



ВИСШЕ УЧИЛИЩЕ ПО ТЕЛЕКОМУНИКАЦИИ И ПОЩИ

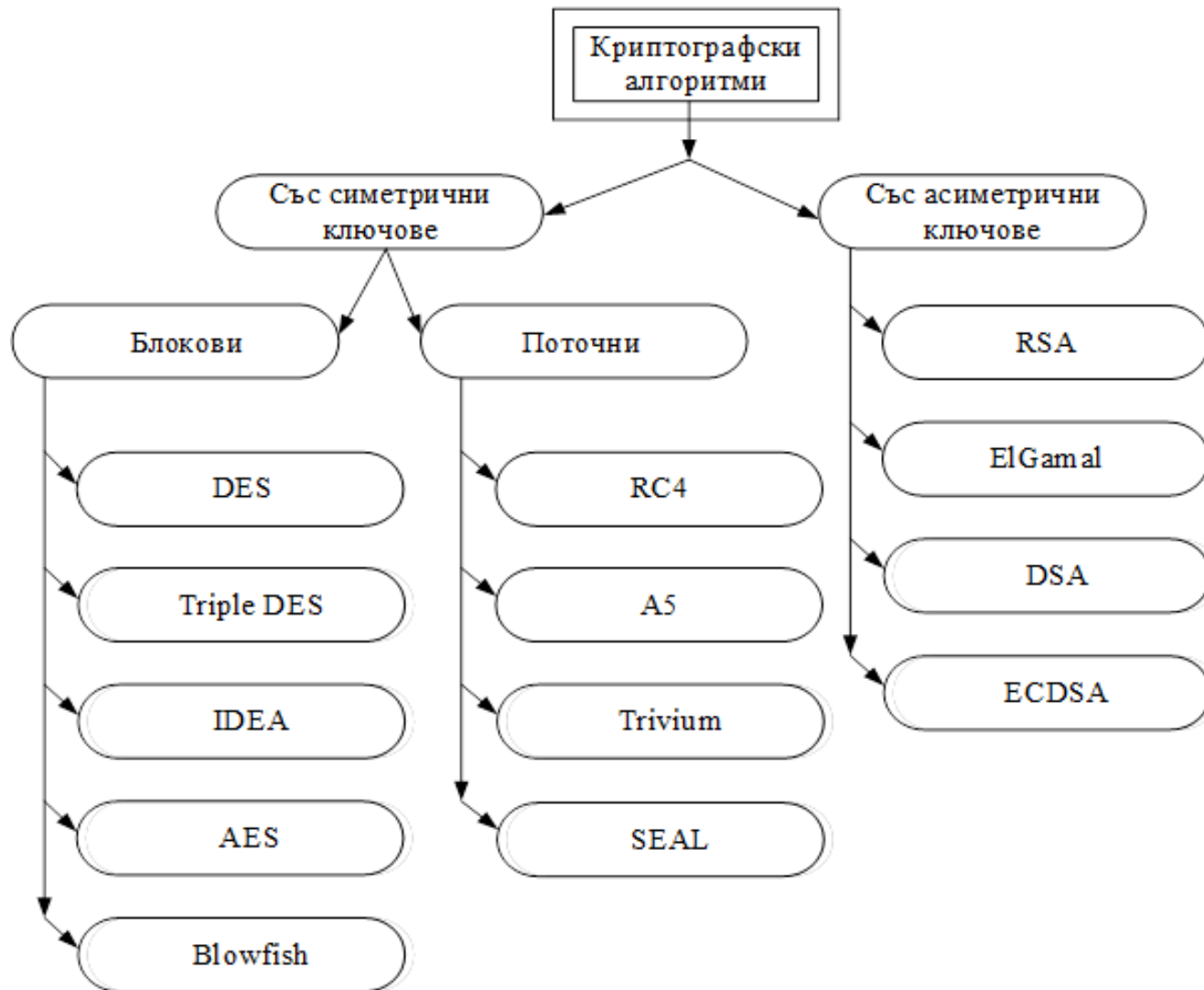
**ТЕМА: БЛОКОВ КРИПТОГРАФСКИ АЛГОРИТЪМ
IDA**

гл. ас. д-р инж. Иван Иванов



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.

