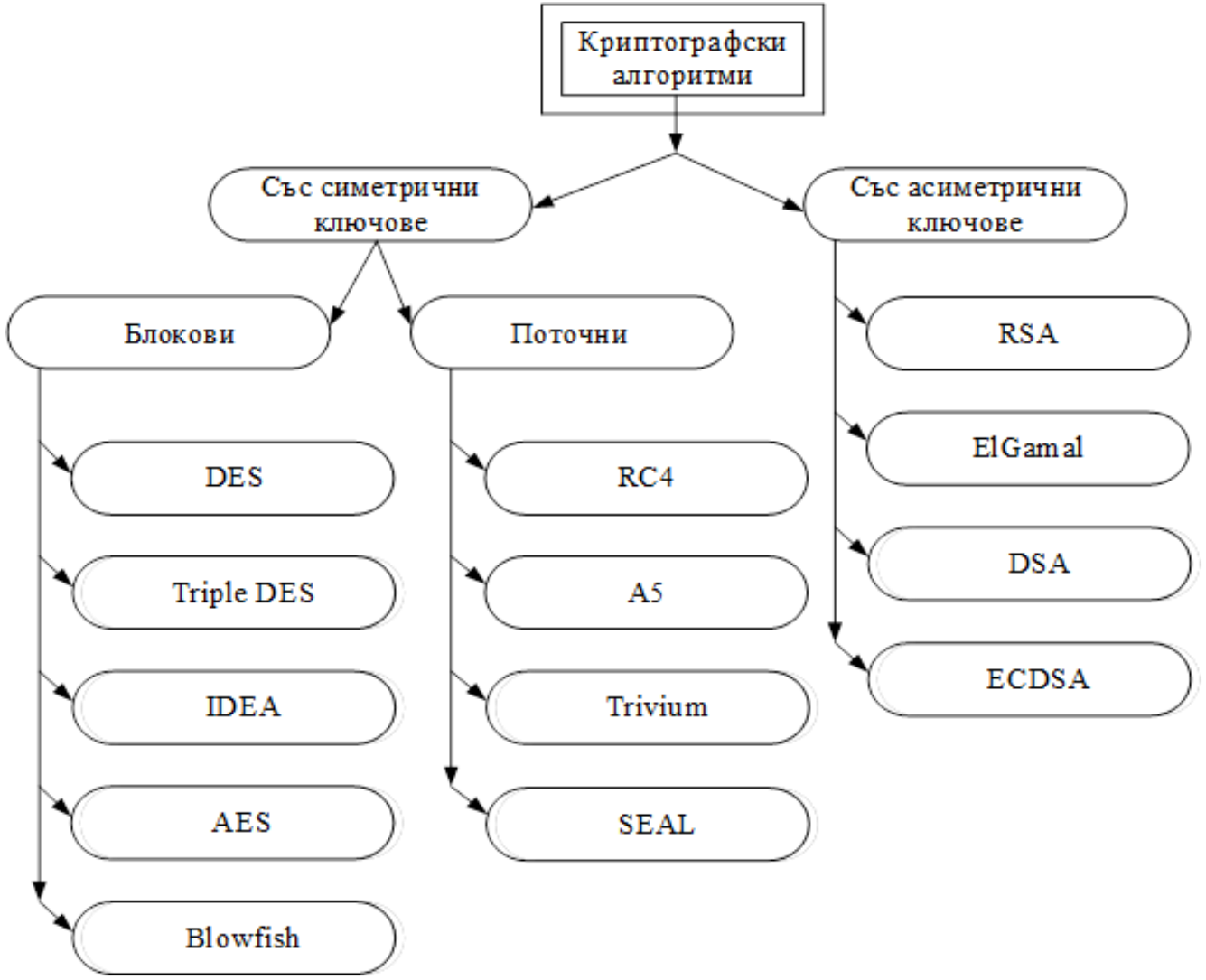
ТЕМА: БЛОКОВ КРИПТОГРАФСКИ АЛГОРИТЪМ IDA

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:

