ды злоумышленника также важно, как и пытаться им противостоять. Информационно-аналитический анализ – только один из способов, который позволяет противодействовать манипуляциям сознанием, однако знание и применение его необходимо для нашей же безопасности.

Литература

1. А.И. Доронин Бизнес разведка, 5-е издание: Ось 89; Москва; 2009
2. Семёнова А.В., Корсунская М.В. Контент-анализ СМИ: проблемы и опыт применения / Под ред. В.А. Мансурова. – М.: Институт социологии РАН, 2010. – 324 с.
3. Контент-анализ публикаций СМИ [Электронный источник]. - https://studopedia.ru/14_88868_kontent-analiz-publikatsiy-smi.html.
4. Информационное воздействие: виды, средства, объекты [Электронный источник]. - https://studfiles.net/preview/1113130/page:2/.

О.Ш. Узаков

ОЦЕНКА СЛОЖНОСТИ АЛГОРИТМА ШИФРОВАНИЯ ДАННЫХ ГОСУДАРСТВЕННОГО СТАНДАРТА УЗБЕКИСТАНА DST2005

(Каршинский филиал Ташкентского университета
информационных технологий имени Мухаммада аль-Хоразмий)

Настоящий стандарт «Алгоритм шифрования данных» (АШД) DSt2005 представляет собой криптографический алгоритм, предназначенный для защиты электронных данных. АШД DSt2005 - симметричный блочный шифр, который используется для зашифрования и расшифрования информации. АШД DSt2005 может использовать криптографические ключи длиной 128, 256, 512 бит для зашифрования и расшифрования блоков данных длиной 128 или 256 бит.

Стандарт устанавливает единый алгоритм шифрования информации для систем обработки информации в сетях электронных вычислительных машин (ЭВМ), телекоммуникаций, отдельных вычислительных комплексах и ЭВМ и определяет правила шифрования данных.

Стандарт может быть использован для криптографической защиты данных, хранимых и передаваемых в сетях ЭВМ, телекоммуникаций, в отдельных вычислительных комплексах или в ЭВМ коммерческих организаций и предприятий для шифрования данных не являющихся под грифом (ДСП, секретно, сов. секретно, особой важности).

Ниже приведем оценку сложности АШД DSt2005, схема алгоритма шифрования данных приведена на рис. 1. для случая 128-битного блока данных.

Вначале мы имеем значение выхода из массива *Holat* выходных блоков *chiqish* по 32 бита. Восстановление входных значений массива *Holat* блоков

chiqish по 32 бита никакой сложности не составляет преобразование однозначно обратимое.

Далее нам необходимо найти входное значение преобразования *AralashUstun(Holat,* k_s*)* – перемешивание строк, сводится к выполнению следующих действий:

1) вычислить $K_{sch} \otimes H_{ch}[4,4](\mathrm{mod}\, p)$ – умножение матриц по модулю *p* и результат присвоить в массив H_{ch}.

2) вычислить $K_{so} \otimes H_o[4,4](\mathrm{mod}\, p)$ и результат присвоить в массив H_o.

Где $H_{ch}[4,4]$ – левая половина и $H_o[4,4]$ – правая половина массива *Holat,* K_{sch} – левая половина (часть) и K_{so} – правая половина (часть) массива сеансового ключа шифрования. Данное преобразование является обратимым, и сложность его восстановления связана с нахождением K_{sch} и K_{so} частей сеансового ключа шифрования экспоненциальная сложность нахождения, которых составляет 2^{80}. Поскольку для формирования K_{sch} и K_{so} изначально из k_{se} – сеансового ключа шифрования берется 80-битовая часть справа, из которых формируется линейный массив k_{ss} = *[0,1,2,3,…19]* с элементами на полу байтовом уровне, из которого и формируется двумерный массив $k_s[4, 8]$ с элементами в один полубайт.

Таким образом, мы нашли выходное значение преобразования *Qo'shBosqichKalit(Holat,*k_{e1}*)* – побитовое сложение по модулю 2 (операция XOR) массивов *Holat* и первого массива этапных ключей k_{e1}. Сложность нахождения входного значения данного преобразования составляет нахождение первого массива этапных ключей k_{e1} – экспоненциальная сложность нахождения которого составляет 2^{128}операций полного перебора.

Далее нам необходимо восстановить значение восьми раундов шифрования.

Для нахождения входного значения преобразование *BaytAlmash(Holat,* k_{e1} , k_{e2}*)* – перемешивание байтов массива *Holat* и массивов этапных ключей k_{e1} , k_{e2} необходимо найти значение второго массива этапных ключей k_{e2}.

