

Выгрузка BIOS устройства «Криптон-4»

- аппаратура **КРИПТОН-3 –4К/16** обеспечивает генерацию имитоприставки (имитовставки) длиной 4 байта в соответствии с **ГОСТ 28147-89**;
- выгрузка BIOS устройства «**Криптон-4**» в память компьютера значительно повышает скорость шифрования. Эту операцию можно осуществить одним из двух способов:
 1. в **Setup** компьютера установить **Shadow RAM** по адресу **BIOS Криптон** в состояние **Enabled, Cached** или **Into-486**;
 2. после инициализации устройства запустить программу **crtover.com**, поставляемую в составе базового ПО(можно в **autoexec.bat**).

Инсталляция программ *Crypton API* для работы устройства КРИПТОН-8/PCI в среде WINDOWS-95/98/NT4.0/ 2000

- инсталляция программ *Crypton API* для работы устройства *КРИПТОН-8/PCI* в среде *WINDOWS-95/98/NT4.0/ 2000* выполняется до установки платы в компьютер по следующему алгоритму:
 1. открыть на дискете , входящей в комплект поставки, каталог *Crypton API*;
 2. запустить программу *install.exe*;
- установка *API* произойдет автоматически;
- для размещения программ *Crypton API* потребуется около 2.0 Мбайт свободного пространства на жестком диске.

Функции прерываний

- существует возможность разработать свое собственное ПО для работы с криптоплатой;
- обращение к шифратору осуществляется через прерывание *4Ch*;
- код функции, которая должна быть выполнена, передается через регистр *AL*;
- при возникновении ошибки *Carry_flag = 1*;

Функции прерываний

- значения кодов функций приведены ниже:
 - **0(1)** - зашифрование данных на ключе ФК в режиме гаммирования (гаммирования с самовосстановлением);
 - **2(3)** - расшифрование данных на ключе ФК в режиме гаммирования (гаммирования с самовосстановлением).
 - **CX**=число байт выходной информации (кратно 8 байт без синхропосылки);
 - **DS:SI**=>адрес входного буфера с исходной открытой (зашифрованной) информацией;
 - **ES:DI**=>адрес выходного буфера с выходной зашифрованной (расшифрованной) информацией. При шифровании 8 первых байт в обоих буферах синхропосылка, все остальные байты - расшифровываемая информация. При расшифровке синхропосылка в выходной буфер не передается.
Синхропосылка не учитывается при задании длины данных. Длина данных должна быть кратна 8 байтам;

Функции прерываний

- **4(8)** - ввод ключа ФК и расшифрование его на ключе ПК(ГК);
- **6** - ввод ключа ПК и расшифрование его на ключе ГК;
- **10** - ввод ключа ФК и расшифрование его на ключе ГК (аналогично режиму 8), но при вводе данные запрашиваются с ДСЧ;
- **12-14** - ввод ключа ФК(ПК*, ГК*) без расшифрования:
 - **DS:SI**=>адрес буфера с 32 байтами ключевой информации;
- **5(9)** - вывод ключа ФК, зашифрованного на ключе ПК (ГК);
- **7(11)** - вывод ключа ПК, зашифрованного на ключе ГК (ФК):
 - **ES:DI**=>адрес буфера для записи 32 байт ключевой информации;

Функции прерываний

- **15*** - ввод узла замены (УЗ) (долговременного ключа) без расшифрования:
 - **DS:SI**=>адрес буфера с 64 байтами узла замены;
- **16** - выработка имитоприставки для входных данных на ключе ФК:
 - **CX**=число байт исходной информации;
 - **DS:SI**=>адрес буфера с исходной информацией;
 - **ES:DI**=>адрес буфера для 4 байт имитоприставки;
- **17,20** - выработка имитоприставки для ключа ФК на ключе ПК (ГК);
- **18,19** - выработка имитоприставки для ключа ПК на ключе ГК (ФК):
 - **ES:DI**=>адрес буфера для 4 байт имитоприставки;