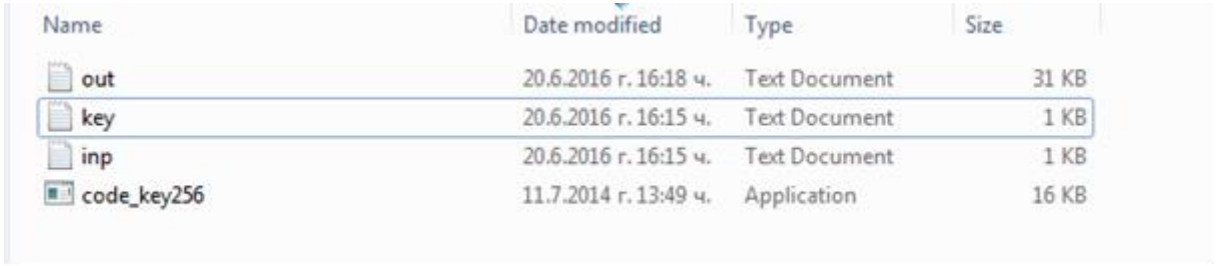
- Въвежда се реалното използване на 256-битов основен ключ;
- Заложената е възможност за промяна дължината на ключа на 512, 1024 и 2048 бита, без да е необходима промяна на функционалната схема;
- Използват се по два 48-битови и два 32-битови под-ключа на всеки цикъл;
- Общо използваните под-ключове 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**

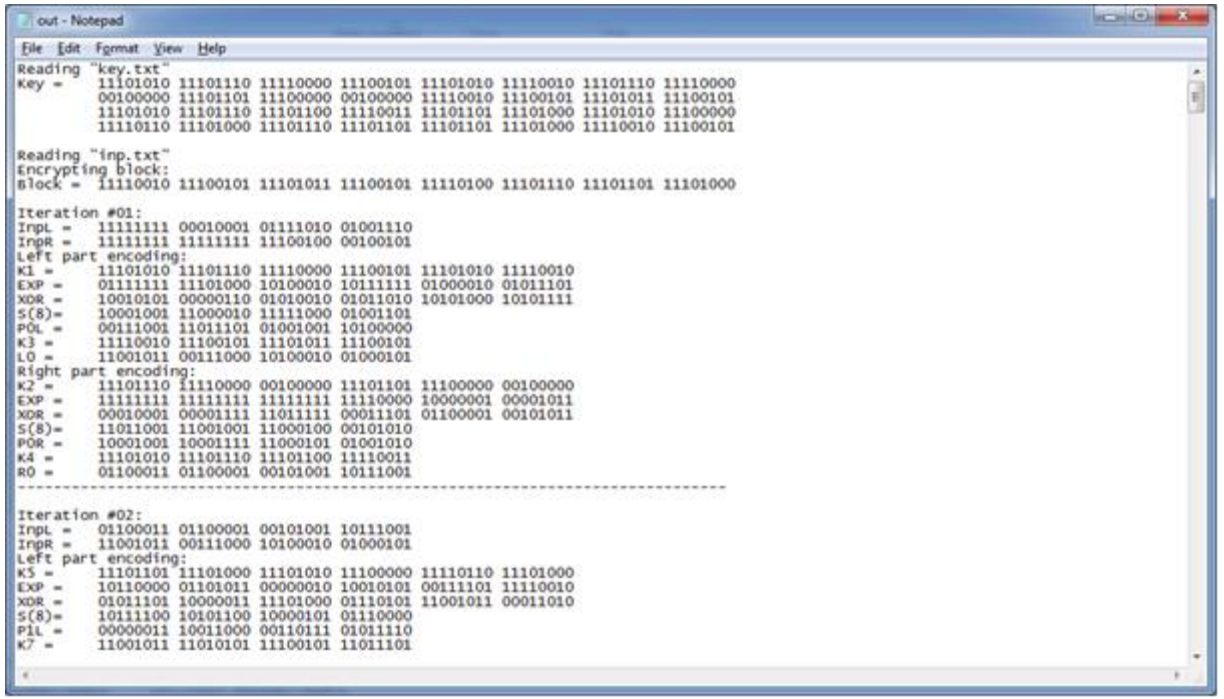
Изследвана е функционалността на IDA алгоритъма чрез ръчно представяне на действието му на ниво бит, както и чрез програмна разработка, като по този начин е определена правилната работа на неговата схема, функции, логически и математически операции. Направените изследвания и оценки доказват, че алгоритъмът 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.