Преобразование заключается в следующем для каждой из ячеек *i* = {0,1,2,3}, *j* = {0,1,2,3,4,5,6,7} вычислить:

$$h[i, j] \;\circledR\; k_{e2}[i, j](\mathrm{mod}\, p) \equiv k_{e2}[i, j] + h[i, j] \times (1 + k_{e1}[i, j] \times k_{e2}[i, j])(\mathrm{mod}\, p).$$

где ® – операция умножения массивов с коэффициентом *R* по модулю *p*;

Как видно данное преобразование является обратимым и никакой сложности не дает. Экспоненциальная сложность нахождения второго массива этапных ключей k_{e2} – составляет 2^{128}операций полного перебора.

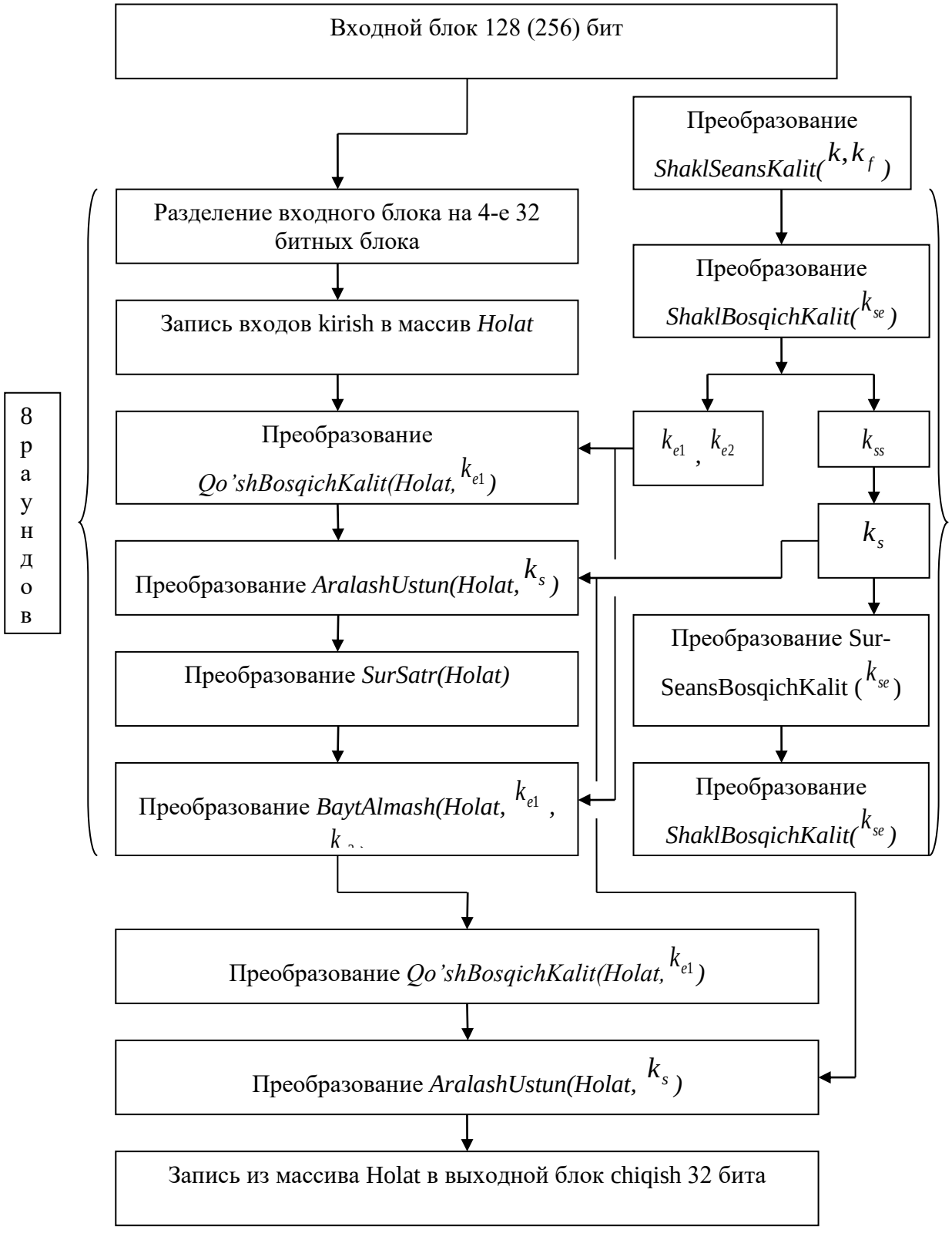

Рисунок 1. Схема алгоритма шифрования данных DSt2005.

