ПРИЛОЖЕНИЕ 2 «Инструкция пользователя программного комплекса Visual AES»

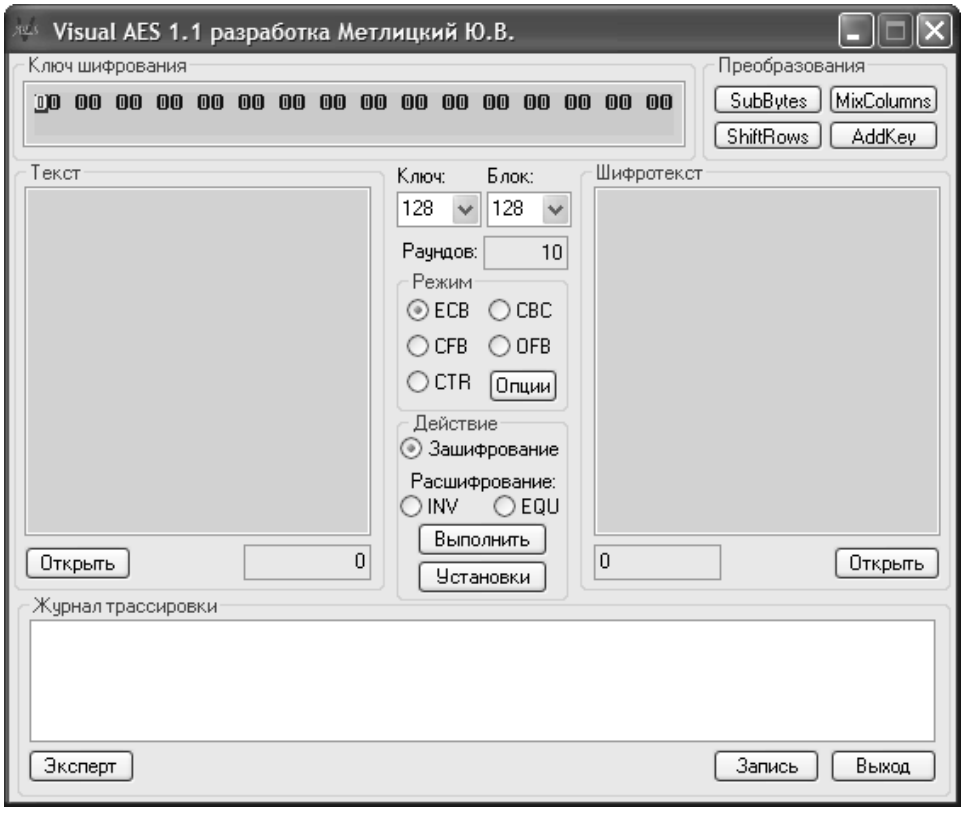
Программный комплекс Visual AES представляет собой многофункциональную систему визуализации, анализа и, собственно, реализации шифрования данных с использованием алгоритма AES. Системные требования – компьютер на базе Intel Pentium и выше, ОС – Windows 95 + IE 4.0 и выше. Основными компонентами системы являются:

- инструментарий шифрования по стандарту AES – реализация зашифрования/расшифрования данных согласно алгоритму AES с поддержкой большинства существующих режимов шифрования с обратной связью (ECB, CBC, CFB, OFB и CTR);
- подсистема визуализации, с помощью соответствующего графического материала, а также специально встроенного инструментария («Журнал» и «Эксперт») раскрывающая суть алгоритма и принципов преобразований реализованных в нем;
- подсистема анализа, включающая в себя средства управления математическим аппаратом преобразований, проводимых в процессе шифрования и визуальная реализация известной атаки «Квадрат» на криптоалгоритм AES.

Начало работы

После запуска программы Visual AES на выполнение на экране ПК отображается главное окно, содержимое которого условно можно разбить на три составляющих:

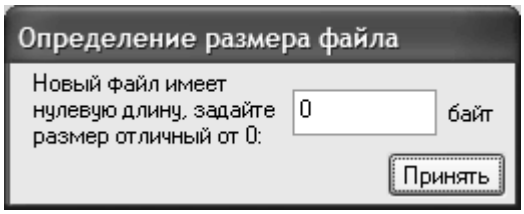
- настройка алгоритма («Ключ шифрования», «Преобразования»);
- настройка режима работы («Ключ», «Блок», «Режим», «Действие»);
- средства трассировки («Журнал трассировки», «Эксперт»);



Поля «Текст» и «Шифротекст», соответственно, предназначены для отображения содержимого открытого и зашифрованного входных файлов (*все исходные данные, параметры и результаты в программе представляются в шестнадцатеричном виде).
Для начала работы необходимо:

