличната функция.

На изхода на функцията за разместване на L се получава 32 битова последователност, която след това постъпва на единия вход на третия XOR суматор на първия цикъл. На изхода на функцията за разместване на R се получава 32 битова последователност, която след това постъпва на единия вход на четвъртия XOR суматор на първия цикъл. На вторите входове на двата XOR суматора постъпват 32 битовите последователности на ключовете K_3 и K_4 (фиг.2.1). Изходните 32-битови последователности на двата XOR суматора, сменят местата си, т.е. левите стават десни и обратно, при което от своя страна се явяват входни последователности за следващия цикъл. Тези процедури се осъществяват общо 16-пъти, на базата на вътрешните цикли.

На изхода на 16-я цикъл, двете 32 битови последователности от лявата и дясната част се обединяват, при което се получава 64 битова последователност. Тя се обработва с функцията за крайно разместване. Записаните в таблицата числа показват поредния номер на бита от входната последователност и съответната му позиция в изходната последователност. Тази последователност представлява крайният резултат от криптирането на първия блок от явната информация, т.е. криптограмата на този блок, който се подава в съответната мрежа [А4].

2.3.3. Генератор на вътрешните под-ключове

Получаването на 64-те ключа $\{K_j\}$ с дължина 48 бита и 32 бита се извършва по общия алгоритъм, показан в дясната част на фиг.2.1.

Ключовете, участващи на всеки един цикъл, се генерират от основния по следния начин. Взимат се последователно необходимия брой битове за под-ключовете, както следва: първите 48 бита от основния ключ се вземат като ключ K_1 и се подават на входа на функцията $F(L_0, K_1)$. Следващите 48 бита се вземат като ключ K_2, постъпващ на входа на $F(R_0,$

K_2). Следващите 32 бита се вземат като K_3 и се подават на входа на първия суматор XOR на първия цикъл, следващите 32-бита се вземат като ключ K_4 и се подават на входа на втория суматор XOR на първия цикъл. Следващите 48 бита от основния ключ се вземат като ключ K_5 и се подават на входа на функцията $F(L_1, K_5)$. Следващите 48 бита се вземат като ключ K_6, постъпващ на входа на $F(R_1, K_6)$. След достигане до последния бит на основния ключ, се осъществява линейно отместване на 25 бита наляво в 256-битовата последователност, съгл. Таблица. 2.7 (общо десет пъти за да се получат необходимия брой под-ключове за 16-те цикъла). След това, по същия начин се генерират останалите (общо 64) ключове за втория цикъл, и т.н. до 16-я цикъл.

2.3.4. Процес на дешифриране

Процесът на дешифриране на данните се явява инверсен по отношение на процеса за шифриране. Всички действия трябва да се изпълняват в обратен порядък.

2.4. Научни и научно-приложни приноси към Глава 2

Научно-приложни приноси

1. Предложена е функционална схема на симетричен 64-битов блоков криптографски алгоритъм, използващ 256-битов ключ.
2. Синтезиран е метод за повишаване на сигурността на данните при предаване на информация в телеметрични системи със специално предназначение и тяхното съхранение. Заявка за патент №111513/25.06.2013.
3. Предложено е графично и таблично представяне на предназначението и действието на отделните функции и операции на ниво битове с възможност за програмна или хардуерна реализация.

2.5. Публикации и патенти на автора, свързани с настоящата глава

A2. Метод за повишаване на сигурността на данните при предаване на информация в телеметрични системи със специално предназначение и тяхното съхранение. Заявка за патент №111513/25.06.2013.

A3. Ivanov I., Algorithm for security and data storage increase using cyclic encryption methods. Известия на Съюза на учените – Русе, Серия 1 „Технически науки“, Том 11, 2014, стр. 63-66, България.

A4. Ivanov I., Vetova S. Cryptography Protection Of Information Data Change In Telecommunication Nets. International conference Robotics, Automation and Mechatronics’ 14 – RAM 2014, pp. 55-58, Bulgaria.

ГЛАВА 3

ИЗСЛЕДВАНЕ НА ФУНКЦИОНАЛНОСТТА И ВНЕДРЯВАНЕ НА *IDA* АЛГОРИТЪМА

3.1. Изследване на функционалността на алгоритъма

Изследването на функционалността на алгоритъма е свързано с решаването на следните задачи:

1. Ръчно разписване на един цикъл на алгоритъма, с цел нагледното проследяване на правилната работа на криптографските процедури, функции и схеми на алгоритъма [А5].
2. Програмна реализация на алгоритъма и съпоставяне на получените от нея резултати, с тези при ръчното описание [А5].
3. Отстраняване на грешки.
4. Оптимизиране на програмната разработка.
5. Внедряване на IDA алгоритъма [П1].

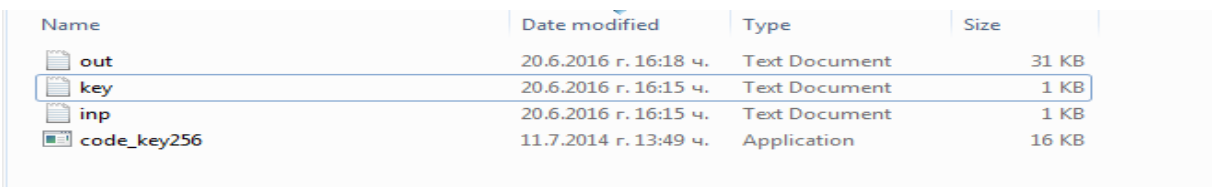
1. Ръчно разписване на един цикъл на алгоритъма

За да се изследва правилната работа на алгоритъма и заложеният в него метод, е необходимо ръчното разписване на няколко цикъла и съпоставяне на получените резултати със същите, получени при програмната реализация.

Поради големия обем от страници, касаещи ръчното разписване на 16-те цикъла при криптиране и декриптиране, в дисертацията са показани само първите три.