Криптографските алгоритми са един от начините за защита на информацията, като е много важно задълбоченото анализиране на целият жизнен цикъл на информацията, т.е. от нейното създаване, пренасяне и съхранение, както и правилният избор на подходящ алгоритъм за нейната защита.



Обща класификация на криптографските алгоритми



Описание на алгоритъма

Алгоритъмът IDA (Ivanov, Dikov, Arnaudov) 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.

На базата на разработената схема се постигат следните резултати:

- Въвежда се реалното използване на 256-битов основен ключ;
- Заложената е възможност за промяна дължината на ключа на 512, 1024 и 2048 бита, без да е необходима промяна на функционалната схема;
- 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.



Обща блокова схема на алгоритъма за криптиране **IDA**



Изследвана е функционалността на IDA алгоритъма чрез ръчно представяне на действието му на ниво бит, както и чрез програмна разработка, като по този начин е определена правилната работа на неговата схема, функции, логически и математически операции. Направените изследвания и оценки доказват, че алгоритъмът е приложим както в 64-битови процесори с общо предназначение, така и за 32-битови вградени микроконтролери.



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. 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.

Name	Date modified	Type	Size
out	20.6.2016 г. 16:18 ч.	Text Document	31 KB
key	20.6.2016 г. 16:15 ч.	Text Document	1 KB
inp	20.6.2016 г. 16:15 ч.	Text Document	1 KB
code_key256	11.7.2014 г. 13:49 ч.	Application	16 KB