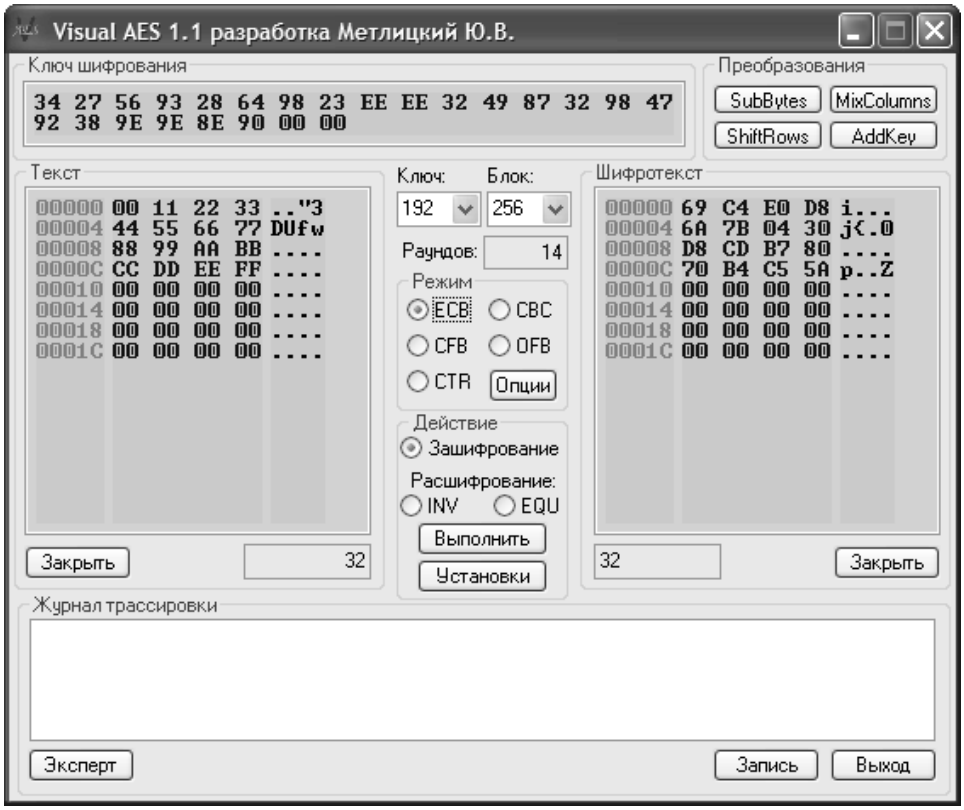
- выбрать в полях «Ключ:» и «Блок:» требующиеся размеры соответственно для ключа и блока;

- по нажатию кнопок «Открыть» выбрать рабочие файлы на одном из носителей представленных на данном ПК (условиями накладываемыми блочным шифром AES их длины будут выровнены между собой на границу размера блока – дополнительным байтам присваивается нулевое значение). В случае необходимости создания нового файла нужно: в поле «Имя файла» ввести имя несуществующего в текущей директории файла и в следующем диалоговом окне задать начальный размер;



- задать значение ключа шифрования в поле «Ключ шифрования»

В результате описанных выше шагов система становится готовой к работе. Далее в зависимости от поставленной задачи выбирается определенный сценарий: шифрование, обучение, исследование, анализ.

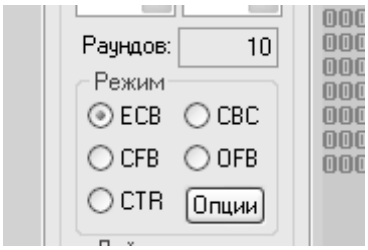


Шифрование с помощью Visual AES.

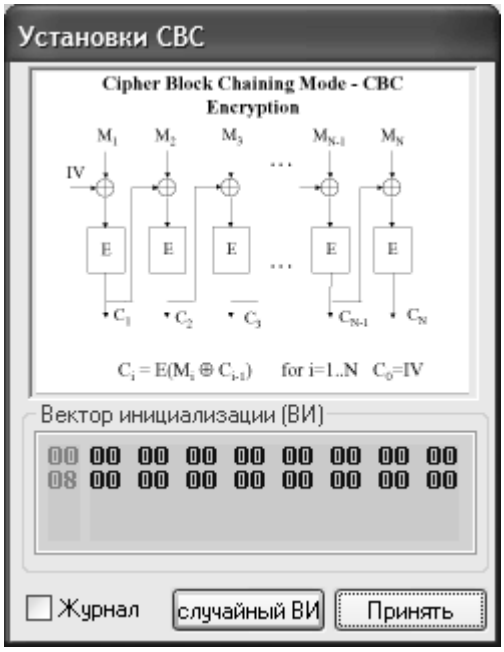
Зашифрование или расшифрование выполняются над выбранными исходными файлами: если выполняется операция зашифрования, то содержимое окна «Текст» (файла предназначенного для зашифрования) преобразуется согласно алгоритму AES и помещается в окно «Шифротекст», а соответственно в файл шифротекста. В случае операции расшифрования выполняется обратное действие: файл из окна «Шифротекст» подвергается операции расшифрования, а результат передается в окно «Текст» (файл открытого текста).

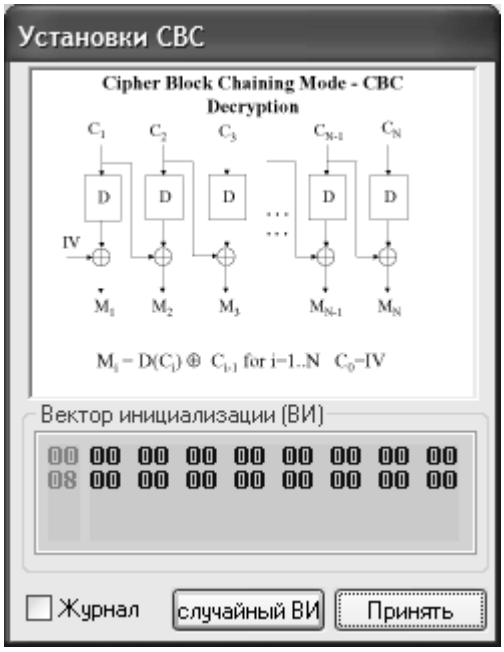
Для выполнения описанных выше операций необходимо при условии уже определенных ключа, его размера и размера блока выполнить следующие операции:

1. Выбрать необходимый режим из предлагаемого перечня режимов шифрования с обратной связью в группе «Режим» (ECB, CBC, CFB, OFB и CTR),



при переключении на одну из радиокнопок, кнопка «Опции» автоматически перестраивается на управление установками именно того режима, который активизируется радиокнопкой. По нажатию на кнопку «Опции» выводится одно из окон установок соответствующее выбранному режиму.

