А.В. АЛЕКСАНДРОВ, к.ф-м.н. доцент каф. ИЗИ;
А.Д. МЕТЛИНОВ, студент гр. КЗИ-108.

АЛГОРИТМЫ ШИФРОВАНИЯ И ДЕШИФРОВАНИЯ НА ОСНОВЕ СХЕМЫ SMT LSS BROADCAST. ВЫБОР ПОЛЯ ГАЛУА И ДЛИНЫ БЛОКА ПЕРЕДАЧИ. МОДЕЛЬНЫЙ ЭКСПЕРИМЕНТ / ENCRYPTION AND DECRYPTION ALGORITHMS BASED ON THE SCHEME OF THE SMT LSS BROADCAST. GALOIS FIELD SELECTION. A MODEL EXPERIMENT

Предложены первые варианты алгоритмов шифрования и дешифрования на основе ранее описанной схемы SMT LSS broadcast. Произведен выбор поля Галуа, в котором будут происходить все последующие вычисления (операции) данного алгоритма. Осуществлена оценка средней длины блока, который будет формироваться алгоритмом и передаваться за один раз. Проведено тестирование возможности разложения секретов в базисе необходимой возрастающей последовательности (в заданном поле Галуа). Теоретически доказана оценка величины плотности укладки рюкзака, которая была экспериментально получена и приведена в предыдущей работе.

Ключевые слова: АЛГОРИТМ ШИФРОВАНИЯ, АЛГОРИТМ ДЕШИФРОВАНИЯ, МОДЕЛЬНЫЙ ЭКСПЕРИМЕНТ, ПОЛЕ ГАЛУА, ЗАДАЧА ОБ УКЛАДКЕ РЮКЗАКА, SMT.

7 источников.

Proposed the first versions of the encryption and decryption algorithms based on a previously described scheme of the SMT LSS broadcast. Make our selection of the Galois field, which will take place all calculations (operations) of the algorithm. The estimation of the average length of the block, which will be formed by the algorithm and transmitted at the same time. Tested the possibility of secret's expansion in the basis of necessary increasing sequence (in a given Galois field). In theory proved estimate of the density of packing a backpack, which was obtained experimentally and shown in previous work.

Keywords: ENCRYPTION ALGORITHM, DECRYPTION ALGORITHM, A MODEL EXPERIMENT, GALOIS FIELD, THE PROBLEM OF PACKING A BACKPACK, SMT.

7 sources.

Объектами исследования данной работы являются: математические алгоритмы шифрования и дешифрования информации, основанные на ранее описанной схеме SMT LSS broadcast; проблема выбора поля Галуа и средней длины блока, который будет формироваться алгоритмом и передаваться за один раз; исследование зависимости количества случаев появления дополнительного коэффициента Δ от величины плотности укладки.

Цели работы – теоретическое (математическое) построение алгоритмов шифрования и дешифрования информации с использованием схемы SMT LSS broadcast; теоретический вывод оценки величины плотности укладки рюкзака, которая была экспериментально получена и приведена в предыдущей работе; выбор конкретного поля Галуа и средней длины блока, который будет формироваться алгоритмом и передаваться за один раз; проведение тестирования возможности разложения секретов в базисе необходимой возрастающей последовательности (в заданном поле Галуа); экспериментальное исследование зависимости количества

случаев появления дополнительного коэффициента Δ от величины плотности укладки.

В процессе разработки темы проводилось теоретическое рассмотрение отдельных работ Куросавы и Сузуки по проектированию алгоритмов шифрования и дешифрования, их научному оформлению.

В конечном итоге будут приведены алгоритмы шифрования и дешифрования информации с использованием схемы SMT LSS broadcast, теоретический вывод оценки величины плотности укладки рюкзака в заданной возрастающей последовательности; результаты проведенного тестирования и результаты выбора поля Галуа и средней длины блока передачи.

На первом этапе выполнения данной работы был произведен выбор конкретного поля Галуа, в котором будет происходить все последующие вычисления (операции). Осуществлен выбор средней длины блока передачи и реализован эксперимент по исследованию зависимости количества случаев появления дополнительного коэффициента Δ от величины плотности укладки.

Основным моментом на данном этапе проектирования алгоритма передачи сообщений с использованием схемы SMT LSS является необходимость оценки средней длины блока - l, который будет формироваться алгоритмом и передаваться за один раз. Предполагается, что передаваемый секрет (документ) состоит из большого количества символов и делится на блоки одинаковой длины l, последний блок при необходимости дополняется до заданной длины.