Наименование и вид на файловете за тестване

```

out - Notepad
File Edit Format View Help
Reading "key.txt"
key = 11101010 11101110 11110000 11100101 11101010 11110010 11101110 11110000
00100000 11101101 11100000 00100000 11110010 11101011 11100101 11100101
11101010 11101110 11101100 11110011 11101101 11101000 11101010 11100000
11110110 11101000 11101110 11101101 11101101 11101000 11110010 11100101

Reading "inp.txt"
encrypting block:
Block = 11110010 11100101 11101011 11100101 11110100 11101110 11101101 11101000

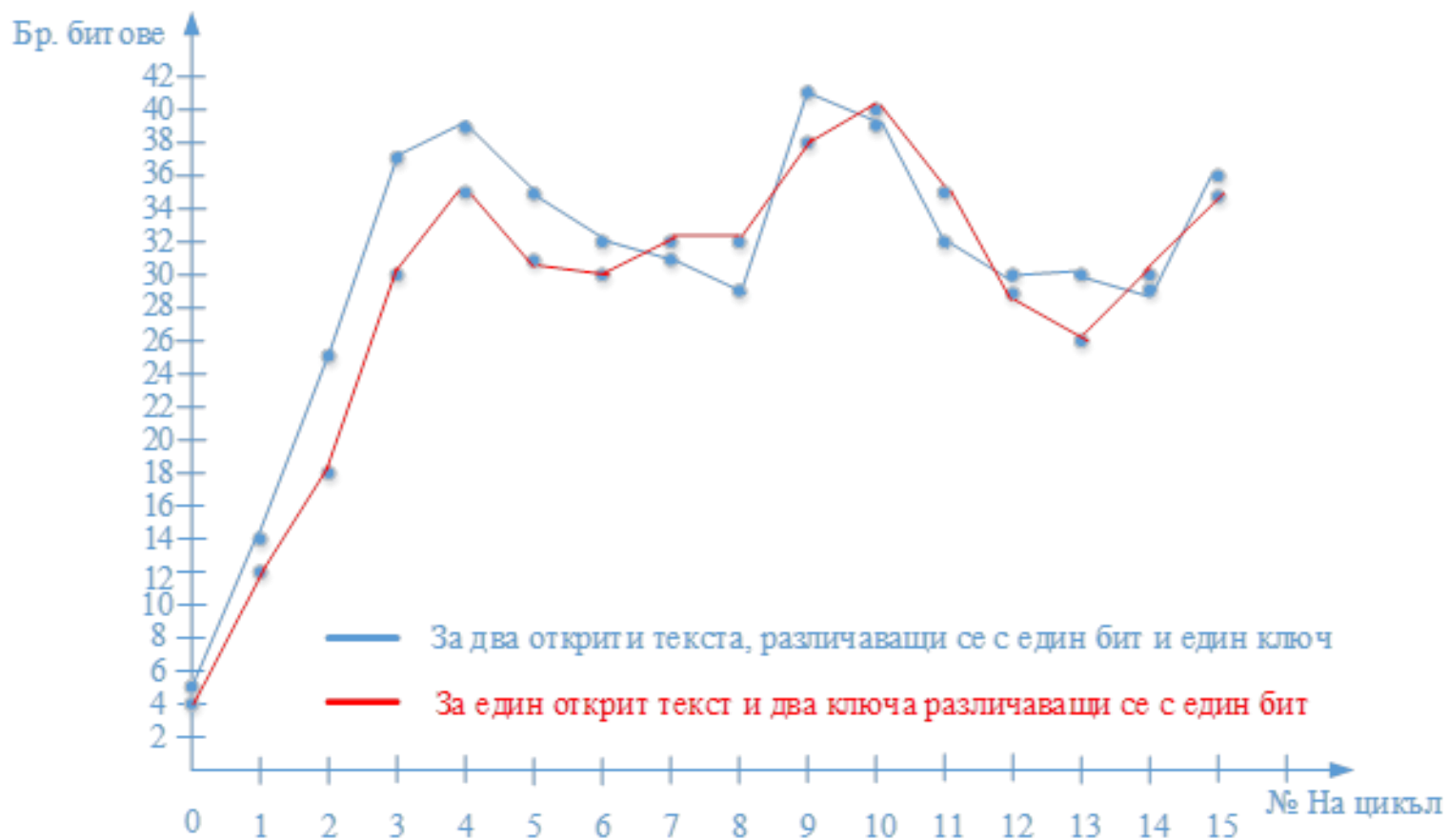
Iteration #01:
Inpt = 11111111 00010001 01111010 01001110
InpR = 11111111 11111111 11100100 00100101
Left part encoding:
K1 = 11101010 11101110 11110000 11100101 11101010 11110010
EXP = 01111111 11101000 10100010 10111111 01000010 01011101
XDR = 10010101 00000110 01010010 01011010 10101000 10101111
S(8) = 10001001 11000010 11111000 01001101
POR = 00111001 11011101 01001001 10100000
K3 = 11110010 11100101 11101011 11100101
L0 = 11001011 00111000 10100010 01000101
Right part encoding:
K2 = 11101110 11110000 00100000 11101101 11100000 00100000
EXP = 11111111 11111111 11111111 11110000 10000001 00001011
XDR = 00010001 00001111 11011111 00011101 01100001 00101011
S(8) = 11011001 11001001 11000100 00101010
POR = 10001001 10001111 11000101 01001010
K4 = 11101010 11101110 11101100 11110011
R0 = 01100011 01100001 00101001 10111001

-----
Iteration #02:
Inpt = 01100011 01100001 00101001 10111001
InpR = 11001011 00111000 10100010 01000101
Left part encoding:
K5 = 11101101 11101000 11101010 11100000 11110110 11101000
EXP = 10110000 01101011 00000010 10010101 00111101 11110010
XDR = 01011101 10000011 11101000 01110101 11001011 00011010
S(8) = 10111100 10101100 10000101 01110000
P11 = 00000011 10011000 00110111 01011110
K7 = 11001011 11010101 11100101 11011101

```

Резултат от тестването на програмната разработка

РЕЗУЛТАТИ ОТ ИЗСЛЕДВАНИЯТА НА АЛГОРИТЪМА



Резултати на свойството „лавинен ефект“ в IDA алгоритъма



Същност на метода с теоретично цифровата устойчивост

Теоретичната цифрова устойчивост е оценка, която се дава при условие, че криптографският алгоритъм е качествен и не може да бъде преодоляван чрез ускорени атаки за крипто-анализ, а само чрез методи на “грубата сила”.