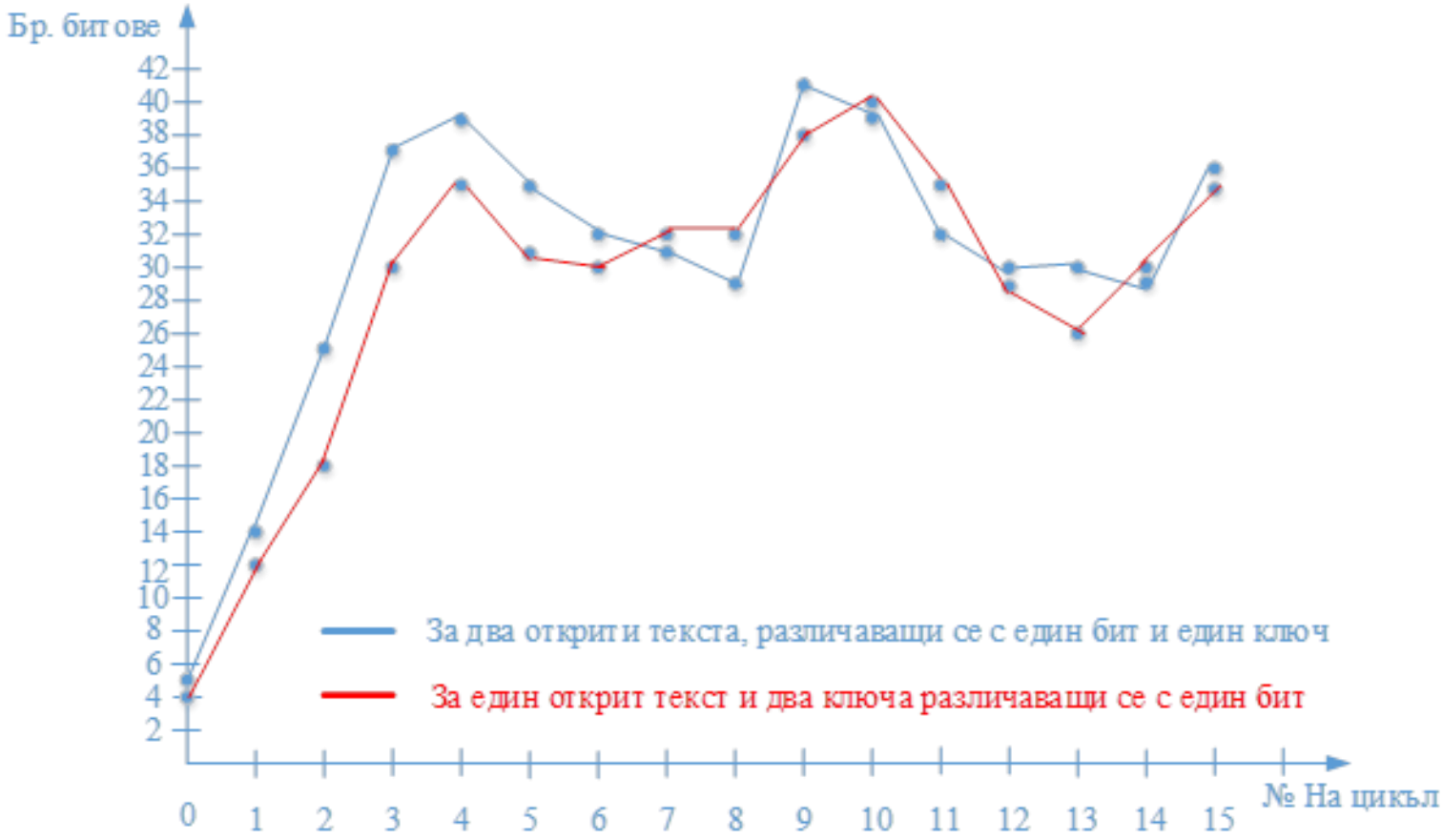


Наименование и вид на файловете за тестване



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”.