Функции прерываний

- **21** - перезапись ФК на место ГК с одновременным стиранием ФК на старом месте;
- **22** - обращение к ДСЧ:
 - ***CX***=число байт, считываемых с ДСЧ;
 - ***ES:DI***=>адрес буфера для записи случайных чисел;
- **23** - сброс устройства:
 - ***выход: AH***=версия BIOS-а платы
 - ***AL*** = модификация версии BIOS-а платы или код 23, если плата не инициализирована;
 - ***примечание:*** после сброса вся ключевая информация в плате сохраняется;

Функции прерываний

- **24** - зашифрование данных на ключе ФК в режиме гаммирования с самовосстановлением:
 - **АН**=число блоков информации по 512 байт - макс. 127 блоков(т.е. 64Кбайт)
 - **СХ**=младшее слово синхропосылки
 - **DX**=старшее слово синхропосылки
 - **DS:SI**=>адрес буфера с исходной (открытой) информацией
 - **ES:DI**=>адрес буфера с выходной (зашифрованной) информацией
 - **примечание:** для зашифрования каждого блока берется синхропосылка из регистров СХ и DX. Перед зашифрованием следующего блока синхропосылка увеличивается на 1;
- **25** - получение номера платы:
 - **СХ** = число необходимых байт;
 - **ES:DI**=>адрес буфера для записи номера;
 - **выход:** **АН**=версия BIOS-а платы;
 - **AL**=модификация версии BIOS-а платы;
 - **ES:DI**=>строка с номером;
 - первые 4 байта есть номер платы в двоично-десятичном упакованном формате. Если **СХ**=0, то возвращается только регистр **АХ**.

Функции прерываний

– 26 - расшифрование данных на ключе К1 в режиме гаммирования с самовосстановлением:

- AH =число блоков информации по 512 байт - макс. 127 блоков (т.е. 64Кбайт);
- CX, DX =младшее, старшее слово синхропосылки;
- $DS:SI$ =>адрес буфера с исходной (зашифрованной) информацией;
- $ES:DI$ =>адрес буфера с выходной (расшифрованной) информацией;
- *примечание:* для расшифрования каждого блока берется синхропосылка из регистров CX и DX . Перед расшифрованием следующего блока синхропосылка увеличивается на 1;

– 27* - тестирование платы:

- $DS:ES$ =>сегмент буфера для размещения тестовой информации длиной не менее 4 Кбайт;
- $SI=DI=0$;
- *примечание:* после выполнения теста состояние УЗ и ГК не определено. Плата находится в начальном состоянии, требующем инициализации, т.е. ввода УЗ и ГК;

Функции прерываний

- **28*** - проверка состояния платы:
 - выход:
 - $CF=0$ указывает, что плата уже инициализирована;
 - $CF=1$ указывает на начальное состояние платы (необходимость загрузки УЗ и ГК;
- **29** - обращение к ДСЧ с контролем:
 - $ES:DI \Rightarrow$ адрес буфера для записи 512 байт случайных чисел;
- **30** - установка недоверных ГК:
 - загружаются разные ГК в СБИС узла шифрования. Функция применяется для установки аппаратуры в начальное состояние, требующее инициализации, т.е. ввода УЗ и ГК;
- **31** - получение режима работы платы (значений переключателей):
 - выход: AL =инверсное значение переключателей - код режима(3 младших бита переключателя);

Функции прерываний

- шифрование ключевой информации выполняется в режиме простой замены, в соответствии с *ГОСТ 28147-89*;
- для генерации ключей ФК и ПК рекомендуется использовать данные с ДСЧ (функция BIOS 22). Значения ключей ФК и ПК, считанные с ДСЧ, можно считать уже зашифрованными;
- для генерации ГК рекомендуется использовать данные с ДСЧ с контролем (функция BIOS 29);
- для шифрования блока данных необходима синхропосылка, которая не является секретной и может передаваться по каналам связи и храниться на внешних носителях в открытом виде;
- для генерации синхропосылки рекомендуется использовать данные с ДСЧ (функция BIOS 22);