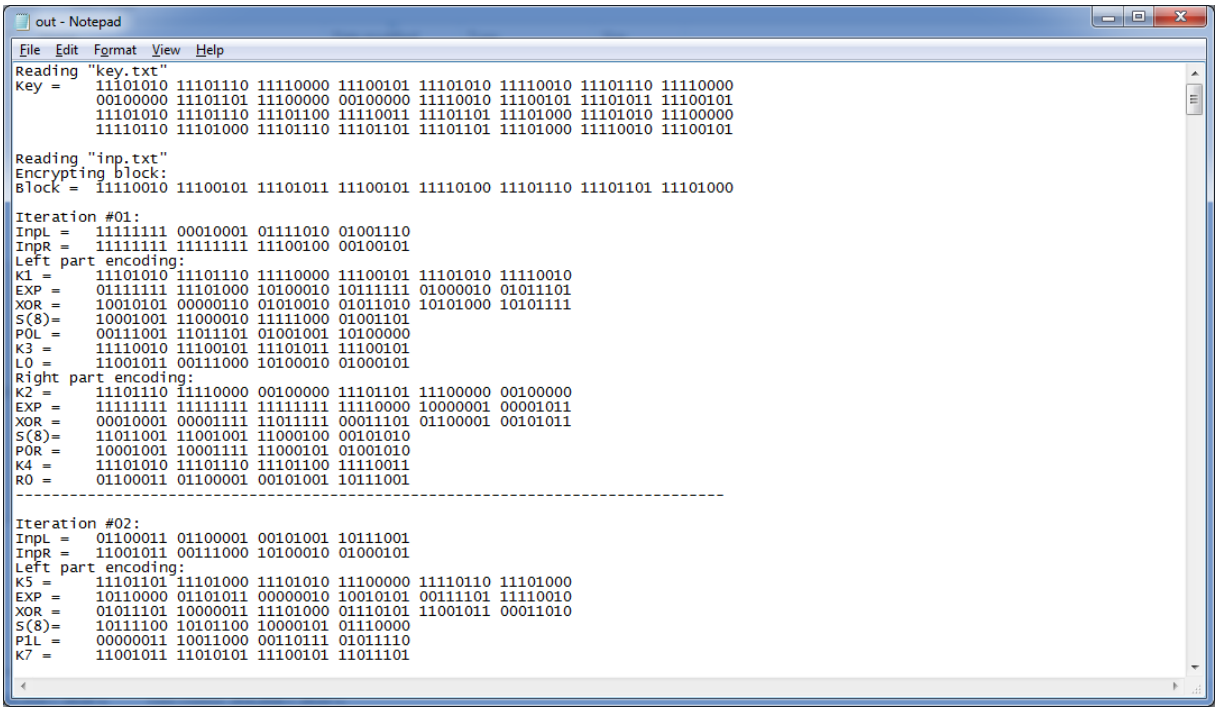
2. Програмна реализация на алгоритъма

Програмата по алгоритъма ***IDA*** е изпълнен на стандартен език за програмиране ***C***. Използвана е среда VisualStudioExpress 2010 на операционна система Windows7 и по-подробно е описан в точка 3.2. Тъй като разработката е подготвена за внедряване, не е наблегнато на това да се създаде добър графичен интерфейс, а по скоро на изпълнението на необходимата функционалност. За да се демонстрира неговото действие, за нуждите на настоящата работа, е създаден изпълним файл „code_key256“, който използва три текстови файла, съответно: inp.txt – за входната информация, key.txt – за основния ключ и out.txt – за криптираната информация (фиг. 3.1).



Фиг. 3.1. Наименование и вид на файловете за тестване

Също така за онагледяване на процеса в изходния out.txt се записват резултатите от всяко едно действие и функция на алгоритъма (фиг. 3.2).



Фиг. 3.2. Резултат от тестването на програмната разработка.

За по-прегледното представяне на резултатите, същите са копирани и поставени в този документ.

При съпоставянето, резултатите от ръчното представяне на първите три цикъла и програмното представяне на същите съвпадат. Освен това се получава възстановяване на явната информация от криптограмата, което е гаранция за правилната работа както на алгоритъма, така и на програмната разработка. Това беше постигнато след доста дни отстраняване на грешки в програмната реализация, чрез проследяване на процесите бит по бит и сравнението им с ръчно разписаните 16 цикъла на шифриране и дешифриране.

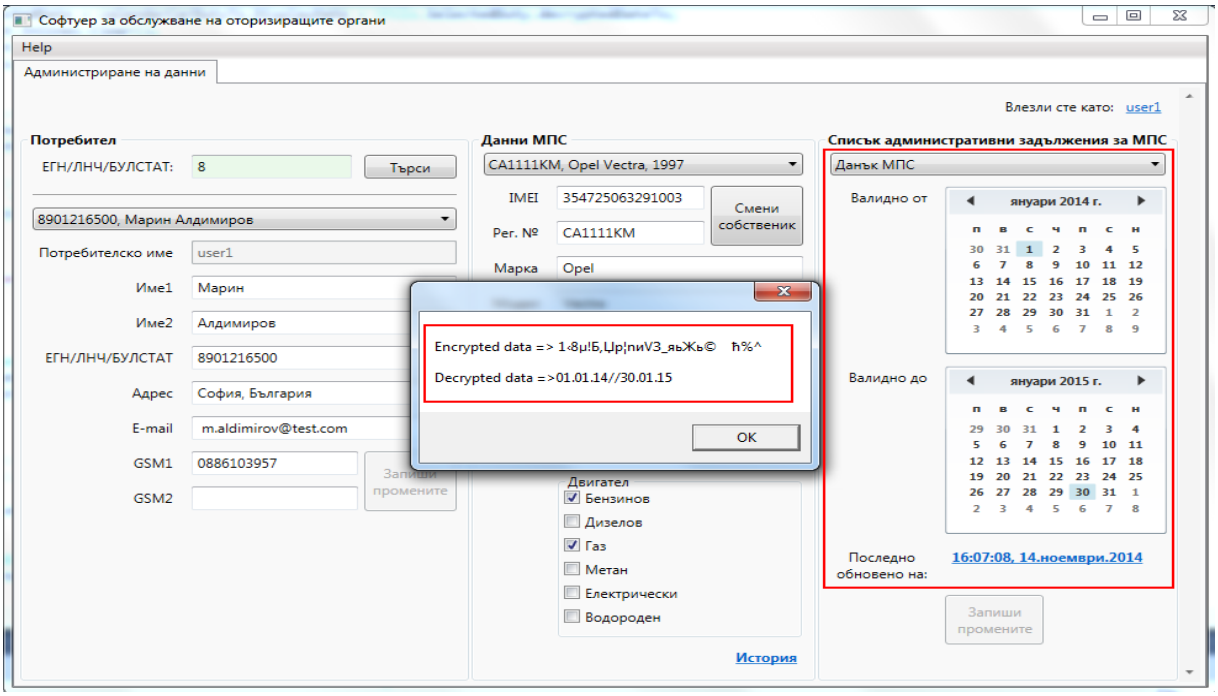
3. Внедряване на IDA алгоритъма

Алгоритъмът IDA е внедрен в система, базирана на системата „eCall” и интегрирана със система с допълнителни функции - управление на автопарк, в услуга на собственика или водача, на застрахователи и в помощ на полицията [А2, А5, П1], както следва:

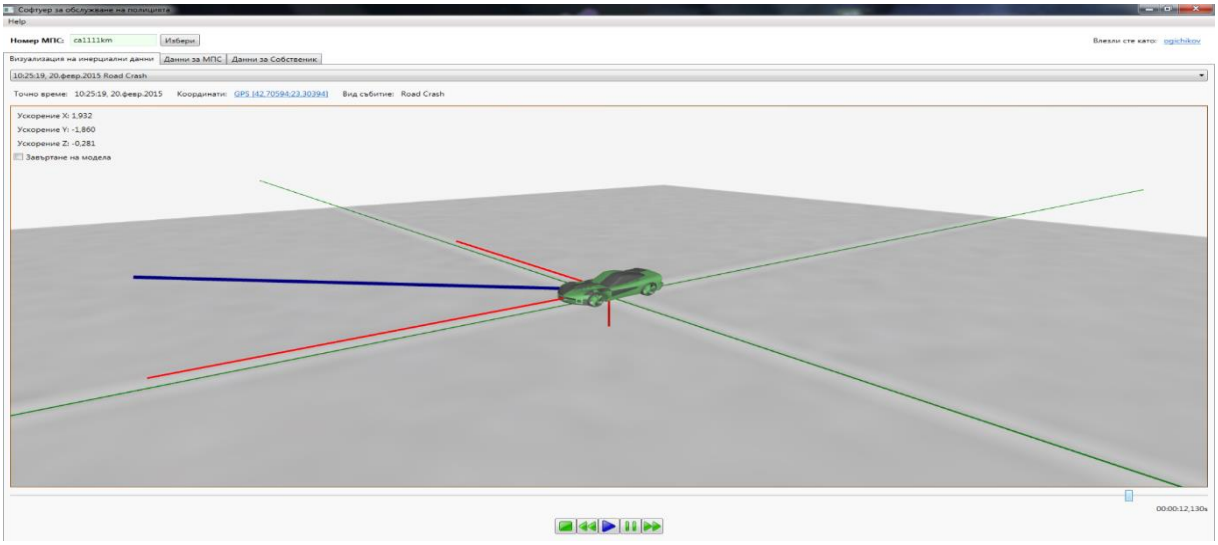
3.1.3.1. В софтуера за обслужване на собственика или водача на МПС, чрез следните функции:

3.1.3.2. В софтуера за ползване от оторизирани органи и застрахователи (фиг.3.4):

3.1.3.3. В софтуер за обслужване на полицията (фиг.3.5).