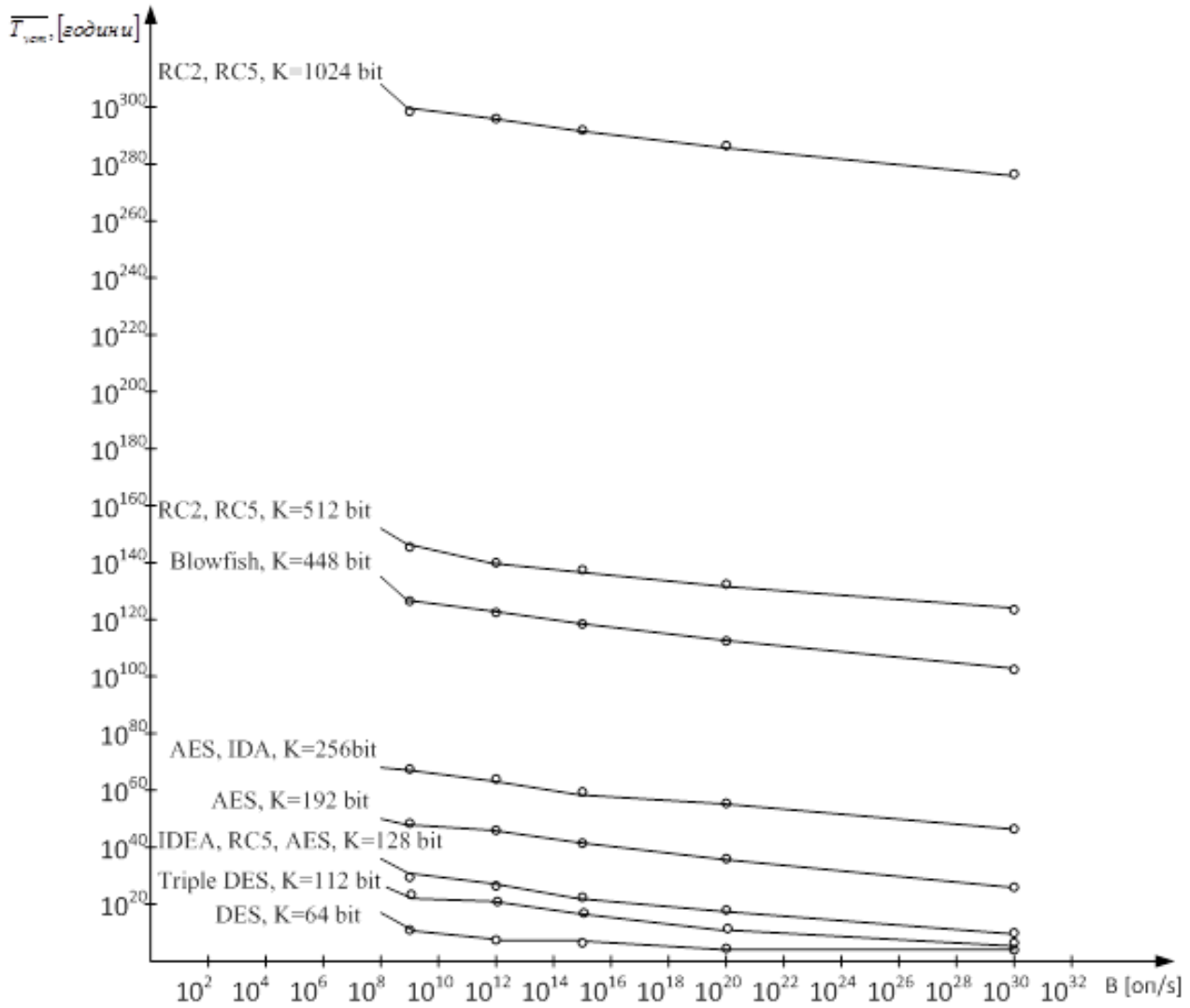
$$\overline{T_{уст}} \approx \frac{N n_{op} S_{\min}}{6B} 10^{-7}, [години]$$

На следващата фигурата е показана зависимостта на теоретичната цифрова устойчивост, количеството ключове за взаимодействие N при nopSmin=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: к е дължината на използвания от криптографския алгоритъм основен ключ.