Пакет программ Crypton API 2.2

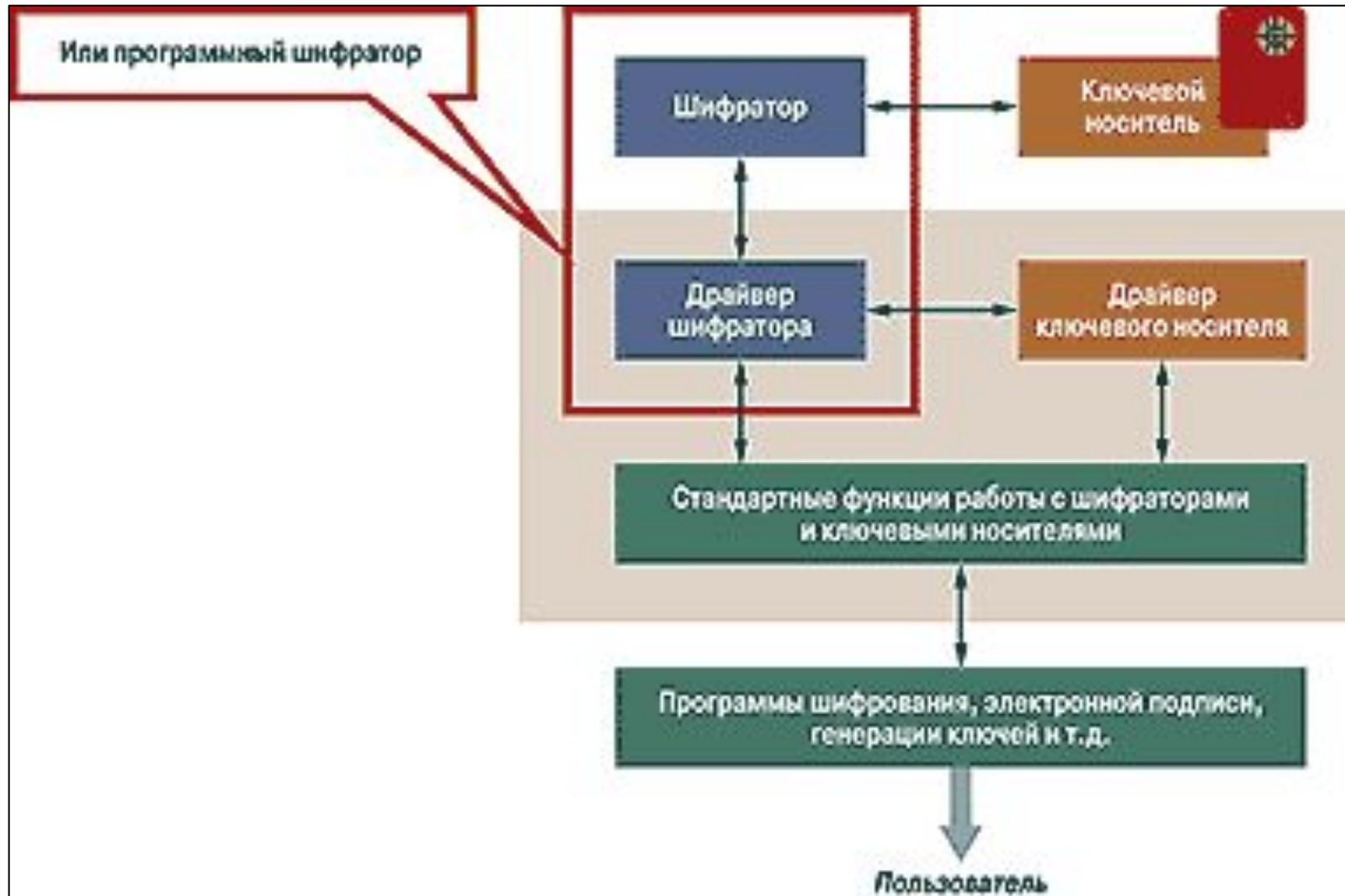
Использование универсального программного интерфейса *Crypton API*

- т.к. в многозадачных ОС, например, Windows шифратор может получать команды сразу от нескольких программ, то *во избежание возникновения коллизий программы не имеют прямого доступа к шифратору* и управляют им с помощью специальных программных *API-модулей*, а именно универсального программного интерфейса *Crypton API*;