Фиг.3.4. Данните в криптиран и декриптиран вид и визуализацията им в софтуера за оторизиращи органи



Фиг.3.5. Визуализация на декриптираните инерциални данни в софтуера за полицията

3.2. Научно-приложни и приложни приноси към Глава 3

Научно-приложни приноси

1. Изследвана е функционалността на IDA алгоритъма чрез ръчно разписване на действието му на ниво бит, като по този начин е

определена правилната работа на неговата схема, функции, логически и математически операции.

2. Изследвана е функционалността на IDA алгоритъма чрез програмна разработка, като крайният резултат е представен чрез подробно описание на резултатите на всяка операция и функция в отделните вътрешни цикли.

Приложни приноси

1. Реализирано е програмно приложение на алгоритъма, изпълнено на стандартен език за програмиране C. Използвана е среда VisualStudioExpress 2010 на операционна система Windows7. Отделните последователни фази на алгоритъма са обособени във функции, които се изпълняват в просто конзолно приложение. Не се ползват екзотични или нестандартни библиотечни функции с цел по-добра съвместимост с различни варианти на езика C. Проведени са тестове (1000 на брой) с произволни данни, които се криптират, декриптират и полученият резултат се сравнява за съвпадение с първоначалните данни.
2. Алгоритъмът IDA е внедрен в система, базирана на системата „eCall" и интегрирана със система с допълнителни функции - управление на автопарк, в услуга на собственика или водача, на застрахователи и в помощ на полицията.

3.2. Публикации и проекти на автора, свързани с настоящата глава

A5. Ivanov I., Vetova S., A Method For Enhancing The Security And Data Storage During Information Transsmission In Telemetry Systems, DCCN, Eighteenth International Scientific Conference, 19–22 october 2015 г., Moscow, Russia, pp. 326 – 330.

П1. Участие и работа по проекта HeERO2 в консорциума на българската пилотна реализация на системата eCall, 2014.

ГЛАВА 4

ИЗСЛЕДВАНЕ НА ОСНОВНИТЕ ПАРАМЕТРИ, КРИПТОГРАФСКАТА УСТОЙЧИВОСТ И БЪРЗОДЕЙСТВИЕ НА *IDA* АЛГОРИТЪМА

4.1. Изследване на основните параметри в структурата на IDA алгоритъма

4.1.1. Брой цикли

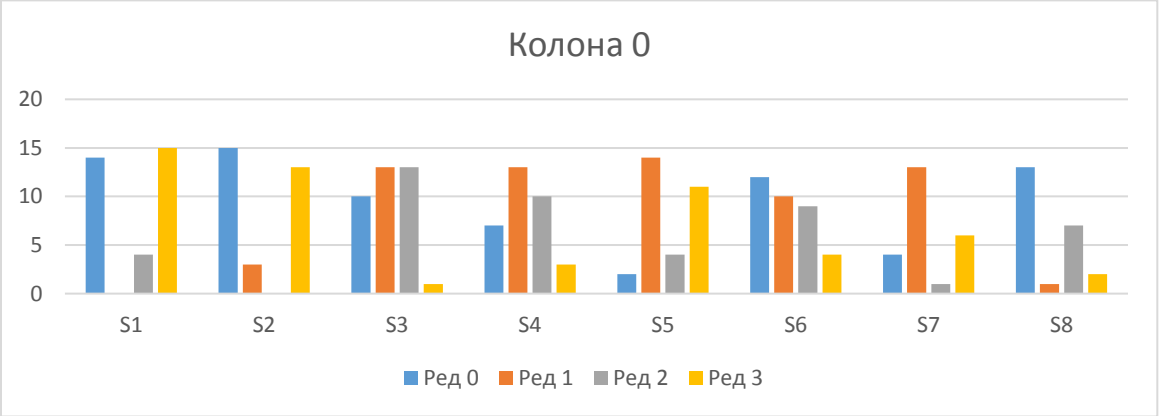
Колкото по-голям е броят на вътрешните цикли, толкова по-затруднен е криптоанализът на шифъра, дори при относително слаба функция F. В общия случай, броят на циклите трябва да се избира така, че за всички известни методи за крипто-анализ да е необходимо повече време в сравнение с анализа, използващ проверката на всички възможни ключове.

4.1.2. Функция за шифриране

4.1.2.1. Изследване на S матриците по критерий 1 от 2.2.2.2.

Стойностите в отделните колони на S матриците са определени с помощта на така наречените "bent " функции. Бент функциите формират специален клас на булеви функции, характеризиращи се с висока степен на нелинейност, в съответствие с определени математически критерии. Тези функции осигуряват напълно изпълнението на критерий 1. Както се вижда от фиг. 4.1, разпределението на стойностите (от 0 до 15) във всяка една колона на отделните S матрици има нелинеен характер.

Колоните на S матриците са представени на фиг. 4.1.



Фиг. 4.1. Стойностите в колона „0“ на осемте S матрици

За останалите колони, разпределението на стойностите е аналогично.

4.1.1.1. Изследване на S матриците по критерий 2 от 2.2.2.2.

В таблица 4.1 са показани стойностите (в десетичен вид) на S1 матрицата.