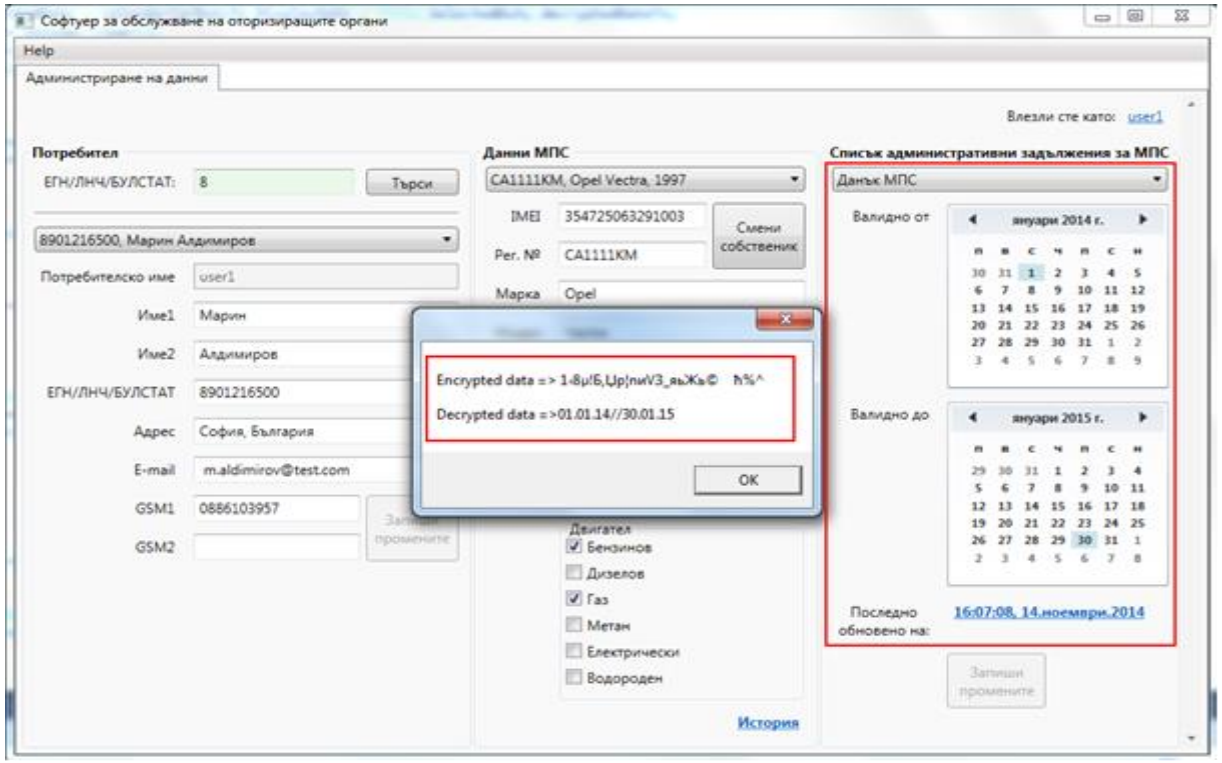


Графика на зависимостта при различните алгоритми и $n_{op}S_{min}=10^8$

