конференция
РусКрипто

Ежегодная международная научно-практическая конференция

«РусКрипто'2023»

РАЗРАБОТКА СПОСОБОВ ПОИСКА ЭКВИВАЛЕНТНЫХ КЛЮЧЕЙ В ПОТОЧНЫХ ШИФРСИСТЕМАХ, ОСНОВАННЫХ НА АЛГОРИТМЕ ГЕНЕРАЦИИ СЛУЧАЙНЫХ ПОДСТАНОВОК ФИШЕРА-ЙЕТСА

Киндеев Юрий,
студент, НИЯУ МИФИ

Научный руководитель:
Пудовкина Марина Александровна, д.ф-м.н., профессор, НИЯУ МИФИ

Поточная шифрсистема RC4 и ее модификации


Ronald Linn Rivest

RC4 разработан в 1987 году Роном Ривестом для RSA Data Security.

На основе RC4 разработано множество модификаций:

- RC4A (2004)
- VMPC (2004)
- ТРу6-A и ТРу6-B (2007)
- RC4+ (2008)
- NGG и GGHN (2011)
- Spritz (2014)
- mRC4 (2019)
- eRC4 (2021)
- RC4D (2021)
- и другие.

Анализу RC4 и её модификаций посвящено множество работ:

- S. Sarkar Further non-randomness in RC4, RC4A and VMPC // WCC 2013, April 15–19, 2013
- Sumartono, I. Siahaan, A. Putera, U. Mayasari Nova An Overview of the RC4 Algorithm. IOSR Journal of Dental and Medical Sciences. 2016

Описание алгоритма генерации начальной подстановки (KSA) в RC4

- RC4 моделируется автономным автоматом:

Функция ρ:

s_0' – тождественная подстановка, $i_0 = 0,\ j_0 = 0.$

Для $\forall\ t \in \{1, \dots, m\}$:

1. $i_t = i_{t-1} + 1\ ,$
2. $j_t = j_{t-1} + s_{t-1}'[i_t] + k_{t-1(mod\ L)}(mod\ m)\ ,$
3. переставляем элементы $s_t'[i_t], s_t'[j_t]$ местами

- Алгоритм Фишера-Йетса:

1. Первоначально полагаем:

s – тождественная подстановка

2. Для $i = m - 1, m - 2, \dots, 1$ выполняем:
   a. Выработать случайное число $r_i \epsilon Z_m$
   b. Выполнить транспозицию $s[i] \leftrightarrow s[r_i]$

- Основная идея заключается в использовании алгоритма Фишера-Йетса для генерации начальной подстановки

Уязвимости шифрсистемы RC4

- 1. Корреляция гаммы и ключа
- 2. Корреляция подстановок и ключа
- 3. Использование не случайных или связанных ключей
- 4. Использование одной гаммы дважды
- 5. Классы эквивалентных ключей
- (кол-во ключей $m^m > m!$ кол-ва подстановок)

S. Maitra, G. Paul Analysis of RC4 and Proposal of Additional Layers for Better Security Margin // INDOCRYPT 2008
M. McKague Design and Analysis of RC4-like Stream Ciphers UWSpace 2005
A. Roos A class of weak keys in the RC4 stream cipher Vironix Software Laboratories 1995
S. Paul, B. Preneel A New Weakness in the RC4 Keystream generator and an approach to improve the security of the cipher Lecture notes in computer science : journal 2004

Сравнительный анализ алгоритма генерации начально подстановки RC4 и модификации RC4A

- RC4A

Функция ρ:

s_0' – тождественная подстановка, $i_{1,0} = 0, j_{1,0} = 0,\ j_{2,0} = 0.$

Для $\forall\ t \in \{1, \dots, m\}$:

1. $i_t = i_{t-1} + 1\ ,$
2. $j_{1,t} = j_{1,t-1} + s'_{1,t-1}[i_t] + k_{t-1(mod\ L)}(mod\ m)\ ,$
3. переставляем элементы $s'_{1,t}[i_t], s'_{1,t}[j_{1,t}]$ местами
4. $j_{2,t} = j_{2,t-1} + s'_{2,t-1}[i_t] + k_{t-1(mod\ L)}(mod\ m),$
5. переставляем элементы $s'_{2,t}[i_t], s'_{2,t}[j_{2,t}]$ местами