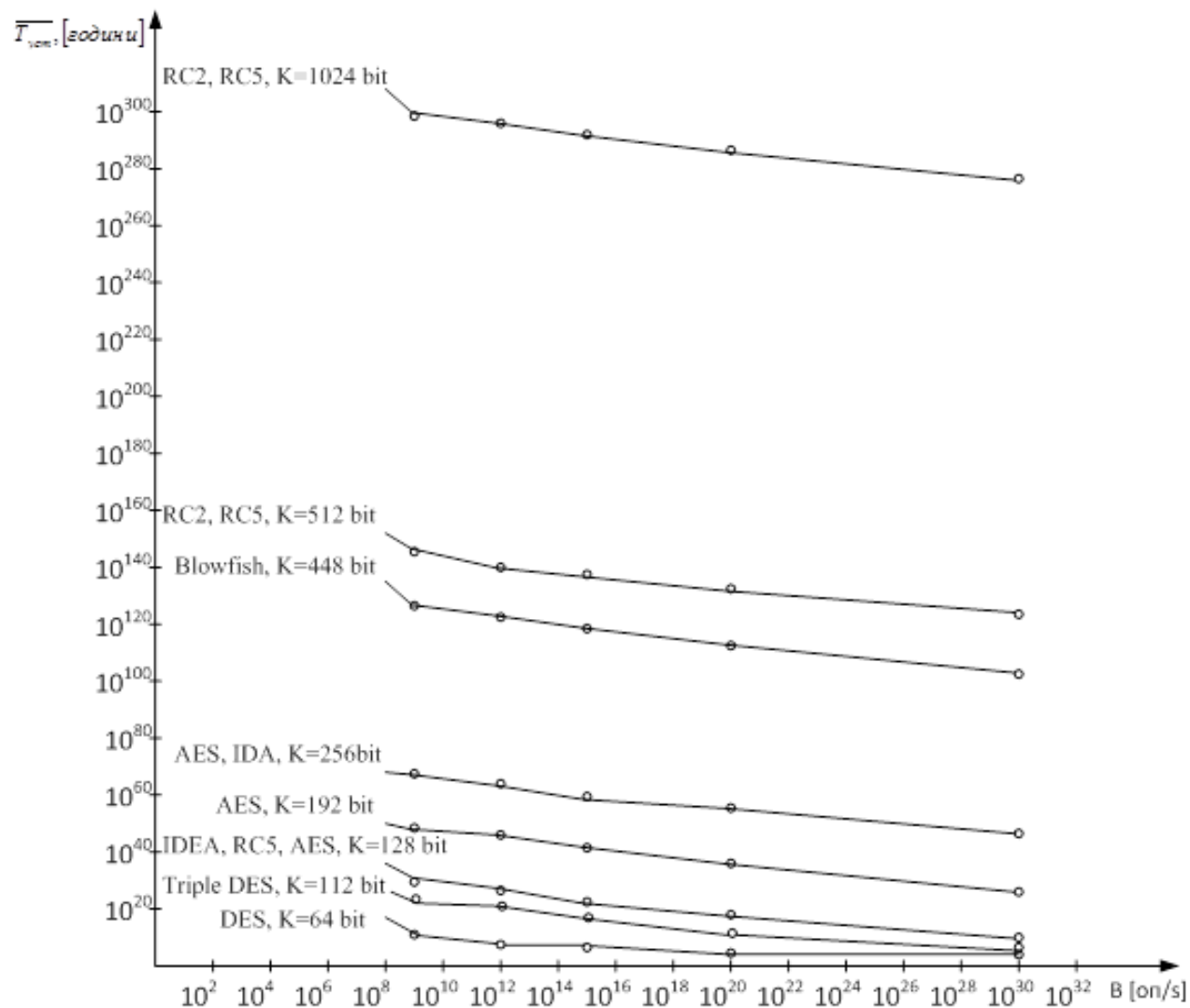
$$\overline{T}_{уст} \approx \frac{Nn_{op}S_{min}}{6B} 10^{-7}, [години]$$