Далее нам необходимо найти входное значение преобразования *Sur-Satr(Holat)* – сдвиг строк, первую строку массива *Holat* циклически сдвинуть вправо на 1 полубайт, вторую строку на 2 полубайта, третью строку на 3 полубайта. Данное преобразование никакой сложности не дает и является однозначно обратимым.

Затем нам необходимо найти входное значение преобразования *AralashUstun(Holat,* k_s*)* в данном случае для нас это преобразование никакой сложности не дает, поскольку, найдя значение двумерного массива k_s[4, 8] конечного преобразования можно восстановить предыдущего значения сеансового ключа k_{se} преобразования *ShaklBosqichKalit(*k_{se}*)* – формирование сеансового ключа. Осуществив обратный сдвиг k_{se} на 41 бита влево преобразования Sur-SeansBosqichKalit (k_{se}) – циклический сдвиг сеансового ключа на 41 бита вправо.

Далее нам необходимо найти входное значение преобразования *Qo'shBosqichKalit(Holat,* k_{e1}*)*, которое никакой сложности уже не представляет при известном значении первого массива этапных ключей k_{e1}. Таким образом, мы получим выходное значение массива *Holat*. Затем мы восстановим значение 4-х 32-х битных блока, которые является выходными значениями с седьмого раунда шифрования.

Далее еще семь раз проводятся аналогичные восстановления данных, до нахождения входных значений 4-х 32-х битных блока первого раунда шифрования. Последние и являются исходным значением блока открытого текста (128 бит).

Подводя итог, мы получаем, что в АШД DSt2005 отсутствуют криптографические преобразования сложность, которых имеет экспоненциальную зависимость 2^n. Сложность АШД DSt2005 выражается экспоненциальной сложность нахождения K_{sch} и K_{so} частей сеансового ключа, равной 2^{80}, а также экспоненциальной сложность нахождения k_{e1}, равной 2^{128} и k_{e2}, равной 2^{128}. Таким образом, для случая входного блока данных– 256 бит, соответственно ключа шифрования 256 бит экспоненциальной сложность нахождения K_{sch} и K_{so} частей сеансового ключа, равной 2^{160}, а также экспоненциальной сложность нахождения k_{e1}, равной 2^{256} и k_{e2}, равной 2^{256}. Ниже в таблице 1. приведем значения степени экспоненциальной сложности ключевой системы АШД DSt2005.

Таблица 1 Степень экспоненциальной сложности ключевой системы АШД DSt2005.

Тип ключа шифрования	Степень экспоненциальной сложности
АШД DSt2005 – 128	
K_{sch} и K_{so} массива сеансового ключа шифрования	2^{80}
Первый массив этапных ключей k_{e1}	2^{128}
Второй массив этапных ключей k_{e2}	2^{128}
Ключевая система в целом k_{se}	2^{336}
АШД DSt2005 – 256	
K_{sch} и K_{so} массива сеансового ключа шифрования	2^{160}
Первый массив этапных ключей k_{e1}	2^{256}
Второй массив этапных ключей k_{e2}	2^{256}
Ключевая система в целом k_{se}	2^{672}

Литература

1. Столлингс В. Криптография и защита сетей: принципы и практика. – М. , Изд. дом «Вильямс», 2001. – 672 стр.

2. Венбо Мао. Современная криптография. Теория и практика. – Москва–Санкт-Петербург–Киев: Лори Вильямс, 2005. –768 стр.

3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие, 1-2-е изд. –М.: Гелиос АРВ, 2002.-480 с

О.Ш. Узаков

ОЦЕНКА ЭКСПОНЕНЦИАЛЬНОЙ СЛОЖНОСТИ СТАНДАРТА АЛГОРИТМА ШИФРОВАНИЯ ГОСТ 28147-89

(Каршинский филиал Ташкентского университета информационных технологий имени Мухаммада аль-Хоразмий)

Оценка экспоненциальной сложности дешифрования шифр текстов позволит дать ответ на вопрос, “каким должен быть крипто стойкий алгоритм шифрования”, чтобы дешифрование шифр текста не было практически возможным без исходного ключа шифрования. С развитием сетевых технологий и с ростом объемов передачи данных по сетям телекоммуникациям возникает проблема защиты информации, где активным способом защиты выступает применение криптографических методов, т.е. фактически возникает проблема создания современного стойкого алгоритма шифрования. Для этого необходимо знать степень полиномиальной сложности шифрования и экспоненциальной сложности дешифрования алгоритма шифрования.