Использование универсального программного интерфейса Cryption API

- *в функции* данного *API* входит обеспечение корректного последовательного выполнения шифратором команд, инициированных различными программами:
 - для каждой программы создается отдельная сессия шифрования;
 - ресурсы шифратора поочередно переключаются между сессиями;
 - каждая сессия имеет собственный виртуальный шифратор со своими ключами шифрования, которые перезагружаются при переключении между сессиями. Это несколько напоминает разделение ресурсов ПК между приложениями в многозадачной операционной системе.

Использование универсального программного интерфейса Crypton API



Использование универсального программного интерфейса Cryptedon API

- кроме того, *API* поддерживает возможность ***подключения различных типов шифраторов*** через драйверы со стандартным набором функций. Это ***исключает зависимость прикладной программы от конкретного типа шифратора***. Например, вместо аппаратного шифратора можно использовать программный - ***Cryptedon Emulator***, работающий на уровне ядра операционной системы;
- таким образом, при обращении программы к ***УКЗД*** любая команда проходит четыре уровня:
 - приложений;
 - интерфейса между приложением и драйвером УКЗД;
 - ядра операционной системы - драйвера УКЗД;
 - аппаратный (собственно уровень шифратора).

Пакет программ Crypton API 2.2

- обеспечивает программный интерфейс к устройствам криптографической защиты данных (УКЗД) серии «Криптон» для приложений **Win32** и программ ДОС в режиме эмуляции ДОС в операционных средах **Windows 9x/NT/ 2000/2003**;
- в состав данного пакета программ входят:
 - драйверы УКЗД;
 - драйверы поддержки ДОС приложений в режиме эмуляции ДОС;
 - **Win32**-приложение, тестирующее УКЗД.

Программа конфигурации драйвера оборудования

«Driver setup» (*DrvSetup.exe*)

- *Программа конфигурации драйвера оборудования «Driver setup» (DrvSetup.exe) позволяет:*
 - получить информацию о версии и производителе текущего драйвера, текущую операционную систему, номер устройства;
 - сменить текущий драйвер (кнопка «**Сменить**»), выбрать драйвер УКЗД из списка доступных драйверов;
 - протестировать работоспособность драйвера;
 - получить информацию о количестве открытых сессий шифрования на текущий момент времени, выбрать базовые адреса ввода-вывода, протестировать работоспособность оборудования (кнопка «**Тест**»);
 - выбрать способ запуска драйвера УКЗД (в *Windows NT* с правами администратора);
 - включить/выключить регистрацию в системном журнале (только *Windows NT*).

Программа тестирования функций Crypton API
(*TestAPI.exe*). Основные возможности

С помощью программы тестирования функций возможно:

- оценить возможности платы шифрования «Криптон»;
- протестировать некоторые параметры:
 - скорость шифрования и расшифрования;
 - правильность шифрования в многозадачном режиме;
 - правильность работы функций ***Crypton API***.

Программа тестирования функций Crypton API
(*TestAPI.exe*). Работа с драйвером

*На странице «**Драйвер**» представлена информация:*

- о версии драйвера;
- о производителе драйвера;
- о версии **Crypton API (CryptAPI.dll)**.

Для начала работы необходимо:

- открыть драйвер (кнопка «**Открыть**»);
- выбрать тип драйвера (драйвер оборудования или эмулятор).

При успешном открытии драйвера создается сессия шифрования для доступа к функциям, предоставляемым УКЗД.