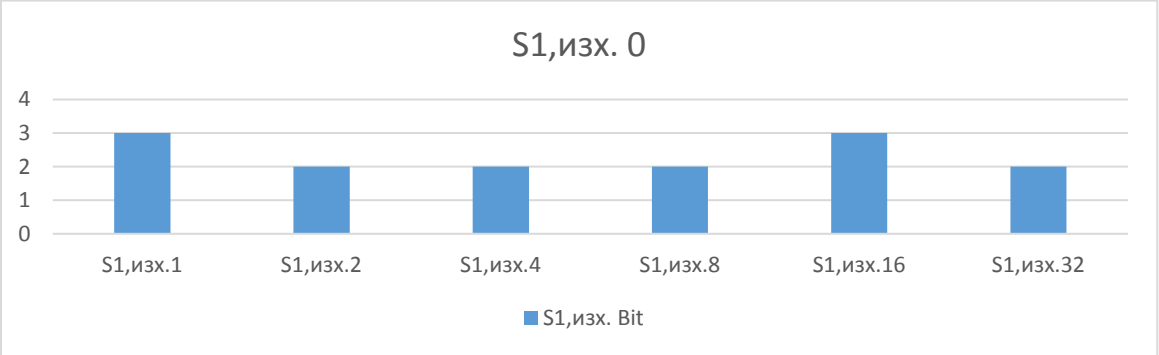
Таблица 4.1. Стойности на S1 матрицата

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

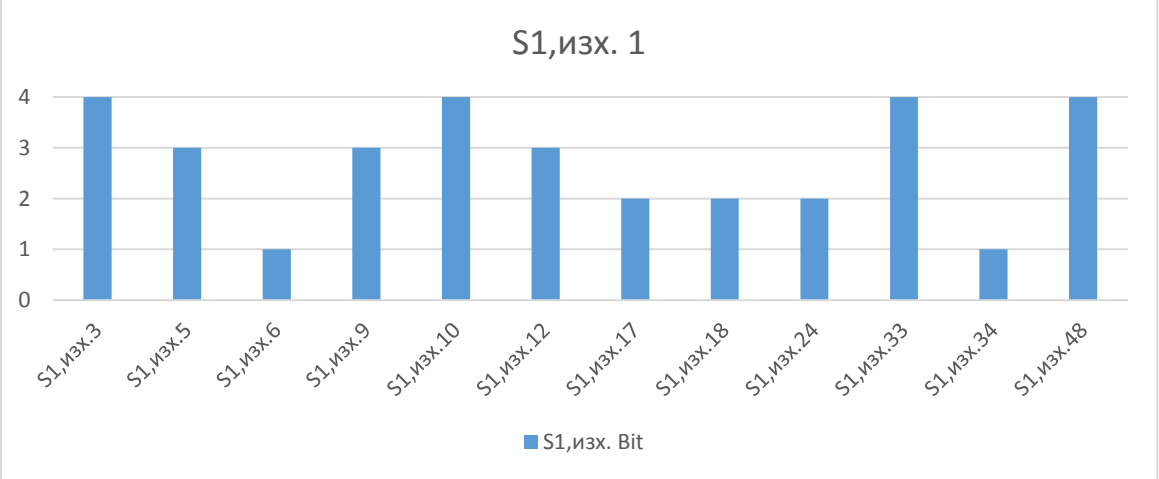
Както може да се види от таблицата, всеки ред на S матрицата съдържа всички 16 възможни комбинации на изходните битове. Това гарантира 100% изпълнение на критерий 2.

4.1.2.2. Изследване на S матриците по критерий 3 от 2.2.2.2. (1)

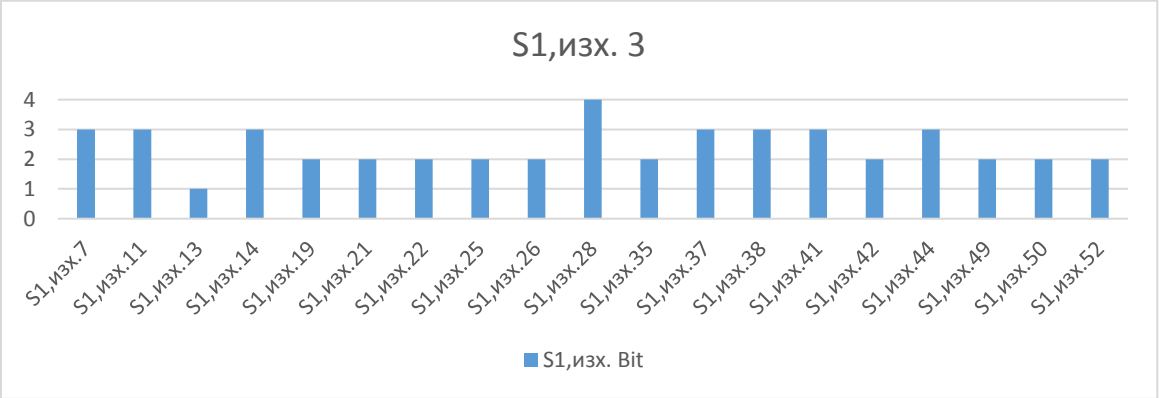
За тази цел на входа се подават комбинации, различаващи се с един бит, а след това се сравняват изходните комбинации (фиг. 4.17 до 4.23).



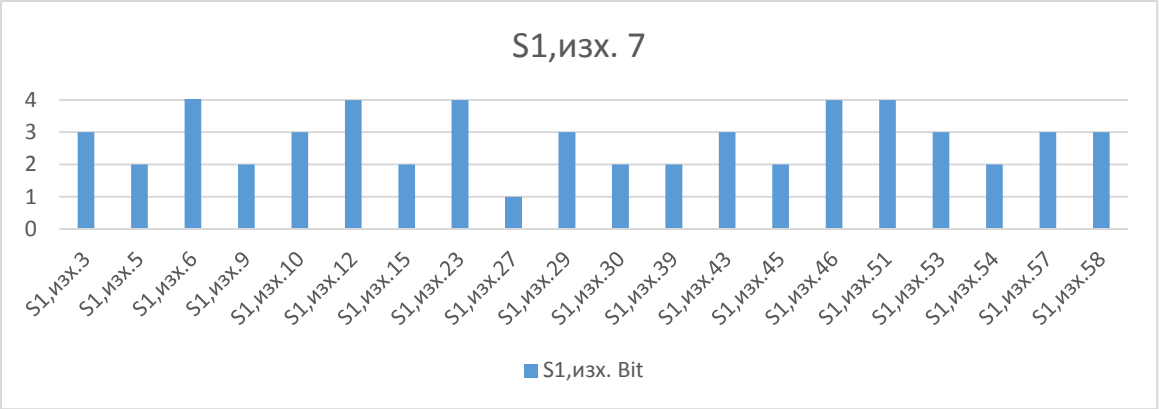
Фиг. 4.17. Резултатите при $S_{1,вх,0}$ = 000000 и $S_{1,изх,0}$ = 1110



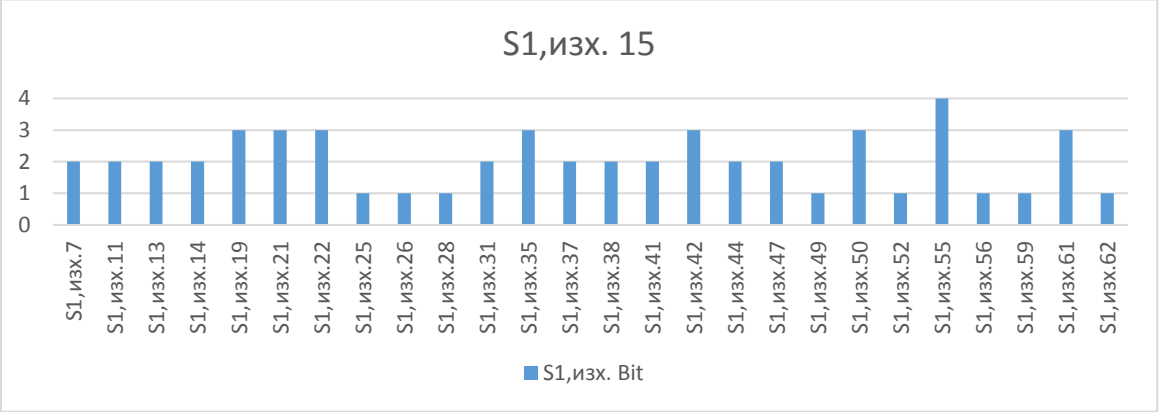
Фиг. 4.18. Резултатите при $S_{1,вх,1}$ = 000001 и $S_{1,изх,1}$ = 0000