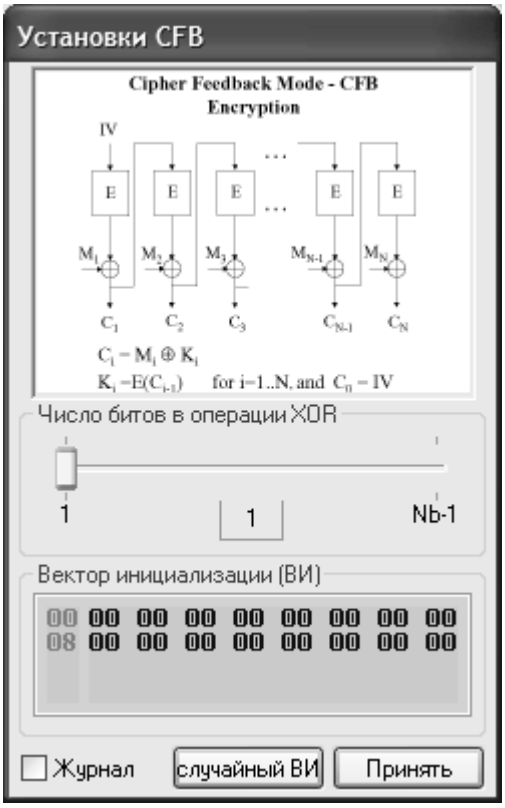


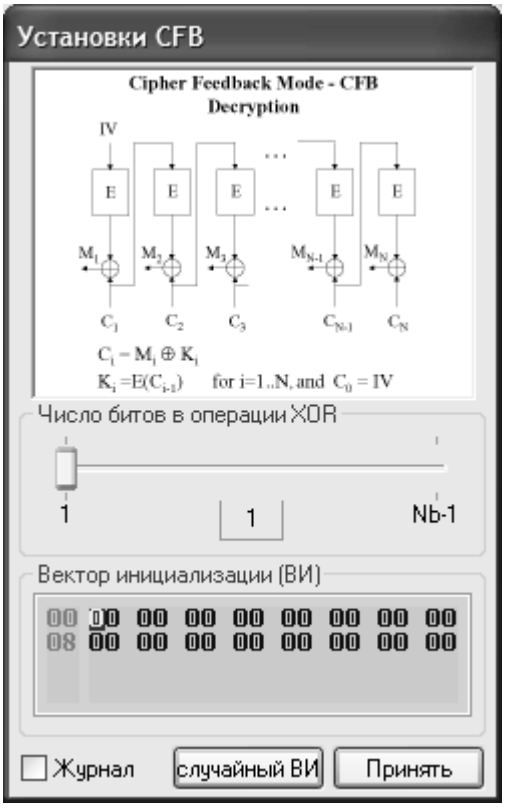


В режиме сцепления блоков шифротекста перед шифрованием над открытым текстом и предыдущим блоком шифротекста выполняется операция XOR. При шифровании в режиме CBC одинаковые блоки открытого текста превращаются в различающиеся друг от друга блоки шифртекста только в случае различия каких-либо предшествующих блоков.

Поле «Вектор инициализации» представляет блок случайных данных инициализирующих процедуру сцепления блоков начальным значением. Кнопка «случайный ВИ» позволяет присвоить ему результат вызова генератора псевдослучайной последовательности

Опция «Журнал» позволяет в журнал трассировки (см. ниже) помещать соответствующие сообщения режима (номер блока, значения каждого входного и выходного блоков).





В отличие от остальных в режиме CFB можно шифровать единицы данных размером не превышающие размер блока. Один из вариантов - шифрование по одному байту (8-битовый CFB), с помощью 1 -битового CFB можно шифровать данные побитово, но полное шифрование блочным шифром единственного бита требует много ресурсов.

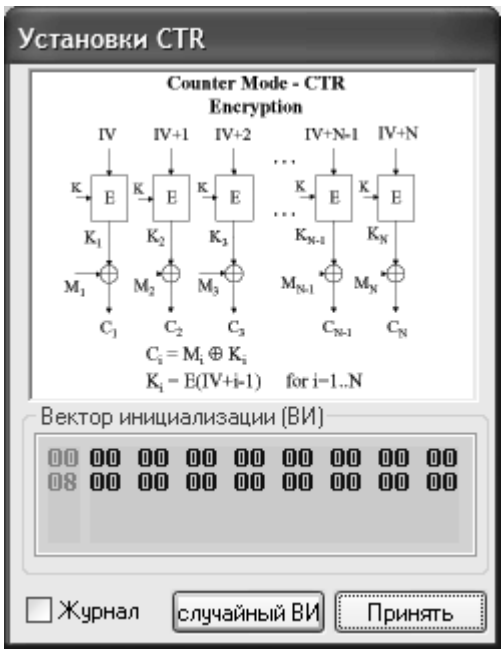
Поле «Число битов в операции XOR» задает размер шифруемой битовой последовательности.

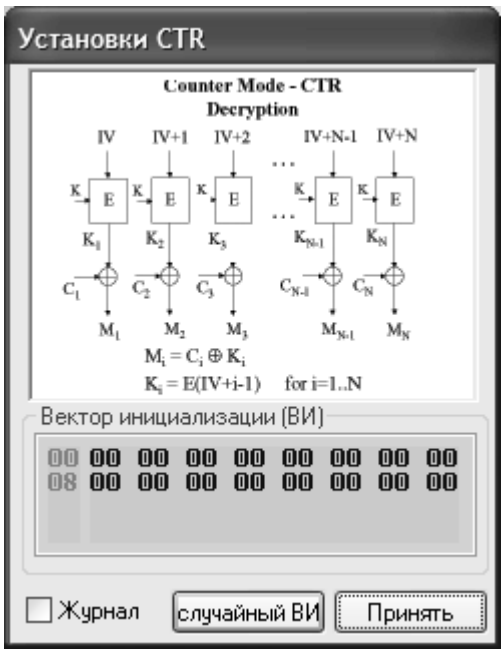
Поле «Вектор инициализации» представляет блок случайных данных инициализирующих процедуру сцепления блоков начальным значением. Кнопка «случайный ВИ» позволяет присвоить ему результат вызова генератора псевдослучайной последовательности.