Для удобства работы в конкретной IDE (использование стандартных типов данных) и быстроты выполнения необходимых расчетов, при выборе длины блока передаваемой информации разумно остановится на величине $l = 64$, если длину блока брать меньше – очень сильно падает плотность укладки, что в нашем случае неприемлемо. Все элементы сформированной возрастающей последовательности будут находиться в пределах значений $1 \leq f_i \leq 2^l-1$, при достаточно больших значениях i.

Плотность вышеописанной последовательности будет находиться в пределах $1.00 \leq d \leq 1.15$ ($d \sim 1.10$), что соответствует заданным требованиям усложнения

возможности осуществления L^3-атаки на данную криптологическую рюкзачную систему. Также при таких значениях плотности укладки заданной исходной возрастающей последовательности выполняется условие единственности (в общем случае) решения криптологической задачи об укладке рюкзака. Если исходная ключевая последовательность {E} будет содержать только нули (ключ отсутствует – {E} = 0), то в формируемую возрастающую последовательность будет записан классический ряд Фибоначчи, плотность которого соответствует заданным требованиям усложнения успешного проведения L^3-атаки на рюкзачную криптосистему. Плотность такого ряда приблизительно равна d = 1.72.

В соответствии с выбранным размером блока подбирается поле Галуа, в пределах которого будут происходить все последующие вычисления, которому будут принадлежать все элементы заданной возрастающей последовательности. Для блока длины l = 64 необходимо взять поле Галуа – GF_p, где p ~ 2^{64}. Плотность укладки для такого рюкзака равна d = 1.0747. Полученная плотность удовлетворяет вышеописанным условиям. Выше приведена примерная оценка величины p, где p необходимо подобрать так, чтобы число находилось близко к заданному значению и являлось бы простым.

После выбора конкретного поля Галуа и длины блока, который будет формироваться алгоритмом, а затем передаваться за один раз можно приступить к проведению модельного эксперимента на сформированной рюкзачной криптосистеме (на конкретной возрастающей последовательности).

План проведения тестирования:

- выбор числа p, довольно большого значения, для формирования необходимого поля Галуа GF_p;
- формирование конкретно заданного поля Галуа GF_p, где $GF_p = \{0, 1, \dots, p-1\}$;
- выбор (задание) начального ключа $k = \{k_1, k_2, \dots, k_n\}$, с помощью которого из начальной общей базы документов $\{d_1, d_2, \dots, d_n\}$ формируется необходимая возрастающая последовательность $\{f_1, f_2, \dots, f_n\}$, плотность

укладки которой удовлетворяет заданным условиям усложнения успеха проведения L^3-атаки на эту рюкзачную криптосистему;

- до того момента, пока $f_i < p-1$ строим возрастающую последовательность $\{f_1, f_2, \dots, f_n\}$;
- для полученной возрастающей последовательности $\{f_1, f_2, \dots, f_n\}$ считаем и выводим значение плотности укладки;
- в итоге, формирование возрастающей последовательности $\{f_1, f_2 \dots f_n\}$ необходимо и возможно подчинить следующим условиям: плотность укладки рюкзака $d \geq 1$ ($d \sim 1$) и значения элементов последовательности в пределах $1 \leq fi \leq 2^l-1$;
- для всех целых чисел от единицы до p-1 решается аддитивная задача разложения секрета с помощью «жадного алгоритма»;
- регистрация при разложении заданных секретов количества случаев, когда $\Delta \neq 0$, обозначим эту величину как «amount»;
- определение зависимости числа случаев появления Δ ($\Delta \neq 0$) от плотности укладки заданной возрастающей последовательности – f = amount (d).

После проведения данного эксперимента строится общая таблица, с помощью которой будет произведена попытка выявления зависимости f = amount (d). Итог тестирования позволяет сделать следующие выводы:

- при величине плотности укладки в заданных пределах ($d \sim 1$) количество случаев, когда появляется коэффициент Δ в процессе разложения секрета, составляется 15-25% от общего числа разложений;
- при уменьшении величины плотности укладки увеличивается количество случаев появления коэффициента Δ;
- для классического ряда Фибоначчи количество вышеописанных случаев появления Δ стремится к нулю.

Сами результаты тестирования будут предоставлены в отдельном Excel – файле, который идет в дополнение к данному отчету.