Программа тестирования функций Crypton API (*TestAPI.exe*). Работа с драйвером

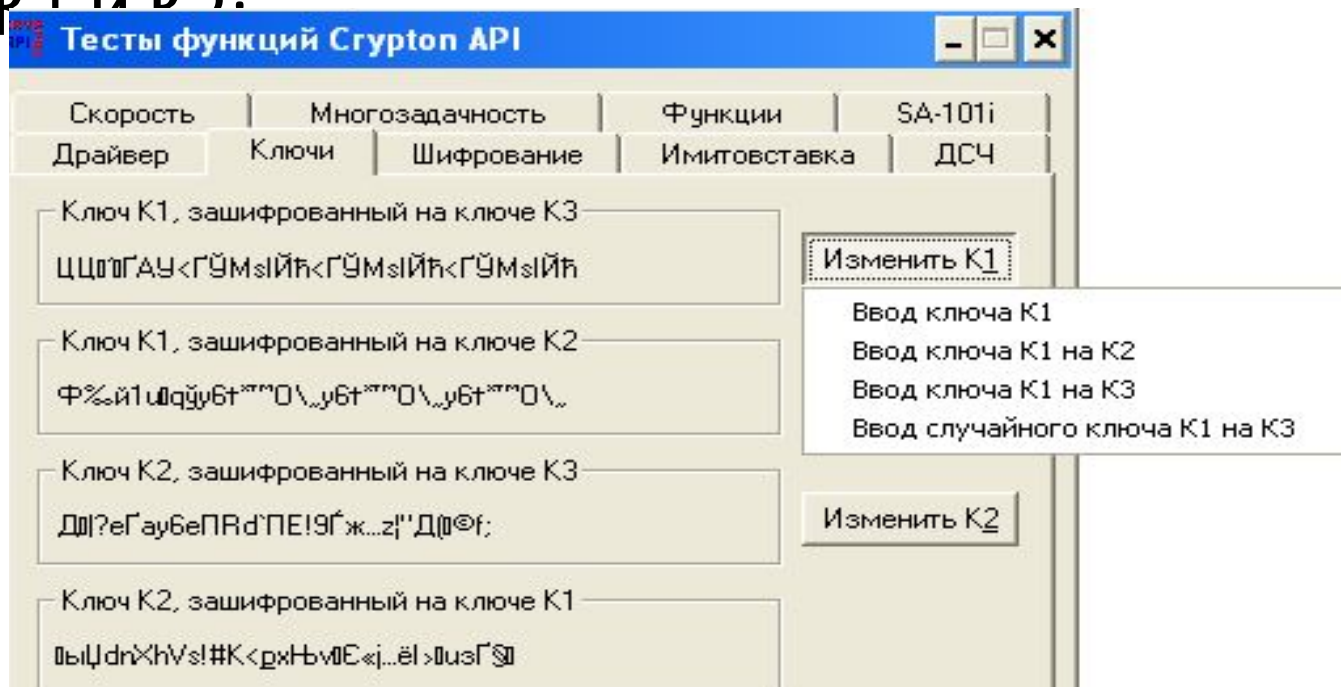
Сессия шифрования имеет:

- собственную виртуальную плату шифрования со своими ключами;
- ***K1*** – файловый ключ;
- ***K2*** - узел замены.

Главный ключ и узел замены являются общими для всех сессий.

Программа тестирования функций Crypton API (*TestAPI.exe*). Страница «Ключи»

- на странице «**Ключи**» представлена информация о шифрованных текущих ключах **K1 и K2**.



Программа тестирования функций Crypton API (*TestAPI.exe*). Страница «Шифрование»

- на странице «**Шифрование**» можно протестировать шифрование и расшифровку на ключе **K1**, введя **синхропосылку** и **любой текст** («Строка для шифрования»), нажав кнопку «**Зашифровать**» («**Расшифровать**») и выбрав **режим шифрования** по **ГОСТ 28147-89** («**Гаммирование**» или «**Гаммирование с восстановлением**»).