Опция «Журнал» позволяет в журнал трассировки (см. ниже) помещать соответствующие сообщения режима (номер блока, значения каждого входного и выходного блоков).

Режим ECB - простейший режим шифрования. Все блоки открытого текста шифруются независимо друг от друга.

Опция «Журнал» позволяет в журнал трассировки (см. ниже) помещать соответствующие сообщения режима (номер блока, значения каждого входного и выходного блоков).

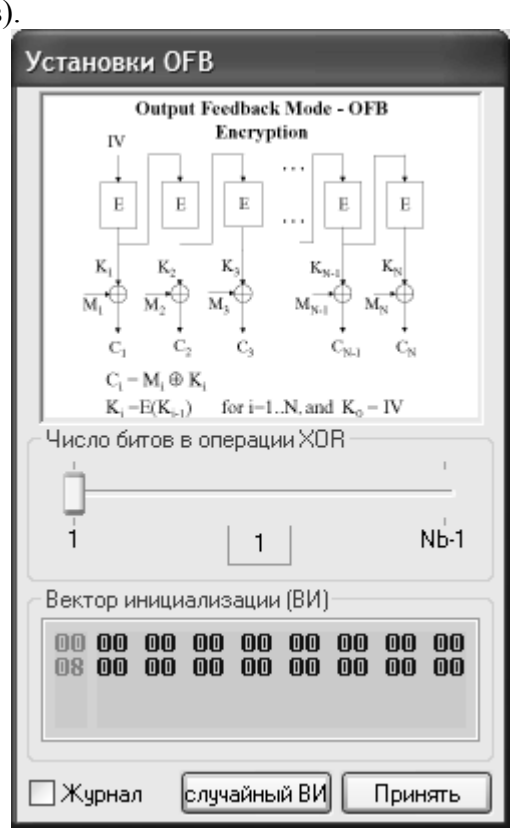


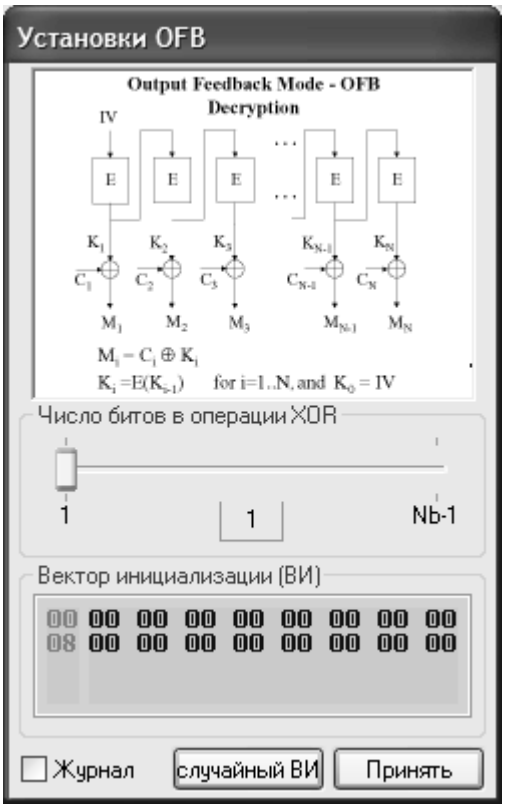


Блочные шифры в режиме счетчика используют последовательность чисел в качестве входов алгоритма. Для заполнения регистра используется счетчик, а не вывод алгоритма шифрования. После шифрования каждого блока значение счетчика возрастают на определенную константу, обычно на единицу.

Поле «Вектор инициализации» представляет блок случайных данных инициализирующих процедуру сцепления блоков начальным значением. Кнопка «случайный ВИ» позволяет присвоить ему результат вызова генератора псевдослучайной последовательности.

Опция «Журнал» позволяет в журнал трассировки (см. ниже) помещать соответствующие сообщения режима (номер блока, значения каждого входного и выходного блоков).





Режим OFB представляет собой метод использования блочного шифра в качестве синхронного потокового шифра. Этот режим подобен режиму CFB, за исключением того, что n битов предыдущего выходного блока сдвигаются в крайние правые позиции очере-

ди.

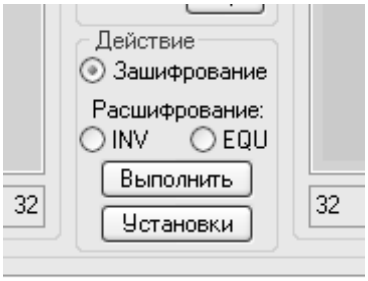
Поле «Число битов в операции XOR» задает размер шифруемой битовой последовательности.

Поле «Вектор инициализации» представляет блок случайных данных инициализирующих процедуру сцепления блоков начальным значением. Кнопка «случайный ВИ» позволяет присвоить ему результат вызова генератора псевдослучайной последовательности

Опция «Журнал» позволяет в журнал трассировки (см. ниже) помещать соответствующие сообщения режима (номер блока, значения каждого входного и выходного блоков).

В каждом окне установок режима представлена графическая диаграмма его работы в зависимости от направления шифрования (зашифрование или расшифрование), а так же соответствующие изменяемые параметры.