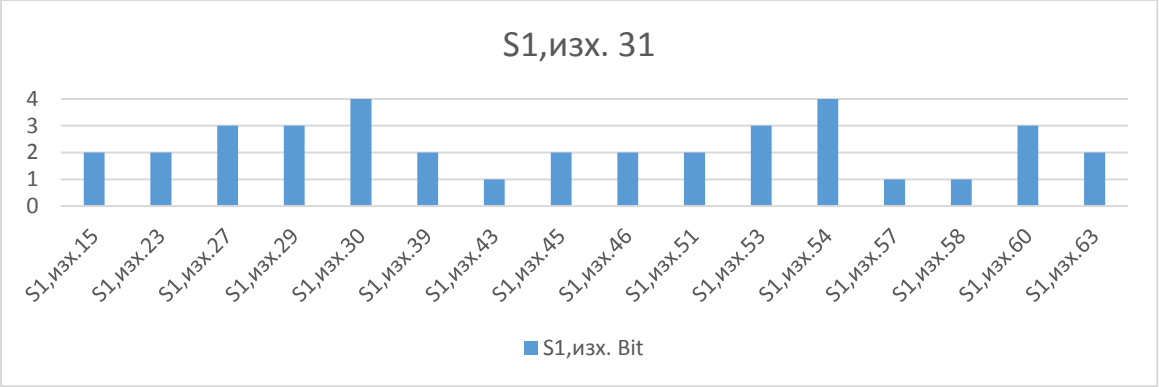
Фиг. 4.19. Резултатите при $S_{1,вх,3}$ = 000011 и $S_{1,изх,3}$ = 1111



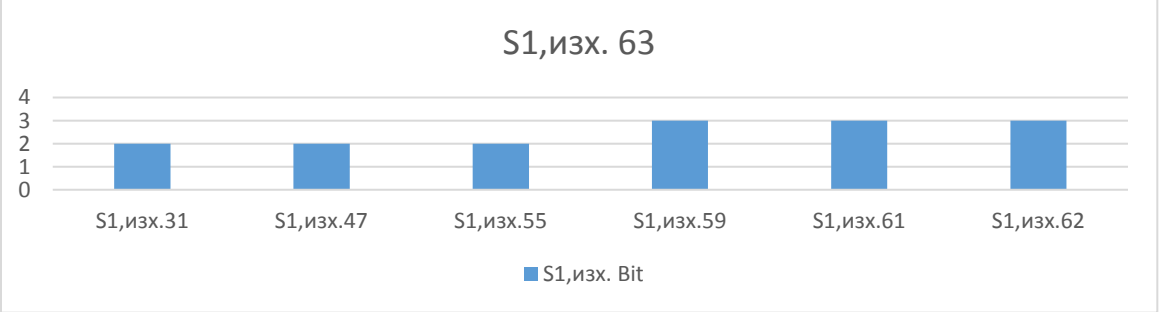
Фиг. 4.20. Резултатите при $S_{1,вх,7} = 000111$ и $S_{1,изх,7} = 0100$



Фиг. 4.21. Резултатите при $S_{1,вх,15} = 001111$ и $S_{1,изх,15} = 0001$



Фиг. 4.22. Резултатите при $S_{1,вх,31} = 011111$ и $S_{1,изх,31} = 1000$



Фиг. 4.23. Резултатите при $S_{1,вх,63} = 111111$ и $S_{1,изх,63} = 1101$

4.1.2.3. Изследване на S матриците по критерий 4

За тази цел на входа се подават комбинации, различаващи се по средните два бита, след което се сравняват изходните комбинации. Разликата е записана в последната колона (таблици от 4.10 до 4.16).

Таблица 4.10. Резултати при $S_{1,вх,0}$ = 000000 и $S_{1,изх,0}$ = 1110

$S_{1,вх,0}$, bit	$S_{1,изх,0}$, bit	$S_{1,вх}$, bit		$S_{1,изх.}$, bit		Разлика, bit
000000	1110	$S_{1,вх,4}$	000100	$S_{1,изх,1}$	1101	2
		$S_{1,вх,8}$	001000	$S_{1,изх,2}$	0010	2
		$S_{1,вх,12}$	001100	$S_{1,изх,4}$	1011	2

Таблица 4.11. Резултати при $S_{1,вх,1}$ = 000001 и $S_{1,изх,1}$ = 0000

$S_{1,вх,1}$, bit	$S_{1,изх,1}$, bit	$S_{1,вх}$, bit		$S_{1,изх.}$, bit		Разлика, bit
000001	0000	$S_{1,вх,5}$	000101	$S_{1,изх,3}$	0111	3
		$S_{1,вх,9}$	001001	$S_{1,изх,5}$	1110	3
		$S_{1,вх,13}$	001101	$S_{1,изх,6}$	1101	3

Таблица 4.12. Резултати при $S_{1,вх,2}$ = 000010 и $S_{1,изх,2}$ = 0100

$S_{1,вх,2}$, bit	$S_{1,изх,2}$, bit	$S_{1,вх}$, bit		$S_{1,изх.}$, bit		Разлика, bit
000010	0100	$S_{1,вх,6}$	000110	$S_{1,изх,6}$	0001	2
		$S_{1,вх,10}$	001010	$S_{1,изх,10}$	1111	3
		$S_{1,вх,8}$	001110	$S_{1,изх,8}$	1000	2

Таблица 4.13. Резултати при $S_{1,вх,3}$ = 000011 и $S_{1,изх,3}$ = 1111

$S_{1,вх,3}$, bit	$S_{1,изх,3}$, bit	$S_{1,вх}$, bit		$S_{1,изх.}$, bit		Разлика, bit
000011	1111	$S_{1,вх,7}$	000111	$S_{1,изх,7}$	0100	3
		$S_{1,вх,11}$	001011	$S_{1,изх,11}$	0010	3
		$S_{1,вх,15}$	001111	$S_{1,изх,15}$	0001	3

Таблица 4.14. Резултати при $S_{1,вх,16}$ = 010000 и $S_{1,изх,16}$ = 0011

$S_{1,вх,16}$, bit	$S_{1,изх,16}$, bit	$S_{1,вх}$, bit		$S_{1,изх.}$, bit		Разлика, bit
010000	0011	$S_{1,вх,20}$	010100	$S_{1,изх,20}$	0110	2
		$S_{1,вх,24}$	011000	$S_{1,изх,24}$	0101	2
		$S_{1,вх,28}$	011100	$S_{1,изх,28}$	0000	2

Таблица 4.15. Резултати при $S_{1,вх,32}$ = 100000 и $S_{1,изх,32}$ = 0100

$S_{1,вх,32}$, bit	$S_{1,изх,32}$, bit	$S_{1,вх}$, bit	$S_{1,изх.}$, bit	Разлика, bit

100000	0100	$S_{1,вх,36}$	100100	$S_{1,изх,36}$	1110	2
		$S_{1,вх,40}$	101000	$S_{1,изх,40}$	1101	2
		$S_{1,вх,44}$	101100	$S_{1,изх,44}$	0010	2

Таблица 4.16. Резултати при $S_{1,вх,48}$ = 110000 и $S_{1,изх,48}$ = 1111

$S_{1,вх,48}$, bit	$S_{1,изх,48}$, bit	$S_{1,вх}$, bit		$S_{1,изх.}$, bit		Разлика, bit
110000	1111	$S_{1,вх,52}$	110100	$S_{1,изх,52}$	1001	2
		$S_{1,вх,56}$	111000	$S_{1,изх,56}$	0011	2
		$S_{1,вх,60}$	111100	$S_{1,изх,60}$	0101	2

4.1.2.4. Изследване на S матриците по критерий 5

За тази цел на входа се подават комбинации, различаващи се по първите два бита и различаващи се по последните два бита, след което се сравняват изходните комбинации. Разликата е записана в последната колона (таблици от 4.17 до 4.21).