Тесты функций Crypton API

Скорость	Многозадачность	Функции	SA-101i
Драйвер	Ключи	Шифрование	Имитовставка
			ДСЧ

Синхропосылка (8 символов):

Строка для шифрования:

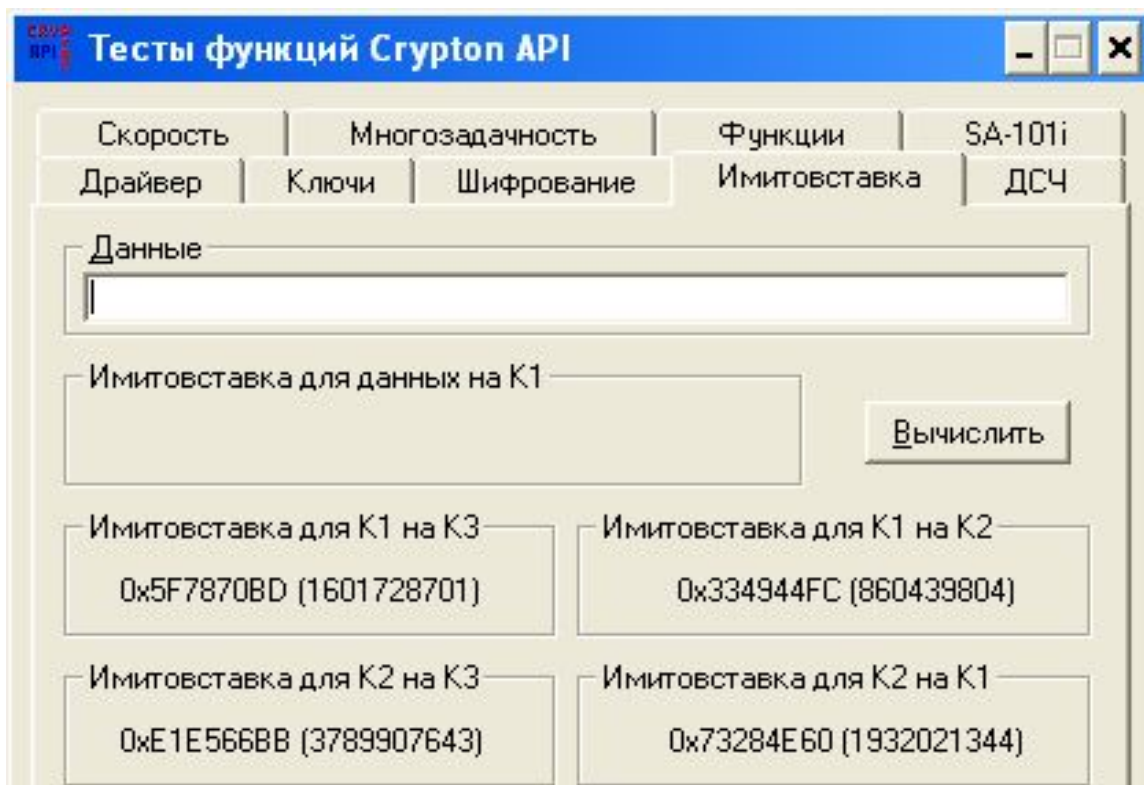
Результат:

Гаммирование на ключе K1
На ключе K1 с восстановлением

Программа тестирования функций Crypton API (*TestAPI.exe*). Страница «Имитовставка»

Страница «**Имитовставка**» позволяет:

- посмотреть имитовставки для ключей;
- вычислить имитовставку для введенных данных (кнопка «**Вычислить**»):



Тесты функций Crypton API

Скорость	Многозадачность	Функции	SA-101i	
Драйвер	Ключи	Шифрование	Имитовставка	ДСЧ

Данные

Имитовставка для данных на K1

Вычислить

Имитовставка для K1 на K3
0x5F7870BD (1601728701)