2. Задать выбором одной из радиокнопок в группе «Действие» вид выполняемой операции «Зашифрование» или «Расшифрование». В Visual AES реализованы 2 режима расшифрования - инверсный («INV») и эквивалентный («EQU») подробности см. «AES Proposal: Rijndael» Joan Daemen, Vincent Rijmen.

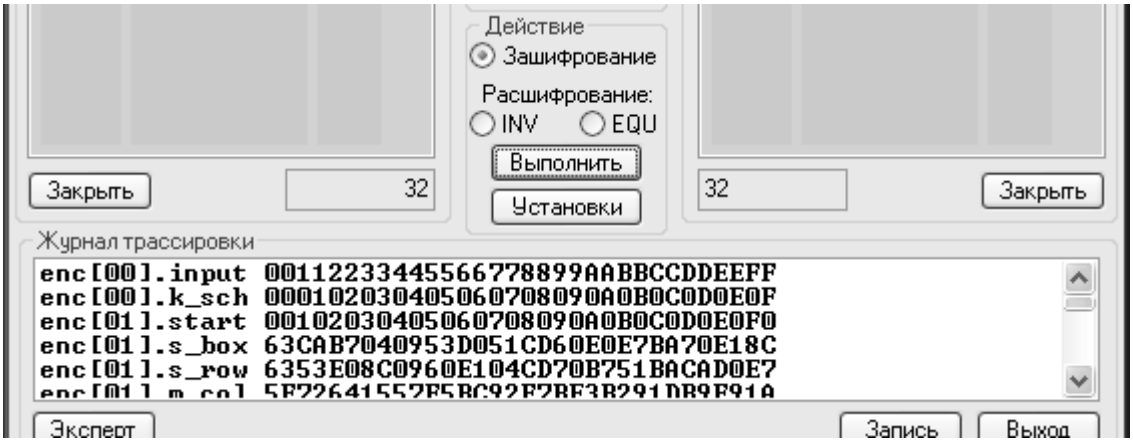


3. После нажатия кнопки «Выполнить» операция шифрования будет выполнена, ее результат будет отображен в окне назначения и записан в соответствующий файл.

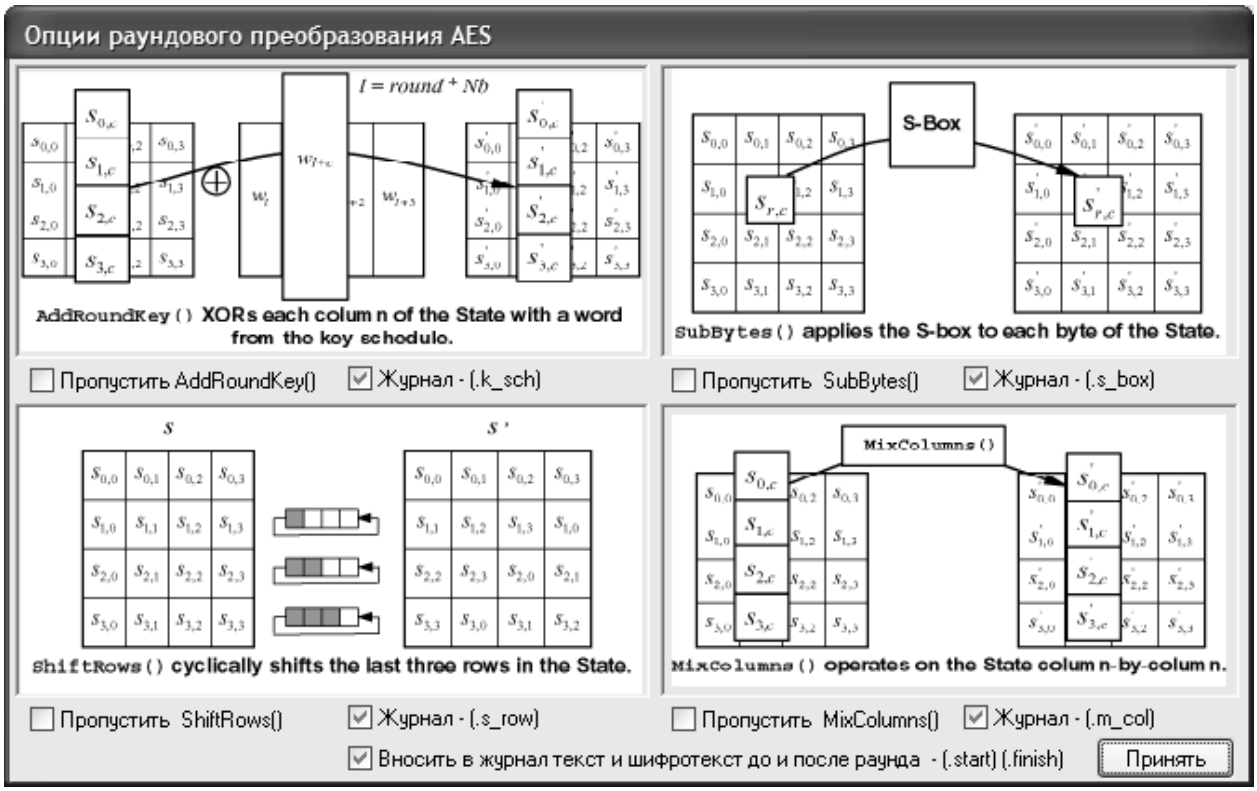
Обучение с помощью Visual AES.

В процессе выполнения операций шифрования с целью изучения структуры алгоритма система Visual AES позволяет вести подробный журнал раундовых трансформаций, в котором по выбору пользователя возможно фиксирование всех состояний, которые проходит блок данных при зашифровании или расшифрованиии.

