Компания «Актив»

О практическом применении White Box криптографии

Щелкунов Д.А.

1 White Box криптография

- Открытый ключ – White Box реализация блочного шифра (шифрование), закрытый ключ – White Box реализация блочного шифра (расшифрование).

- Основное достоинство – высокая скорость работы.

- Вопрос о возможности создания такого рода схем остается открытым.

2 White Box криптография

Попытки создать ассиметричные схемы на базе блочных шифров:

1. S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot, A White-Box DES Implementation for DRM Applications, 2002.

2. S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot, White Box Cryptography and an AES Implementation, 2002.

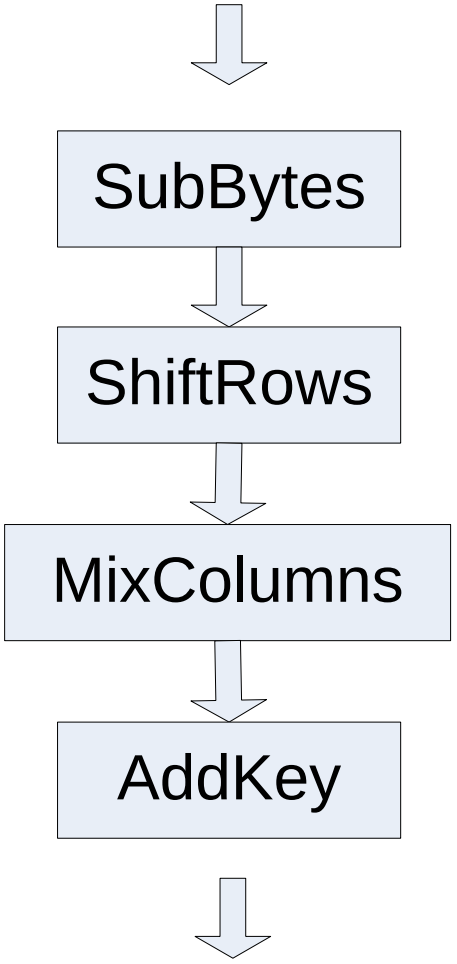
3. Julien Bringer, Herve Chabanne, Emmanuelle Dottax, White Box Cryptography: Another Attempt, 2006.

4. Hamilton E. Link, William D. Neumann, Clarifying Obfuscation: Improving the Security of White-Box Encoding.

5. www.softwaresecurity.org - Ivan V. Petrov, Seculab JSC.

3 White Box AES-128

Раунд AES-128



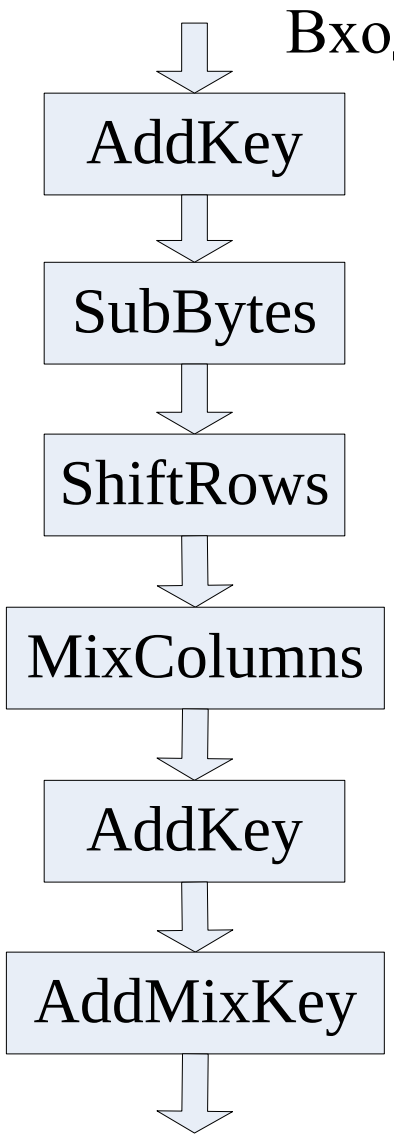
$$\begin{bmatrix} e_{0j} \\ e_{1j} \\ e_{2j} \\ e_{3j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \bullet \begin{bmatrix} S[a_{0j}] \\ S[a_{1j-1}] \\ S[a_{2j-2}] \\ S[a_{3j-3}] \end{bmatrix} \oplus \begin{bmatrix} k_{0j} \\ k_{1j} \\ k_{2j} \\ k_{3j} \end{bmatrix} \quad (1)$$