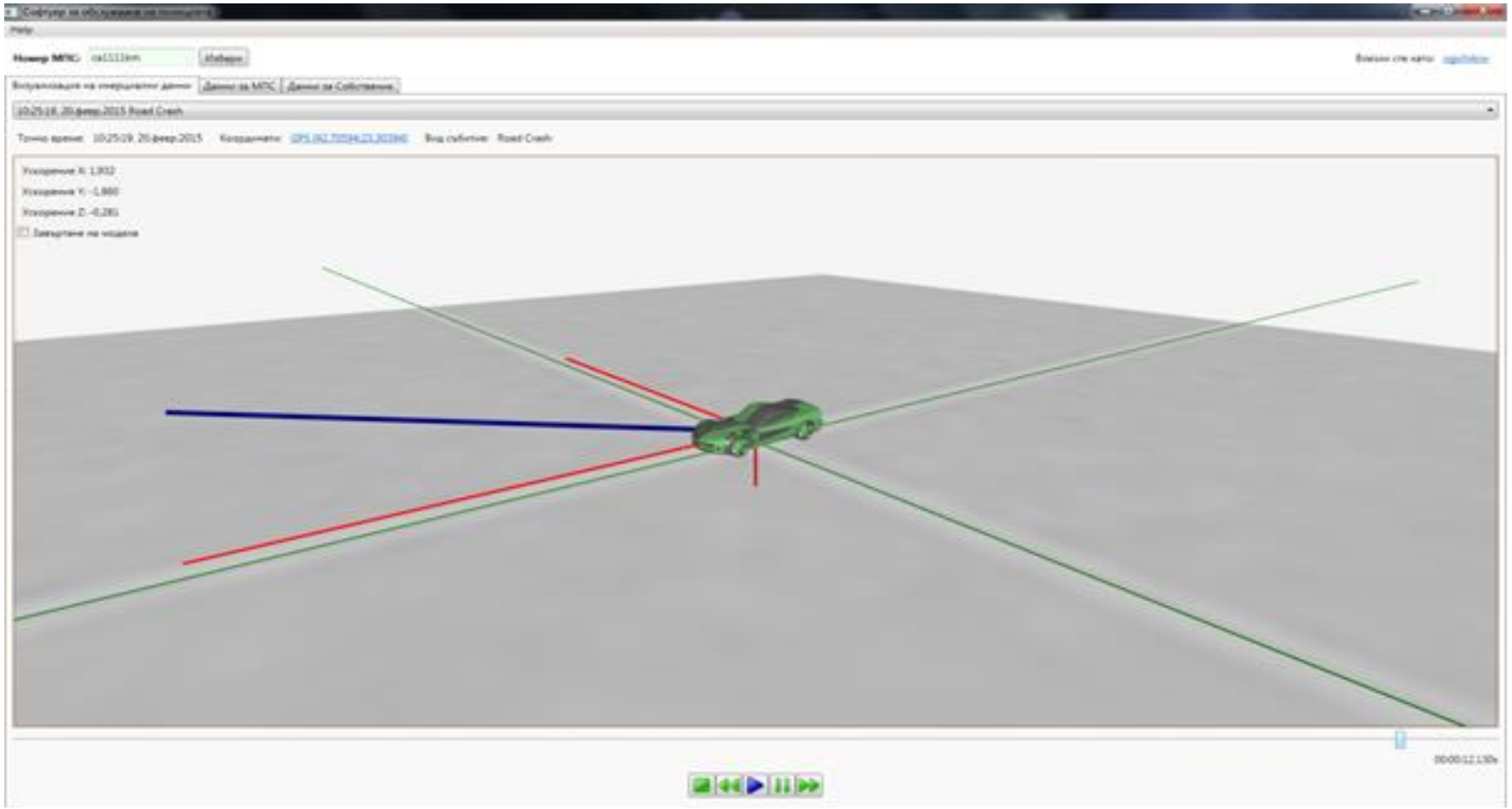
Внедряване на IDA алгоритъма

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:

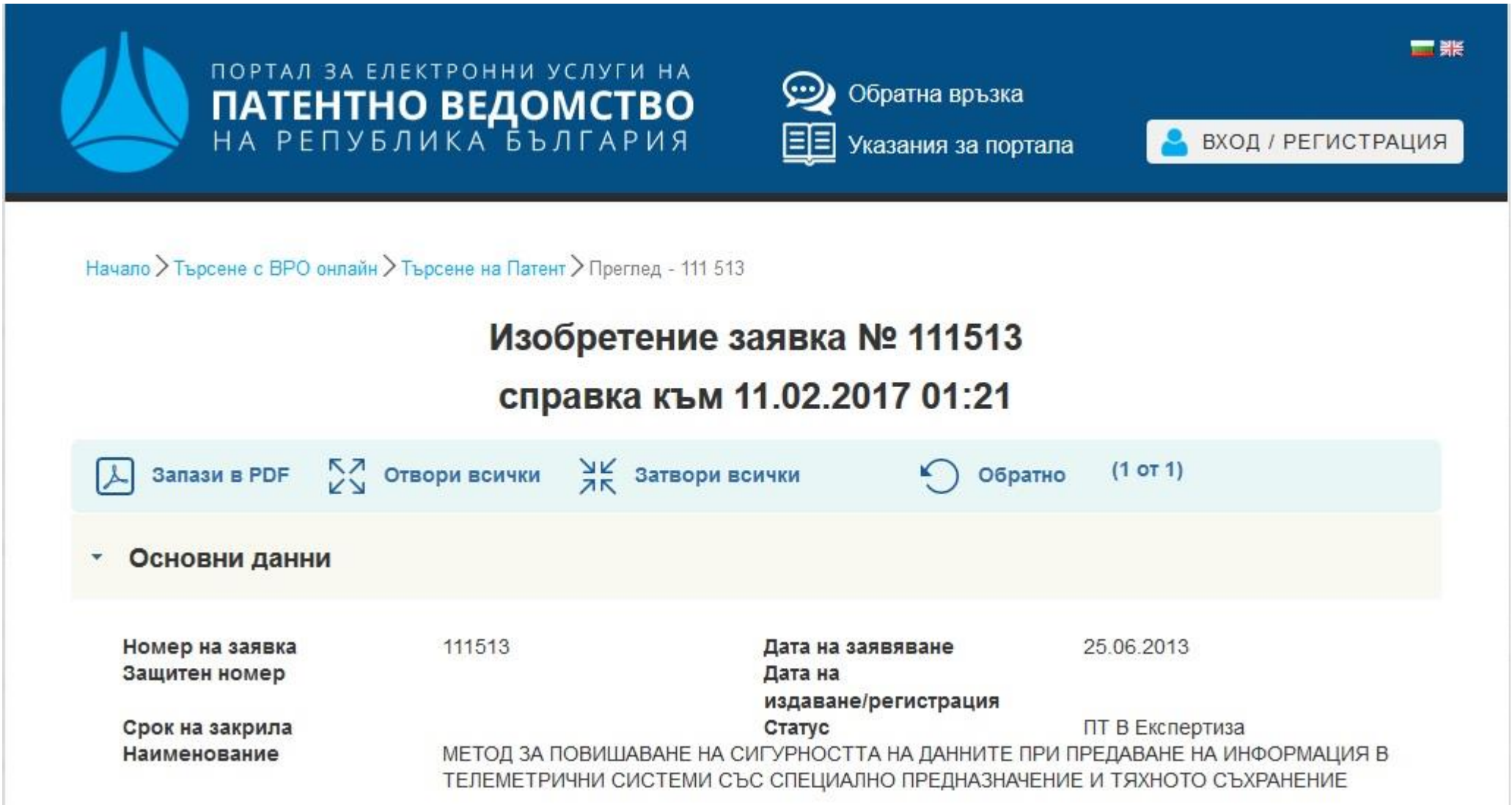
- **В софтуера за обслужване на собственика или водача на МПС;**
- **В софтуера за ползване от оторизирани органи и застрахователи;**
- **В софтуер за обслужване на полицията;**



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



Визуализация на декриптираните инерциални данни в софтуера за полицията



ПОРТАЛ ЗА ЕЛЕКТРОННИ УСЛУГИ НА
ПАТЕНТНО ВЕДОМСТВО
НА РЕПУБЛИКА БЪЛГАРИЯ

Обратна връзка
Указания за портала
ВХОД / РЕГИСТРАЦИЯ

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	111513	**Дата на заявяване**	25.06.2013
Защитен номер		**Дата на издаване/регистрация**	
Срок на закрила		**Статус**	ПТ В Експертиза
Наименование	МЕТОД ЗА ПОВИШАВАНЕ НА СИГУРНОСТТА НА ДАННИТЕ ПРИ ПРЕДАВАНЕ НА ИНФОРМАЦИЯ В ТЕЛЕМЕТРИЧНИ СИСТЕМИ СЪС СПЕЦИАЛНО ПРЕДНАЗНАЧЕНИЕ И ТЯХНОТО СЪХРАНЕНИЕ		

БЛАГОДАРЯ ЗА ВНИМАНИЕТО !