«Журнал трассировки» расположен в нижней части основного окна программы, с помощью полосы прокрутки возможно перемещение по его записям вверх и вниз. В случае выбора некоторых установок, определяющих содержимое журнала, по нажатию кнопки «Выполнить» группы «Действие», журнал очищается и вновь последовательно заполняется результатами производимой операции (зашифрование/расшифрование). Кнопка «Запись» позволяет сохранить его содержимое на внешний носитель для дальнейшего исследования.



Обсудим все возможные установки журнала. Они доступны по нажатию кнопки «Установки» группы «Действие».



Кнопка «Принять» завершает работы с данным окном.

Согласно официальной документации на стандарт AES, в окне «Опции раундового преобразования AES» перечислены последовательно исполняемые раундовые операции и изображены их диаграммы. Под каждой из них размещены по паре элементов выбора позволяющих соответственно включить или исключить из раундового преобразования данную операцию вообще или включить или исключить помещение в журнал трассировки промежуточных результатов последней.

Возможность включения или исключения самой раундовой операции из алгоритма будет обсуждаться ниже в разделе «Исследование с помощью Visual AES».

Строка журнала

```
enc[04].start FA636A2825B339C940668A3157244D17
```

обозначает, что в операции зашифрования («`enc`», возможны «`inv`» и «`equ`») на старте («`.start`») раунда номер `4` содержимое блока шифруемых данных выглядело следующим образом: `FA636A2825B339C940668A3157244D17`.

Ниже приводится полный перечень обозначений всех возможных элементов журнала:

`.input`[xxx] – данные перед операцией шифрования;
`.start`[xxx] – блок на начало раунда;
`.k_sch`[xxx] – значение раундового ключа;
`.k_add`[xxx] – блок после добавления раундового ключа;
`.s_box`[xxx] – блок после операций (Inv)SubBytes;
`.s_row`[xxx] – блок после операций (Inv)ShiftRows;
`.m_col`[xxx] – блок после операций (Inv)MixColumns;
`.final`[xxx] – результат шифрования.

Исследование с помощью Visual AES.

Для исследование математического аппарата алгоритма AES в системе Visual AES предусмотрен инструмент «Преобразования», основная задача которого – предоставить пользователю возможность управления параметрами преобразования байтов данных шифруемых блоков.

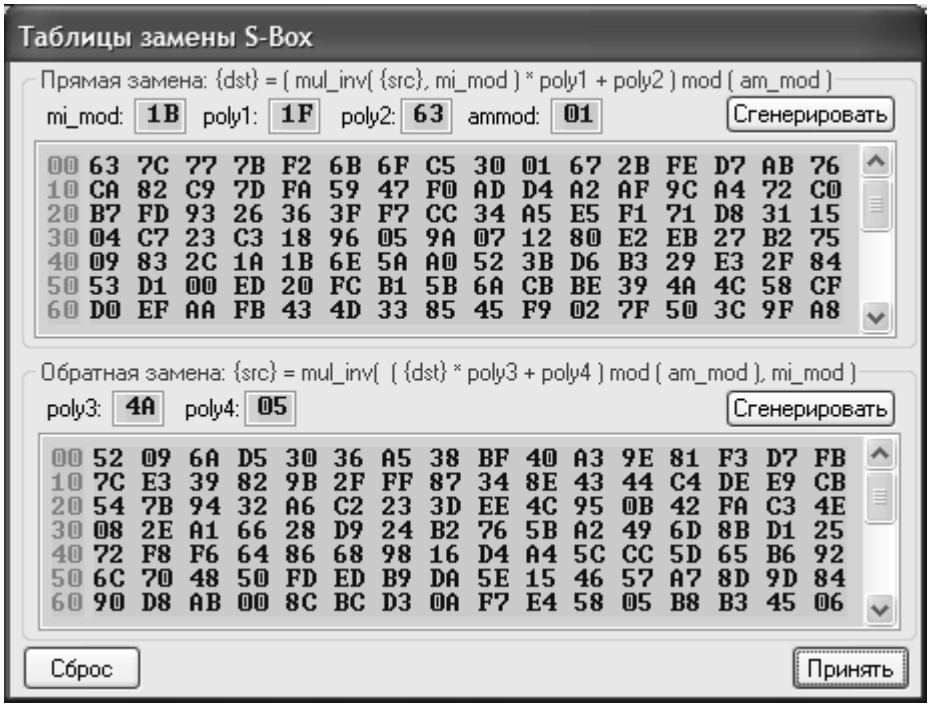
Согласно приводимой документации на стандарт шифрования AES, каждое раундовое преобразование выполняет над блоком данных определенные операции схематически представленные на диаграммах окна «Опции раундового преобразования AES» (за более детальной информацией обращайтесь «AES Proposal: Rijndael» Joan Daemen, Vincent Rijmen).

Преобразование SubBytes (кнопка «SubBytes» группы «Преобразования»)*:*

В рамках данного преобразования на каждом раунде все байты блока данных подвергаются замене: при зашифровании - согласно таблицы «прямой замены», при расшифровании - согласно таблицы «обратной замены». Элементы обеих таблиц имеют математическую зависимость с заменяемыми байтами изображенную в окне «Таблицы замены S-Box» в виде формул.

Параметрами этой зависимости можно управлять. После придания им новых значений необходимо нажать на кнопку «Сгенерировать» и программа создаст новую таблицу замен (прямой или обратной).

Для возврата в состояние, определяемое стандартом AES требуется нажатие кнопки «Сброс».



Кнопка «Принять» завершает работы с данным окном.