Таблица 4.17. Резултати при $S_{1,вх,0}$ = 000000 и $S_{1,изх,48}$ = 1110

$S_{1,вх,0}$, bit	$S_{1,изх,0}$, bit	$S_{1,вх}$, bit		$S_{1,изх.}$, bit		Разлика, bit
000000	1110	$S_{1,вх,48}$	110000	$S_{1,изх,48}$	1111	1
		$S_{1,вх,52}$	110100	$S_{1,изх,52}$	1001	2
		$S_{1,вх,56}$	111000	$S_{1,изх,56}$	0011	3
		$S_{1,вх,60}$	111100	$S_{1,изх,60}$	0101	3

Таблица 4.18. Резултати при $S_{1,вх,1}$ = 000001 и $S_{1,изх,1}$ = 0000

$S_{1,вх,1}$, bit	$S_{1,изх,1}$, bit	$S_{1,вх}$, bit		$S_{1,изх.}$, bit		Разлика, bit
000001	0000	$S_{1,вх,49}$	110001	$S_{1,изх,49}$	0101	2
		$S_{1,вх,53}$	110101	$S_{1,изх,53}$	0011	2
		$S_{1,вх,57}$	111001	$S_{1,изх,57}$	1010	2
		$S_{1,вх,61}$	111101	$S_{1,изх,61}$	0110	2

Таблица 4.19. Резултати при $S_{1,вх,2}$ = 000010 и $S_{1,изх,2}$ = 0100

$S_{1,вх,2}$, bit	$S_{1,изх,2}$, bit	$S_{1,вх}$, bit		$S_{1,изх.}$, bit		Разлика, bit
000010	0100	$S_{1,вх,50}$	110010	$S_{1,изх,50}$	1100	1
		$S_{1,вх,54}$	110110	$S_{1,изх,54}$	0111	2
		$S_{1,вх,58}$	111010	$S_{1,изх,58}$	1010	3
		$S_{1,вх,62}$	111110	$S_{1,изх,62}$	0000	1

Таблица 4.20. Резултати при $S_{1,вх,3}$ = 000011 и $S_{1,изх,3}$ = 1111

$S_{1,вх,3}$, bit	$S_{1,изх,3}$, bit	$S_{1,вх}$, bit		$S_{1,изх.}$, bit		Разлика, bit
000011	1111	$S_{1,вх,51}$	110011	$S_{1,изх,51}$	1011	1
		$S_{1,вх,55}$	110111	$S_{1,изх,55}$	1110	1
		$S_{1,вх,59}$	111011	$S_{1,изх,59}$	0000	4
		$S_{1,вх,63}$	111111	$S_{1,изх,63}$	1101	1

Таблица 4.21. Резултати при $S_{1,вх,32}$ = 110000 и $S_{1,изх,32}$ = 1111

$S_{1,вх,32}$, bit	$S_{1,изх,32}$, bit	$S_{1,вх}$, bit		$S_{1,изх.}$, bit		Разлика, bit
110000	1111	$S_{1,вх,0}$	000000	$S_{1,изх,0}$	1110	1
		$S_{1,вх,4}$	000100	$S_{1,изх,4}$	1101	1
		$S_{1,вх,8}$	001000	$S_{1,изх,8}$	0010	3
		$S_{1,вх,12}$	001100	$S_{1,изх,12}$	1011	1

4.1.2.5. Резултати от изследванията

На базата на направените изследвания, са получени следните резултати:

- 100 % изпълнение на критерий 1;
- 100 % изпълнение на критерий 2;
- 90 % изпълнение на критерий 3;
- 100 % изпълнение на критерий 4;
- 100 % изпълнение на критерий 5;

Изпълнението на критерий 3 е на 90 % поради много големия възможен брой входни и изходни комбинации, които могат да се получат, от където процентът като цяло се понижава, но остава с една много висока стойност.

4.1.2.6. Изследване на структурата на функцията P в IDA алгоритъма, на базата на заложените критерии

За настоящето изследване се използва IDA алгоритъм със следните входни данни:

P=11110010 11100101 11101011 11100101 11110100 11101110 11101101 11101000

K=11101010 11101110 11110000 11100101 11101010 11110010 11101110 11110000 00100000 11101101 11100000 00100000 11110010 11100101 11101011 11100101 11101010 11101110 11101100 11110011 11101101

11101000 11101010 11100000 11110110 11101000 11101110 11101101 11101101 11101000 11110010 11100101

4.1.2.7. Резултати на базата на заложените критерии

- **Резултати на базата на критерий 1**

На базата на направените изследвания, са получени следните резултати: при $S_{0R,32}$ = 11011001110010011100010000101010, се получава P_{0R} = 10001001 10001111 1100010101001010, а при $S_{1L,32}$ = 10111100101011001000010101110000 се получава P_{1L} = 00000011 10011000 0011011101011110. Така получените резултати показват, че този критерий е изпълнен на 100%. Това е така, защото разпределението на отделните четири изходни бита, получени като резултат от S матриците е такова, че два от тях влияят на средните битове на i+1 цикъл, а другите два на крайните битове.

- **Резултати на базата на критерий 2**

На базата на направените изследвания, са получени следните резултати: при $S_{0R,32}$ = 11011001110010011100010000101010, се получава P_{0R} = 10001001 10001111 1100010101001010, а при $S_{1L,32}$ = 10111100101011001000010101110000 се получава P_{1L} = 00000011 10011000 0011011101011110. Така получените резултати показват, че този критерий е изпълнен на 100%. Това е така, защото четирите изходни бита на S матриците, в следващият цикъл, влияят на резултатите на шест различни S матрици, и нито една двойка от тези четири изходни бита не попадат на входа на една S матрица.

- **Резултати на базата на критерии 3**

На базата на направените изследвания, са получени следните резултати: при $S_{0R,32}$ = 11011001110010011100010000101010, се получава P_{0R} = 10001001 10001111 1100010101001010, а при $S_{1L,32}$ = 10111100101011001000010101110000 се получава P_{1L} = 00000011 10011000 0011011101011110. Така получените резултати показват, че този критерий е изпълнен на 100%. Това е така, защото за две S матрици, S_iиS_k, ако някой от изходните битове на S_i матрицата в следващия цикъл влияят на средните битове на S_k, то никой изходен бит на S_k, не влияе на средните битове на S_i.

4.2. Изследване на свойството „лавинен ефект“ в IDA криптографски алгоритъм

4.2.1. Представяне на свойството „лавинен ефект“

Пожелателно свойство на повечето алгоритми за шифриране трябва да бъде високата чувствителност на резултата към изменението на началните данни – всяко малко изменение на открития текст или ключа, трябва да доведе до значително изменение на шифрирания текст. По-конкретно, изменението на всеки един бит от открития текст или ключа, трябва да води до промяната на значенията на голямо количество битове от шифрирания текст. Ако измененията в шифрирания текст са малки, това може да доведе до значително намаляване на множеството от ключове или областта от отрития текст.