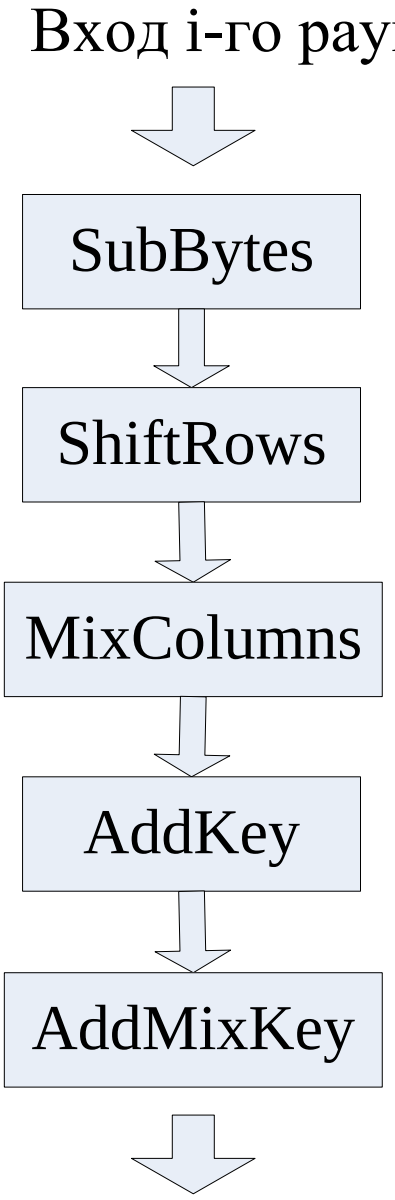
$$T_0[a] = \begin{bmatrix} S[a] \bullet 02 \\ S[a] \\ S[a] \\ S[a] \bullet 03 \end{bmatrix}; T_1[a] = \begin{bmatrix} S[a] \bullet 03 \\ S[a] \bullet 02 \\ S[a] \\ S[a] \end{bmatrix};$$

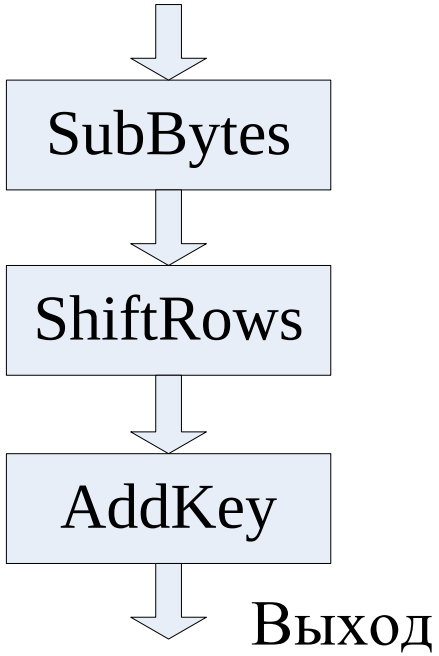
$$T_2[a] = \begin{bmatrix} S[a] \\ S[a] \bullet 03 \\ S[a] \bullet 02 \\ S[a] \end{bmatrix}; T_3[a] = \begin{bmatrix} S[a] \\ S[a] \\ S[a] \bullet 03 \\ S[a] \bullet 02 \end{bmatrix} \quad (2)$$

$$\begin{bmatrix} e_{0j} \\ e_{1j} \\ e_{2j} \\ e_{3j} \end{bmatrix} = T_0[a_{0j}] \oplus T_1[a_{1j-1}] \oplus T_2[a_{2j-2}] \oplus T_3[a_{3j-3}] \oplus \begin{bmatrix} k_{0j} \\ k_{1j} \\ k_{2j} \\ k_{3j} \end{bmatrix} \quad (3)$$

4 White Box AES-128







5 White Box AES-128

По результатам анализа T-box таблиц был построен алгоритм восстановления скрытого ключа.

$$S[val_1 \oplus a] \oplus val_2 = S'[a], \quad (4)$$

$S'[a]$ -результат для каждого входного байта после применения *InvMixColumns;*

$S[x]$ -S-box классического AES-128.

6 Усиленный вариант схемы

1. Используется другое конечное поле (не Rijndael).
2. Используется другой полином в операции MixColumns.

Элементы T-box-ов линейно зависимы друг от друга, поэтому взлом такой схемы возможен посредством нахождения конечного поля и полинома, обратного используемому в операции MixColumns, с последующим построением таблиц инверсии общим размером 40 К.

7 Возможные варианты усиления схемы

1. Введение дополнительных операций циклического сдвига для каждого элемента T-box-а с учетом этого факта в T-box-ах следующего раунда (взлом практически не усложняется).

2. Использование следующего факта:

$$((a \cdot b)(mod\, p_1) \cdot c)(mod\, p_2) \neq (a \cdot (b \cdot c)(mod\, p_2))(mod\, p_1), (5)$$

p_1, p_2 - неприводимые полиномы 8-й степени.

Таким образом, каждый элемент T-box-а умножается на полином в произвольно выбранном конечном поле. При генерации T-box-ов следующего раунда производятся обратные операции.

8

Возможные варианты усиления схемы

ВЫВОД: Возможно построение таблиц инверсии размером 154 Гб. AES мало пригоден для White Box криптографии в силу своей архитектуры.

9

Возможные варианты усиления схемы

1. Операция MixColumns выполняется по модулю $x^{16}+1$.

2. S-box генерируются случайным образом.

3. Полином для MixColumns генерируется случайным образом с учетом необходимости существования обратного.

4. Использование формулы (5) для усложнения нахождения линейной зависимости между элементами T-box-ов.

Пилотный вариант такой схемы уже создан

10 Открытые вопросы

1. Необходимо разработать методику генерации полиномов для операции MixColumns.

2. Необходимо разработать методику генерации S-box-ов, чтобы минимизировать возможность генерации слабых таблиц подстановки.

3. Необходимо оценить количество применений формулы (5) по отношению к элементам T-box таблиц.

11

ВЫВОДЫ

1. Для создания White Box схем необходимо создание специализированных блочных шифров.

2. На базе описанных подходов был создан генератор T-box-таблиц и пример их использования.

ВОПРОСЫ