Условные обозначения:

{dst} – результат прямого преобразования S-Box байта {src};

{src} – результат обратного преобразования S-Box байта {dst};

mi_mod – модуль, по которому вычисляется мультипликативная инверсия в поле $GF(2^8)$;

poly1 – произвольный многочлен в поле $GF(2^8)$, участвующий в операции умножения;

poly2 – произвольный многочлен в поле $GF(2^8)$, участвующий в операции сложения;

am_mod – модуль, по которому вычисляется значения преобразования замены байт (affine map) в поле $GF(2^8)$;

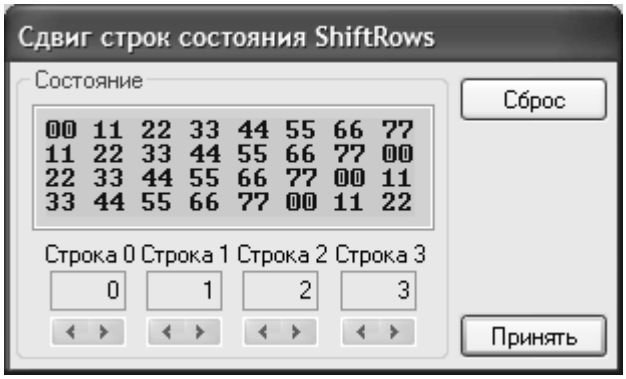
mul_inv() – операция нахождения мультипликативной инверсии в поле $GF(2^8)$;

poly3 – произвольный многочлен в поле $GF(2^8)$, участвующий в операции умножения обращающий операцию прямой замены;

poly4 – произвольный многочлен в поле $GF(2^8)$, участвующий в операции сложения обращающий операцию прямой замены.

Преобразование ShiftRows (кнопка «ShiftRows» группы «Преобразования»):

Следующим по порядку преобразованием в раунде является сдвиг строк блока на определенное число позиций – влево при зашифровании и вправо при расшифровании (по стандарту это 0, 1, 2, 3 позиций по порядку следования строк сверху вниз, восстановление исходных значений по нажатию кнопки «Сброс»). С помощью стрелок возможна перестройка данных смещений в окне «Сдвиг строк состояния ShiftRows» для операции зашифрования. Для операции расшифрования Visual AES выбирает противоположные значения заданным.

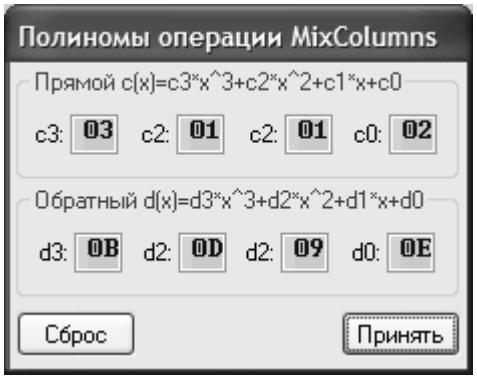


Кнопка «Принять» завершает работы с данным окном.

Преобразование MixColumns (кнопка «MixColumns» группы «Преобразования»)*:*

Операция MixColumns выполняет умножение каждого столбца в поле $GF(2^{32})$ на многочлены представленные в окне «Полиномы операции MixColumns» по подулю am_mod (см. выше). Побайтовое их представление для прямого $c(x)$ и обратного $d(x)$ можно модифицировать для получения новых вариантов алгоритма.

Кнопка «Сброс» возвращает значения определенные в стандарте шифрования AES.



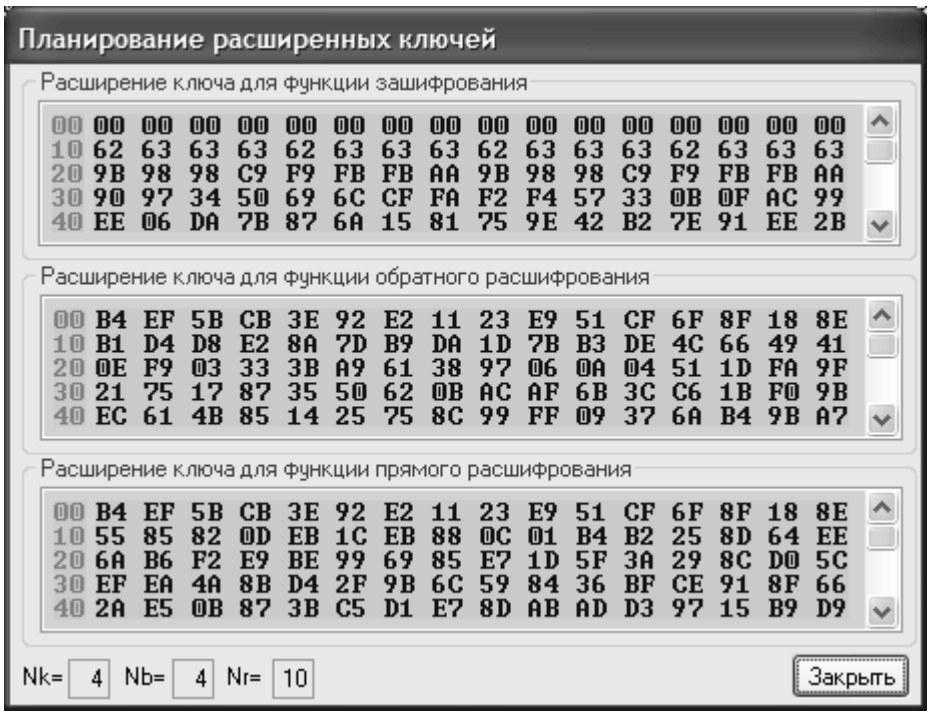
Кнопка «Принять» завершает работы с данным окном.

Преобразование AddRoundKey (кнопка «AddRoundKey» группы «Преобразования»)*:*

Операция добавления раундового ключа требует предварительной генерации «графика» раудовых ключей по заданному ключу с привлечением специального алгоритма планирования. В окне «Планирование расширенных ключей» в зависимости от выбранных размеров блока и ключа в основном окне программы отображаются «Расширение ключа для функции зашифрования», «Расширение ключа для функции обратного расшиф-

рования» и «Расширение ключа для функции прямого расшифрования» - значения всех раундовых ключей для каждой из операций.