На следващата фигурата е показана зависимостта на теоретичната цифрова устойчивост, количеството ключове за взаимодействие N при $porS_{min}=10^5$ 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:

$$N = 2^k, [бр.],$$

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

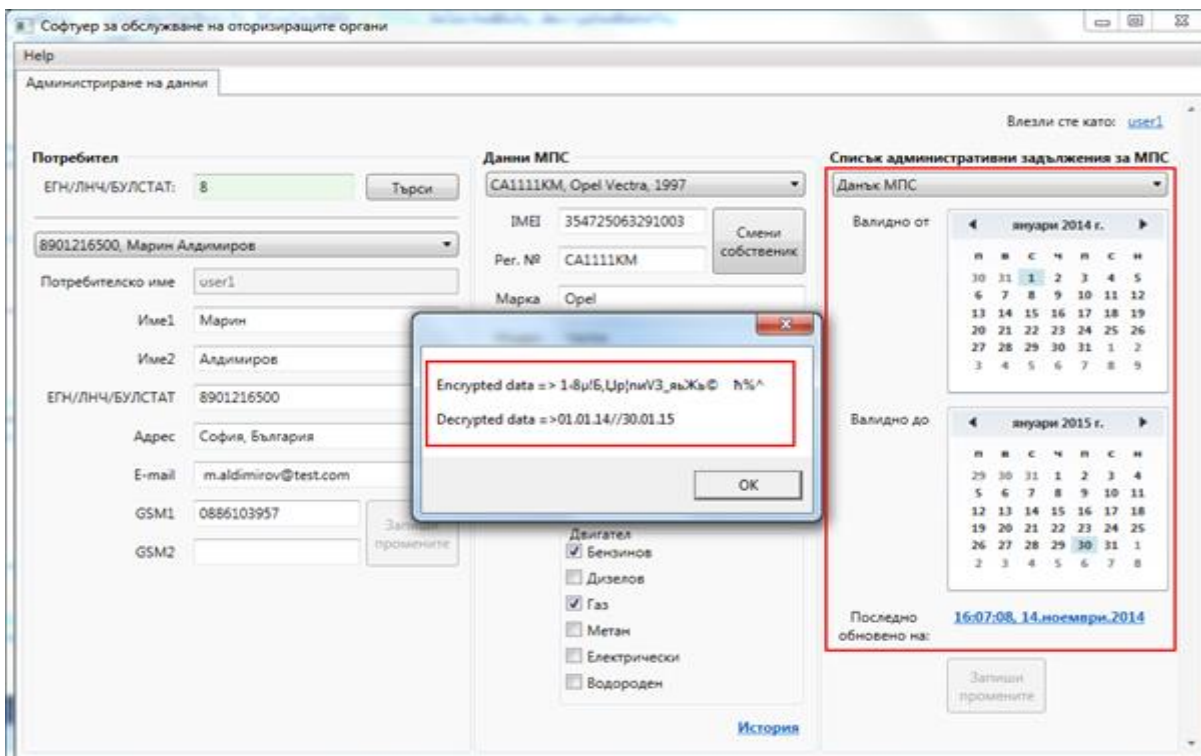


Графика на зависимостта при различните алгоритми и $n_{\text{оп}} S_{\min} = 10^8$