RC4

Функция ρ:

s_0' – тождественная подстановка, $i_0 = 0,\ j_0 = 0.$

Для $\forall\ t \in \{1, \dots, m\}$:

1. $i_t = i_{t-1} + 1\ ,$
2. $j_t = j_{t-1} + s'_{t-1}[i_t] + k_{t-1(mod\ L)}(mod\ m)\ ,$
3. переставляем элементы $s'_t[i_t], s'_t[j_t]$ местами

Сравнительный анализ алгоритма генерации начально подстановки RC4 и модификации VMPC

- VMPC

Функция ρ:

s_0' – тождественная подстановка, $i_0 = 0,\ j_0 = 0.$

Для $\forall\ t \in \{1, \dots, m\}$:

1. $i_t = i_{t-1} + 1 (mod\ m),$
2. $j_t = j_{t-1} + 1 (mod\ 3m),$
3. $s = p_t'[s + p_{t-1}'[i] + k_{j\,(mod\ L)}]) mod\ m],$
4. переставляем элементы $p_t'[i_t], p_t'[s]$ местами

RC4

Функция ρ:

s_0' – тождественная подстановка, $i_0 = 0,\ j_0 = 0.$

Для $\forall\ t \in \{1, \dots, m\}$:

1. $i_t = i_{t-1} + 1\ ,$
2. $j_t = j_{t-1} + s_{t-1}'[i_t] + k_{t-1(mod\ L)} (mod\ m)\ ,$
3. переставляем элементы $s_t'[i_t], s_t'[j_t]$ местами

Сравнительный анализ алгоритма генерации начально подстановки RC4 и модификации RC4D

- RC4D

Функция ρ:

$s_0^{'}$ – тождественная подстановка, $i_0 = 0,\ j_0 = 0.$

Для $\forall\ t \in \{1, \dots, m\}$:

1. $i_t = t + 1,$
2. $j_t = (j_{t-1} + s_{t-1}^{'}[i_t + k_{t-1(mod\ L)}] + k_{t-1(mod\ L)})(mod\ m),$
3. переставляем элементы $s_t^{'}[i_t], s_t^{'}[j_t]$ местами

RC4

Функция ρ:

$s_0^{'}$ – тождественная подстановка, $i_0 = 0,\ j_0 = 0.$

Для $\forall\ t \in \{1, \dots, m\}$:

1. $i_t = i_{t-1} + 1\ ,$
2. $j_t = j_{t-1} + s_{t-1}^{'}[i_t] + k_{t-1(mod\ L)}(mod\ m)\ ,$
3. переставляем элементы $s_t^{'}[i_t], s_t^{'}[j_t]$ местами

Алгоритмы поиска эквивалентных ключей

Вход: длина ключа l, d – номер позиции, в которой будут отличаться ключи

Выход: пара эквивалентных ключей $k \neq k'$ таких, что $KSA(k) = KSA(k')$

- 1. Случайно генерируется пара ключей, которые отличаются в позиции d.
- 2. Итеративный поиск эквивалентных ключей :
- 2.1 Положим в s значение шагов, для которых $\chi(s_1, s_2) \leq 2$ для начальных состояний s_1, s_2. Если s=255, то найдена пара эквивалентных ключей .
- 2.2 Иначе изменяем значения ключей:

$k[x] = k[x] + y$,

$k[x + 1] = k[x + 1] - y$ для всех x, y

Переходим к шагу 2.1

M. Matsui, O. Dunkelman, B. Preneel Key collisions of the RC4 stream cipher FSE 2009, LNCS, vol. 5665, Springer, Heidelberg 2009