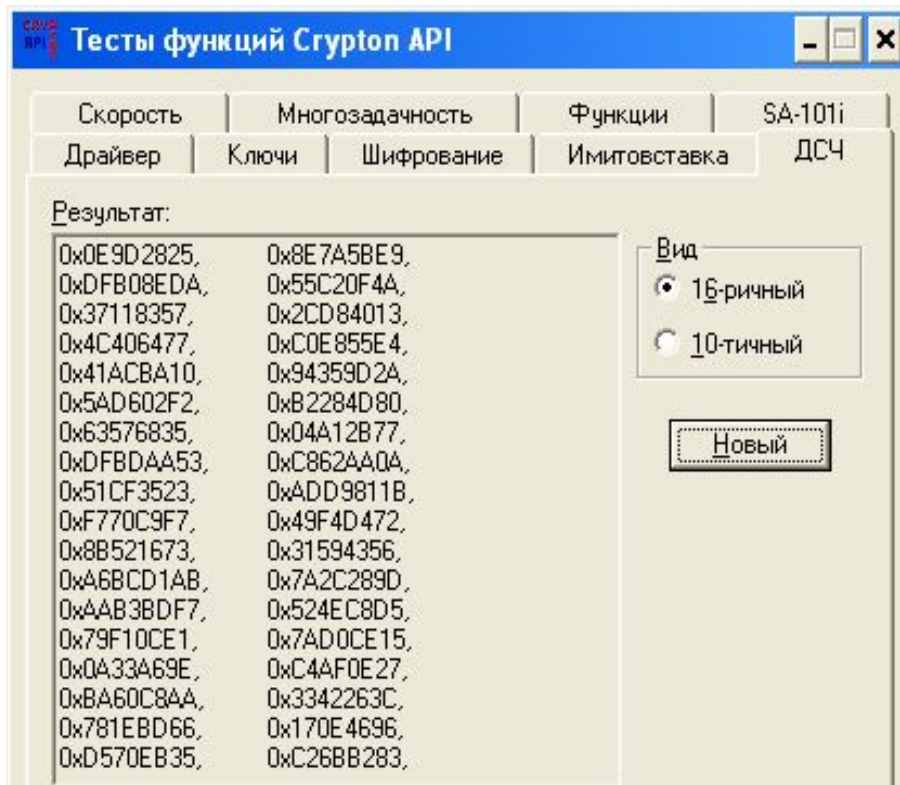
Имитовставка для K1 на K2
0x334944FC (860439804)

Имитовставка для K2 на K3
0xE1E5668B (3789907643)

Имитовставка для K2 на K1
0x73284E60 (1932021344)

Программа тестирования функций Crypton API (*TestAPI.exe*). Страница «ДСЧ»

- страница «**ДСЧ (Датчик случайных чисел)**» позволяет сгенерировать блок случайных чисел;
- по кнопке «**Новый**» в окне «**Результат**» появится последовательность из **беззнаковых 32-битовых случайных чисел**:



Программа тестирования функций Crypton API
(*TestAPI.exe*). Страница «Скорость»

- странице «**Скорость**» позволяет:
определить скорость
шифрования/расшифрования на ключе
K1;
- в поле «**Размер данных**» необходимо
ввести размер данных, при шифровании
(расшифровании) которых будет
измеряться скорость;
- средняя скорость будет отображаться в
окне «**Скорость (Кбайт/сек)**».

Программа тестирования функций Crypton API
(*TestAPI.exe*). Страница «Многозадачность»

- страница «**Многозадачность**» позволяет протестировать работу УКЗД или драйвера-эмулятора в многозадачном режиме;
- при старте теста создаются **15 потоков**, каждый из которых:
 - открывает сессию шифрования;
 - загружает случайный ключ ***K1***;
 - начинает шифровать данные, размер которых указывается в поле «**Размер данных (Кбайт)**»;
- после зашифрования блок данных расшифровывается и расшифрованная информация сверяется с изначальной. **Если данные не совпадают, поток останавливает свою работу и сообщает об ошибке.** Для старта теста необходимо нажать кнопку «Старт» и выбрать режим шифрования.

Программа тестирования функций Crypton API (*TestAPI.exe*). Страница «Функции»

- на странице «**Функции**» можно выборочно протестировать основные функции ***Crypton API***;
- можно задать количество повторов теста каждой функции;
- тест функции завершается успешно, если все повторы были успешными;
- на экран и в файл ***testapi.txt*** будет выведен результат тестирования.

Программа тестирования функций Cryption API
(*TestAPI.exe*). Страница «*SA-101i*»

- страница ***SA-101i*** позволяет просмотреть содержимое памяти смарт-карты;
- для этого необходимо:
 - вставить смарт-карту в устройство ***SA-101i***;
 - указать тип смарт-карты(4-64 кБит или 2-16 кБит);
 - нажать кнопку «***Прочитать***».