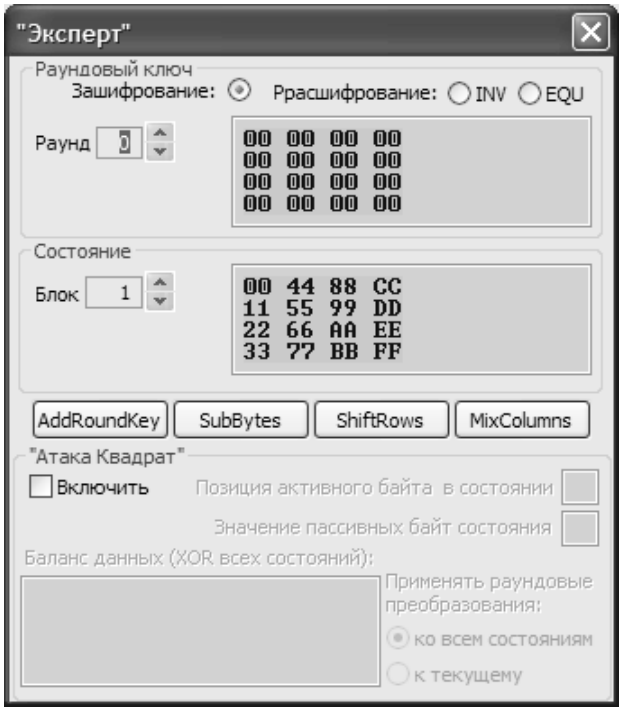
В нижней части окна также выводится характеристики выбранного алгоритма, а именно: Nk – размер ключа в 32-битных словах, Nb – размер блока в 32-битных словах и Nк – число раундов шифрования.



Кнопка «Закрыть» завершает работы с данным окном.

Анализ с помощью Visual AES.

Инструментарий «Эксперт», доступный из основного окна программы Visual AES предназначен для детального анализа данных – результатов раундовых преобразований шифра AES. В нем реализовано 2 режима работы: пошаговая трассировка раундовых трансформаций (основной режим) и атака «Квадрат» (активизирующийся выбором кнопки «Включить» группы «Атака Квадрат»).



В режиме трассировки последовательность работы следующая:

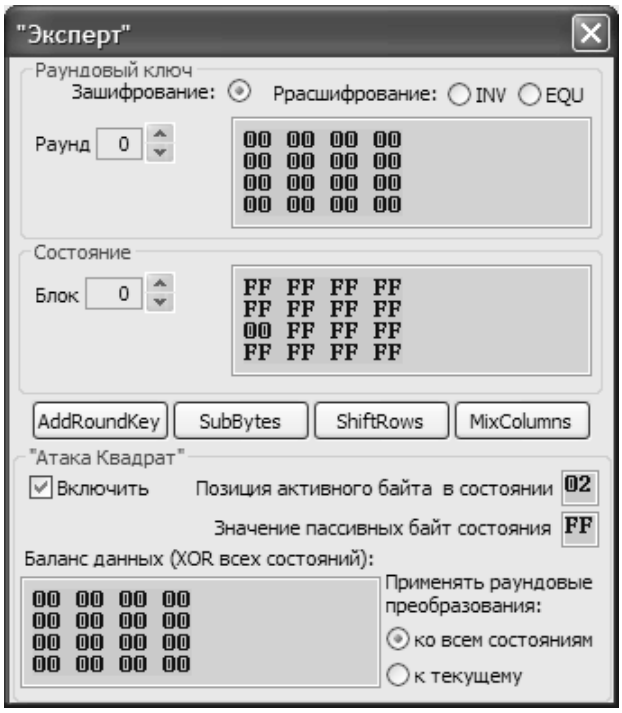
При переходе в режим «Эксперт» происходит копирование первого блока данных из одного из исходных файлов (в зависимости от выбора операции в группе «Действие» основного окна программы), а при его отсутствии создается временный блок с нулевым заполнением.

С помощью прокрутки «Блок» группы «Состояние» возможно переключение между смежными блоками данных исходных файлов. Прокрутка «Раунд» осуществляет выбор раундового ключа согласно его порядкового номера. Радио кнопки «Зашифрование» и «Расшифрование» определяют применяемые раудовых операций.

По нажатию на одну из кнопок «AddRoundKey», «SubBytes», «ShiftRows» и «MixColumns» к текущему блоку данных (состоянию) применяется соответствующая трансформация и на экран выводится ее результат.

В режиме атаки «Квадрат» последовательность работы следующая:

Правила управления результатами раундовых трансформаций такие же, как и в предыдущем режиме. Отличие состоит во входных данных (состояниях), атака квадрат подробно описывается в «AES Proposal: Rijndael» Joan Daemen, Vincent Rijmen.



Для проведения атаки «Квадрат» создается набор из 256 блоков (состояний) заполняющихся значениями «Пассивных байт», а в позиции «Активного байта» каждого состояния размещается его (состояния) порядковый номер (0-255).

Поле «Баланс данных» отображает результат сложения по модулю 2 всех состояний после каждой «кнопочной» раундовой трансформации (в атаке эта возможность требуется для контроля изменений в состояниях).

Применение любой раундовой операции можно ограничить либо текущим отображаемым в окне блоком, либо одновременным ее применением ко всем элементам набора (радиокнопки «Применять раундовые преобразования» группы «Атака Квадрат»).

Завершение работы Visual AES.

Для завершения работы с системой Visual AES необходимо в основном окне программы нажать на кнопку «Выход» и подтвердить свое решение утвердительным ответом в окне «Выход».