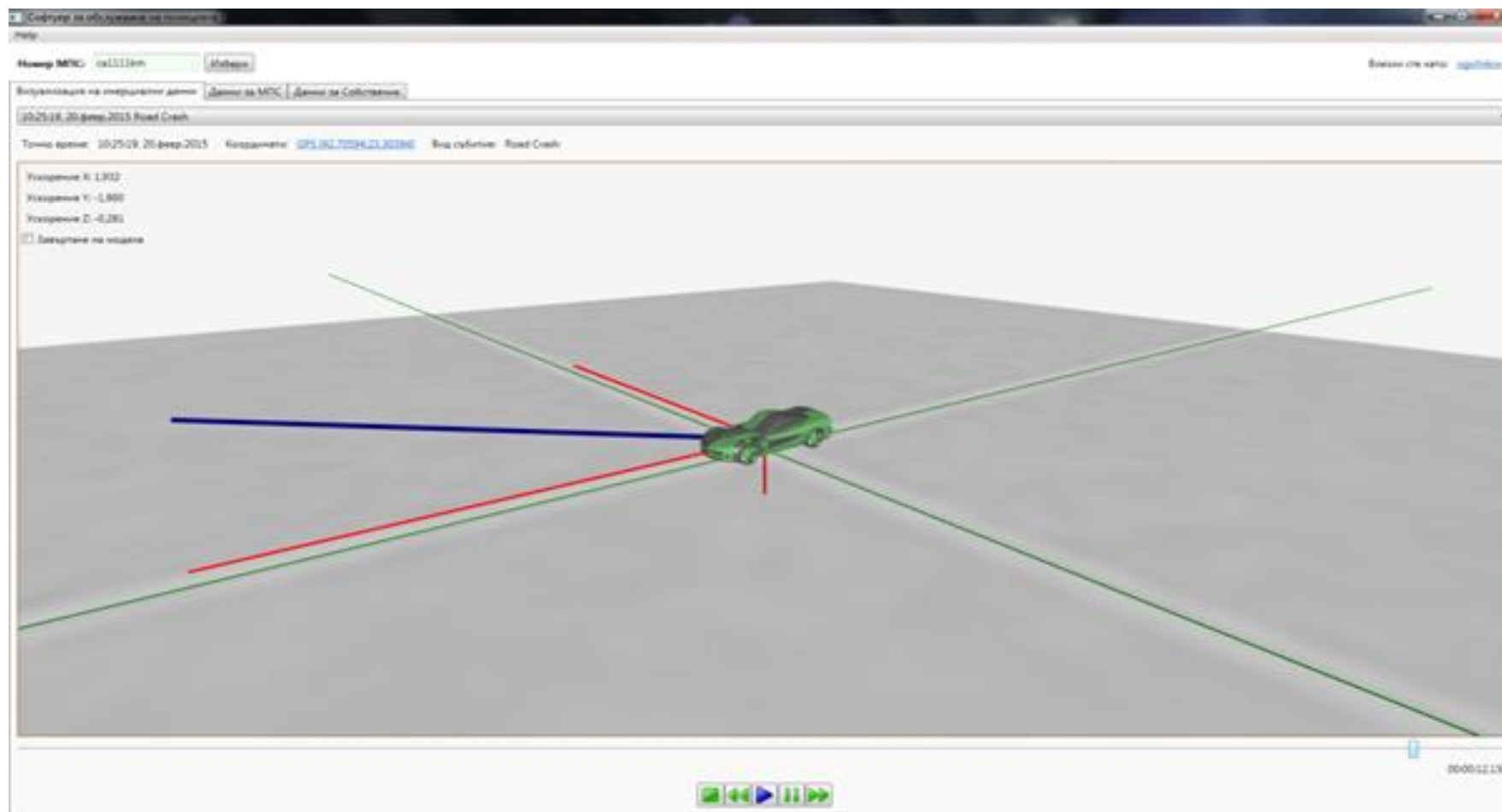
Внедряване на IDA алгоритъма

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, както следва:

- В софтуера за обслужване на собственика или водача на МПС;
- В софтуера за ползване от оторизирани органи и застрахователи;
- В софтуер за обслужване на полицията;



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



Визуализация на декриптираните инерциални данни в софтуера за полицията



[Начало](#) > [Търсене с ВРО онлайн](#) > [Търсене на Патент](#) > Преглед - 111 513

Изобретение заявка № 111513

справка към 11.02.2017 01:21



Запази в PDF



Отвори всички



Затвори всички



Обратно

(1 от 1)

Основни данни

Номер на заявка
Защитен номер

111513

Дата на заявяване
Дата на
издаване/регистрация
Статус

25.06.2013

ПТ В Експертиза

Срок на закрила
Наименование

МЕТОД ЗА ПОВИШАВАНЕ НА СИГУРНОСТТА НА ДАННИТЕ ПРИ ПРЕДАВАНЕ НА ИНФОРМАЦИЯ В ТЕЛЕМЕТРИЧНИ СИСТЕМИ СЪС СПЕЦИАЛНО ПРЕДНАЗНАЧЕНИЕ И ТЯХНОТО СЪХРАНЕНИЕ



ВИСШЕ УЧИЛИЩЕ ПО ТЕЛЕКОМУНИКАЦИИ И ПОЩИ

БЛАГОДАРЯ ЗА ВНИМАНИЕТО !