4.2.2. Изследване на свойството „лавинен ефект“ в IDA алгоритъма

За да се изследва IDA алгоритъма за свойството „лавинен ефект”, трябва да се шифрират два различни открити текста, различаващи се само по един бит:

P = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

P = 10000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000,

а също и с един и същи ключ:

К = 11101010 11101110 11110000 11100101 11101010 11110010 11101110 1111000000100000 11101101 11100000 00100000 11110010 11100101 11101011 1110010111101010 11101110 11101100 11110011 11101101 11101000 11101010 1110000011110110 11101000 11101110 11101101 11101101 11101000 11110010 11100101

Аналогично изследване се прави и за случая, когато се шифрира един открит текст:

Р = 11110010 11100101 11101011 11100101 11110100 11101110 11101101 11101000, и два ключа, различаващи се един от друг с един бит:

К = 11101010 11101110 11110000 11100101 11101010 11110010 11101110 1111000000100000 11101101 11100000 00100000 11110010 11100101 11101011 1110010111101010 11101110 11101100 11110011 11101101 11101000 11101010 1110000011110110 11101000 11101110 11101101 11101101 11101000 11110010 11100101

К = 01101010 11101110 11110000 11100101 11101010 11110010 11101110 1111000000100000 11101101 11100000 00100000 11110010 11100101 11101011 1110010111101010 11101110 11101100 11110011 11101101

11101000 11101010 1110000011110110 11101000 11101110 11101101 11101101 11101000 11110010 11100101

Графичното представяне на резултатите е показано на фиг. 4.24.

Фиг. 4.24. Резултати на свойството „лавинен ефект“ в IDA алгоритъма

4.2.3. Резултати от изследванията

На базата на направените изследвания, са получени следните резултати:

- При IDA алгоритъма, при два открити текста, различаващи се с един бит и един ключ, след третия цикъл на шифриране се наблюдава средна разлика от 35 бита, от общо 64 бита, за циклите от 3 до 15-ти;
- При IDA алгоритъма, при един открит текст и два ключа, различаващи се с един бит, след третия цикъл на шифриране се наблюдава средна разлика от 33 бита, от общо 64 бита, за циклите от 3 до 15-ти;
- IDA алгоритъма притежава по-добър „лавинен ефект” от DES алгоритъма (осреднена разлика от три бита);

4.3. Определяне на криптографската устойчивост с помощта на теоретично цифрова устойчивост

Тъй като за съвременните криптографски алгоритми това време е много голяма величина, то по-удобно е да бъде определена в години. Тогава се получава (табл. 4.31):

$$\overline{T_{уст}} \approx \frac{Nn_{op}S_{\min}}{6B}10^{-7},[години], \qquad (4.4)$$

На фиг. 4.27 е показана зависимостта на теоретичната цифрова

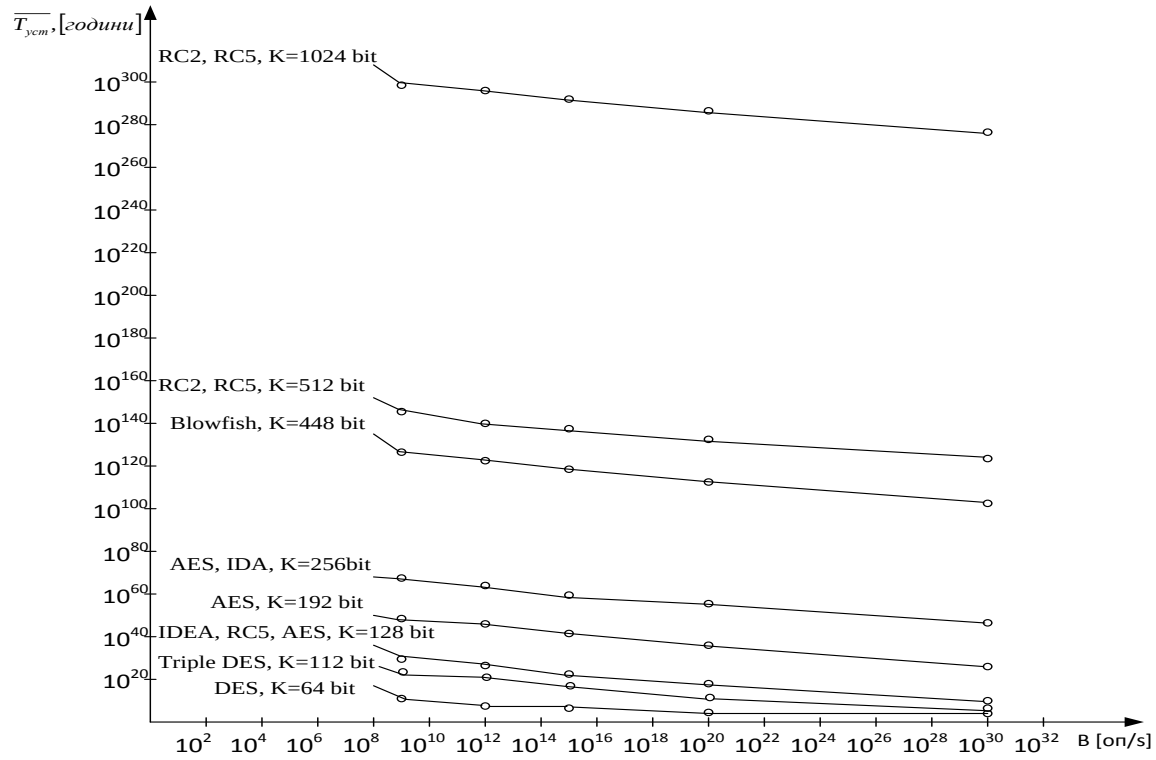
устойчивост, количеството ключове за взаимодействие N при $n_{op}Smin=10^5$ и различни значения на бързодействието на обработката B = 10^8 оп/s; 10^{10} оп/s; 10^{15} оп/s; 10^{20} оп/s; 10^{30} оп/s.

Количеството ключове за взаимодействие N са определени по формулата:

$$N = 2^k, [бр.], \quad (4.5)$$

където: *к* е дължината на използвания от криптографския алгоритъм основен ключ.

4.3.1. Резултати от изчисленията за криптографската устойчивост и анализа на основни блокови криптографски алгоритми



Фиг. 4.27. Графика на зависимостта при различните алгоритми и $n_{op}S_{min}=10^8$

4.1. Изследване на бързодействието на алгоритъма

Изследването на бързодействието на IDA алгоритъма се базира на програмната разработка за целите на дисертацията, използвайки следната конфигурация: CPU Intel Seleron G1820, 2.70 GHz, 4GBRAM, Windows 7 64-bit Operating System. Криптирането се прави само за един блок от явната информация т.е. 64 бита. За сравнение на получения резултат е криптирана същата информация, като са използвани най-близките структура и действие алгоритми, с помощта на Crypto++ 5.6. Получените резултати и изследваните алгоритми са показани на таблица 4.34.

Таблица 4.34. Резултати от изследване на бързодействието на алгоритмите

Алгоритъм	Размер на ключа	Размер на блока	Скорост
DES	64	64	33.6 MB/s
IDEA	128	64	36.7 MB/s
AES	256	128	100.7 MB/s
IDA	256	64	40.0 MB/s
Blowfish	448	64	60.9 MB/s

Както се вижда от таблицата, бързодействието на IDA алгоритъма е достатъчно добро и съизмеримо със световно използваните блокови криптографски алгоритми за криптиране на данни.