Оценки трудоемкостей алгоритмов Чэнь-Миядзи и Мацуи

Длина ключа в байтах	Алгоритм Мацуи	Алгоритм Чэнь-Миядзи
20	2^{16}	2^{36}
22	2^{18}	2^{38}
24	2^{20}	2^{40}
26	2^{22}	2^{42}
28	2^{25}	2^{48}
30	2^{30}	2^{55}
32	2^{40}	2^{65}

J. Chen, A. Miyaji Novel strategies for searching RC4 key collisions. Computers & Mathematics with Applications,Volume 66, Issue 1, 2013

Разработанный алгоритм поиска эквивалентных ключей

Вход: m_0, шаг d, m

Выход: пара эквивалентных ключей $k \neq k'$ таких, что $KSA(k) = KSA(k')$

- 1. Инициализируем алгоритм генерации начальной подстановки RC4 с заданным m_0.
- 2. Находим пару эквивалентных ключей методом полного перебора и сохраняем их в k_1 и k_2 .
- 3. $m_0 := m_0 + d$.
- 4. Находим пару эквивалентных ключей k_1', k_2' длины m_0 :
- полагаем первые $m_0 - d$ элементов k_1', k_2', равными k_1 и k_2 соответственно. Перебираем последние d элементов k_1', k_2' так, чтобы
- KSA(k_1') = KSA(k_1')
- 5. Если $m_0 < m$, то перейти на Шаг 3.

Оценка сверху трудоемкости разработанного алгоритма

- Элементарная операция – выполнение алгоритма генерации начальной подстановки для параметра m
- Находится одна пара эквивалентных ключей

Значение параметра m	При $k = 2$ трудоемкость	При $k = 4$ Трудоемкость
20	$2^{8,6}$	$2^{17,2}$
22	$2^{8,9}$	
24	$2^{9,1}$	$2^{18,3}$
26	$2^{9,4}$	
28	$2^{9,6}$	$2^{19,2}$
30	$2^{9,8}$	
32	2^{10}	2^{20}
256	2^{16}	2^{32}

Оценка вероятности успеха алгоритма

- Под «успехом» алгоритма понимается вероятность найти пару эквивалентных ключей
- Вероятности $p_{\text{усп}}$ найдены экспериментально, для заданных m были опробованы все ключи

Значение параметра m	RC4 $p_{\text{усп}}$	RC4A $p_{\text{усп}}$	VMPC $p_{\text{усп}}$	RC4D $p_{\text{усп}}$
4	1	1	1	1
6	0,985	0,874	0,796	0,863
8	0,897	0,789	0,725	0,805

Вопросы

???

Контактная информация

Электронная почта:

yura2015b@gmail.com

Телефон:

+7 938 316-69-85

Список использованных источников

1. R. Rivest RSA security response to weaknesses in key scheduling algorithm of RC4 // Technical note, RSA Data Security Inc. 2001.
2. R. A. Fisher, F. Yates, Statistical Tables // London– 1938.
3. B. Zoltak VMPC One-Way Function and Stream Cipher // FSE’04, Delhi, India, 2004.
4. S. Paul, B. Preneel A New Weakness in the RC4 Keystream generator and an approach to improve the security of the cipher // Lecture notes in computer science : journal. — 2004. — Vol. 3017. — P. 245—259.
5. R. Alsharidal, M. Hammood , M. A. Ahmed , B. Thamer, M. Shakir RC4D: A New Development of RC4 Encryption Algorithm // Lecture Notes in Networks and Systems, vol 180. Springer 2021
6. J. Chen, A. Miyaji Novel strategies for searching RC4 key collisions. Computers & Mathematics with Applications,Volume 66, Issue 1, 2013.
7. S. Maitra, G. Paul Analysis of RC4 and Proposal of Additional Layers for Better Security Margin // INDOCRYPT 2008, LNCS 5365, pp. 27–39, 2008.
8. I. Mantin A practical attack on the fixed RC4 in the WEP mode, // ASIACRYPT, volume 3788 of Lecture Notes in Computer Science, Springer 2005, pp. 395-411.
9. Sumartono, I. Siahaan, A. Putera, U. Mayasari Nova An Overview of the RC4 Algorithm. IOSR Journal of Dental and Medical Sciences. 2016.