4.1. Научно-приложни приноси към Глава 4

4.1.1. Изследвани са заложените пет критерия за структурата на основните нелинейни елементи в IDA алгоритъма, а именно S матриците (S кутиите), определящи нелинейния характер на S матриците и решаващи задачата по противодействие на диференциалния крипто-анализ на алгоритъма, както и помагащи за получаването на добри показатели, свързани със свойството „confusion“.

4.1.2. Изследвани са заложените три критерия за структурата на функцията за разместване на битовете P, обезпечаващи изискването към алгоритъма за свойството „diffusion“.

4.1.3. Изследвано е свойството „лавинен ефект“, определящ високата чувствителност на резултата към изменението на началните данни – всяко малко изменение на открития текст или ключа, трябва да доведе до значително изменение на шифрирания текст.

4.1.4. Предложена е структурна схема на технология за крипто-анализ.

4.1.5. Изследвана е криптографската устойчивост на IDA алгоритъма и други основни блокови криптографски алгоритми, чрез определяне на теоретичната цифрова устойчивост.

4.2. Публикации на автора, свързани с настоящата глава

А6. Иванов И., Ветова С. Оценка за устойчивост на криптографската защита, Национален форум Електроника 2015, стр. 169-172, България.

A7. Ivanov I., Arnaudov R., Vetova S. Analysis of cryptographic protection of block cryptographic algorithms on the base of the theoretical digital stability, ICEST, pp. 45-48, Sofia 2015.

ГЛАВА 6

НАУЧНО-ПРИЛОЖНИ И ПРИЛОЖНИ ПРИНОСИ В ДИСЕРТАЦИЯТА

Научно-приложни приноси

1. Синтезиран е метод и алгоритъм за повишаване на сигурността на данните при предаване на информация в телеметрични системи със специално предназначение и тяхното съхранение. Патент №111513/25.06.2013 [(фиг. 2.2.)], [A2].
2. Предложена е класификация на криптографските алгоритми, като са описани техните предимства и недостатъци. Определени са основните изисквания за реализиране на нов блоков криптографски алгоритъм [A1].
3. Изследвана е функционалността на IDA алгоритъма чрез ръчно разписване на действието му на ниво бит, като по този начин е определена правилната работа на неговата схема, функции, логически и математически операции[A2, A5].
4. Изследвани са определените критерии за структурата на S матриците и функцията P, обезпечаващи изискванията към алгоритъма за свойствата „confusion“ и „diffusion“, както и решаващи задачата по противодействие на диференциалния криптоанализ на алгоритъма, резултата от което показва, че IDA алгоритъмът е с много висока устойчивост на криптографски анализи [(4.1.2., 4.1.3.)].
5. Изследвано е свойството „лавинен ефект“, резултатът от което показва високата чувствителност на резултата от криптирането към изменението на началните данни – всяко малко изменение на открития текст или ключа води до значително изменение на шифрирания текст [(4.2)].
6. Изследвана е криптографската устойчивост на IDA алгоритъма и други основни блокови криптографски алгоритми, чрез определяне на теоретичната цифрова устойчивост и е предложена структурна схема на технология за крипто-анализ, резултатът от което показва, че IDA алгоритъмът е с много висока устойчивост на криптографски атаки [A6, A7].

Приложни приноси

1. Реализирано е програмно приложение на IDA алгоритъма, изпълнено на стандартен език С. Използвана е среда Visual Studio Express 2010 на операционна система Windows7. Отделните последователни фази на алгоритъма са обособени във функции, които се изпълняват в просто конзолно приложение. Не се ползват екзотични или нестандартни библиотечни функции, с цел по-добра съвместимост с различни варианти на езика С [(фиг. 3.1, 3.2)], [А5].

2. Алгоритъмът IDA е внедрен в система, базирана на системата „eCall" и интегрирана със система с допълнителни функции - управление на автопарк, в услуга на собственика или водача, на застрахователи и в помощ на полицията[(фиг. 3.3., 3.4, 3.5)], [А5, П1].

Научни публикации на автора по темата на дисертацията

А.1. Ivanov I. Analysis of cryptographic algorithms - advantages and disadvantages, First International Scientific Conference "Telecommunications, Informatics, Energy and Management TIEM `15" October 15-18, 2015, pp. 114-117, Bitola, Macedonia.

А.2. Иванов И., Диков Д., Арнаудов Р., Метод за повишаване на сигурността на данните при предаване на информация в телеметрични системи със специално предназначение и тяхното съхранение. Заявка за патент №111513/25.06.2013.

А.3. Ivanov I., Algorithm for security and data storage increase using cyclic encryption methods. Известия на Съюза на учените – Русе, Серия 1 „Технически науки", Том 11, 2014, стр. 63-66, България.

А.4. Ivanov I., Vetova S. Cryptography Protection Of Information Data Change In Telecommunication Nets. International conference Robotics, Automation and Mechatronics' 14 – RAM 2014, pp. 55-58, Bulgaria.

А.5. Ivanov I., Vetova S., A Method For Enhancing The Security And Data Storage During Information Transsmission In Telemetry Systems, DCCN, Eighteenth International Scientific Conference, 19–22 october 2015 г., Moscow, Russia, pp. 326 – 330.

А.6. Иванов И., Ветова С. Оценка за устойчивост на криптографската защита, Национален форум Електроника 2015, стр. 169-172, България.

А.7. Ivanov I., Arnaudov R., Vetova S. Analysis of cryptographic protection of block cryptographic algorithms on the base of the theoretical digital stability, ICEST 2015, Sofia, Bulgaria, pp. 45-48.

П.1. Участие и работа по проекта HeERO2 в консорциума на българската пилотна реализация на системата „eCall", 2014.

TECHNICAL UNIVERSITY OF SOFIA

Faculty of Telecommunications

Department of Radio Communications and Video Technology

IVAN DINKOV IVANOV, M.Sc,

METHODS AND ALGORITHMS FOR ADDED SECURITY AND DATA STORAGE TRANSMISSION OF INFORMATION IN TELEMETRY SYSTEMS

ABSTRACT of Ph.D. THESIS

In this dissertation cryptographic methods and algorithms are analyzed as their advantages and disadvantages are highlighted. On the base of this analysis the need to implement a new cryptographic algorithm combining the advantages of block cryptographic algorithms and accounting for their shortcomings [A1] is defined.

A new method and a new cryptographic algorithm for information transmission in telemetry systems with particular usage and high level protection with universal application is developed. The algorithm IDA (Ivanov, Dikov, Arnaudov) [A2] is designed on the base of the DES algorithm and in accordance with Feystel scheme. It is a 64-bit symmetric block cryptographic algorithm using a 256-bit cryptographic key. It consists of 16 inner cycles containing transpositions, substitutions and nonlinear procedures.

The functionality of IDA algorithm is examined using manual submission of its action at bit level, as well as using developed software. Thus, the accurate work of its circuit, functions, logical and mathematical operations [A5] is defined.

The algorithm IDA is implemented in a telemetry system based on the system "eCall" and integrated with a system with extra functions – auto-park management, in service of the owner or driver, of insurers and to help the police [P1].

The specific criteria for the structure of S matrix and function P which satisfy the requirements towards the algorithm for "confusion" and "diffusion" properties as well as solving the task for counteraction of the differential cryptanalysis of the algorithm are examined.

Yet, this work concerns and examines the "avalanche effect" property, which defines the high sensitivity of the result towards change of the initial data.