На втором этапе выполнения данной работы было сформировано математическое описание алгоритмов шифрования и дешифрования информации с использованием ранее описанной схемы SMT LSS broadcast.

Для начала между отправителем и получателем необходимо организовать (создать) ту самую «общую память», путем информационного обмена между ними определенными документами с помощью широковещательной рассылки – broadcast. После проведения широковещательной рассылки у отправителя и получателя создается общая база документов - $\{d_1 \ldots d_n\}$, где $S_1 = d_1, \ldots, S_n = d_n$ ($S_1 \ldots S_n$ – исходные документы). Отсюда отправитель и получатель имеют совокупность документов $\{d_1 \ldots d_n\}$, причем $d_i \neq d_j$ (нет смысла передавать один и тот же документ два раза и более). Для передачи секрета S будет использоваться криптографическая задача об укладке рюкзака. Предполагается, что передаваемый секрет (документ) состоит из большого количества символов и делится на блоки одинаковой длины *l* равной десяти символам, последний блок при необходимости заполняется нулями (пробелами) до фиксированной длины.

Предположим, что элементы открытого текста обозначаются k-разрядными двоичными числами, где k — некоторое натуральное число. Например, для русского алфавита, состоящего из 32 букв (одновременно стоит учесть знаки препинания, пробелы, цифры и т.п.), каждую из них можно обозначить шестиразрядным двоичным числом от $0 = (000000)_2$ до $63 = (111111)_2$, т.е. а = 000000, б = 000001, . . ., е = 000101, . . ., н = 001101, . . ., т = 010010, затем идут цифры, знаки препинания и т.д. Возможно увеличение разрядности каждого символа, но при этом длина блока будет уменьшена, чтобы необходимые вычисления все также производились в заданном поле Галуа GF_p.

В засекречиваемом тексте берутся блоки длины в 10 символов. Каждый символ представляется в виде шестиразрядного двоичного числа, получается последовательность из 10 * 6 = 60-рязрядного двоичного числа, которое затем переводится назад в десятичную систему счисления. Часть секрета теперь представлена в виде целочисленного числа довольно большого порядка (15-20

знаков), которое будет подвержено разложению в заданной возрастающей последовательности «типа Фибоначчи».

Алгоритм шифрования:

1. С помощью документов из «общей памяти» формируется возрастающая (в поле Галуа GF_p, где p-простое и $p \sim 2^{64}$) последовательность «типа Фибоначчи» $\{f_1, f_2, \dots f_n\}$, где $f_1 = 1$, $f_2 = d_1*k_1$, $f_3 = d_2*k_2 + f_2 + f_1$, $f_4 = d_3*k_3 + f_3 + f_2 + f_1$, …, $f_n = d_{n-1}*k_{n-1} + f_{n-1} + \sum f_i$, $\{k_1 \dots k_n\}$ – ключ формирования $\{f_1 \dots f_n\}$, где $k_i = 1$ – элемент d_i участвует в формировании последовательности или $k_i = 0$ – не участвует.

2. Каждый секрет S (секретный документ) в любом случае может быть представлен в виде целочисленного числа довольно большого порядка (15-20 знаков). Вариант формирования подобного числа из заданного текста описан выше.

3. С помощью «жадного алгоритма» исходный секрет S раскладывается ранее описанным способом в базисе заданной возрастающей последовательности «типа Фибоначчи» $\{f_1, f_2, \dots f_n\}$.

4. После разложения секрета в рамках заданной возрастающей последовательности получаем ключ его разложения $E = \{e_1, e_2 \dots e_n\}$, где $e_i = 0$, либо $e_i = 1$ и $E \neq \{0, 0, \dots 0\}$ – ключ не существует.

5. Если элемент e_i ключевой последовательности $\{E\}$ равен единице, то соответствующий элемент f_i возрастающей последовательности входит в разложение секрета S, если элемент e_i ключевой последовательности $\{E\}$ равен нулю, то соответствующий элемент f_i возрастающей последовательности не входит в разложение секрета S.

6. Полученная ключевая последовательность передается получателю с помощью схемы разделения секрета, либо по выделенному каналу связи. Вместе с ключом передается сформированная возрастающая последовательность $\{f_1, f_2, \dots f_n\}$. Возможна ее передача по открытым каналам. Обеспечение ее секретности не обязательно. При разложении секрета, может возникнуть ситуация, когда появляется ранее описанный дополнительный коэффициент Δ. Его также необходимо передать получателю вместе с ключевой последовательностью.

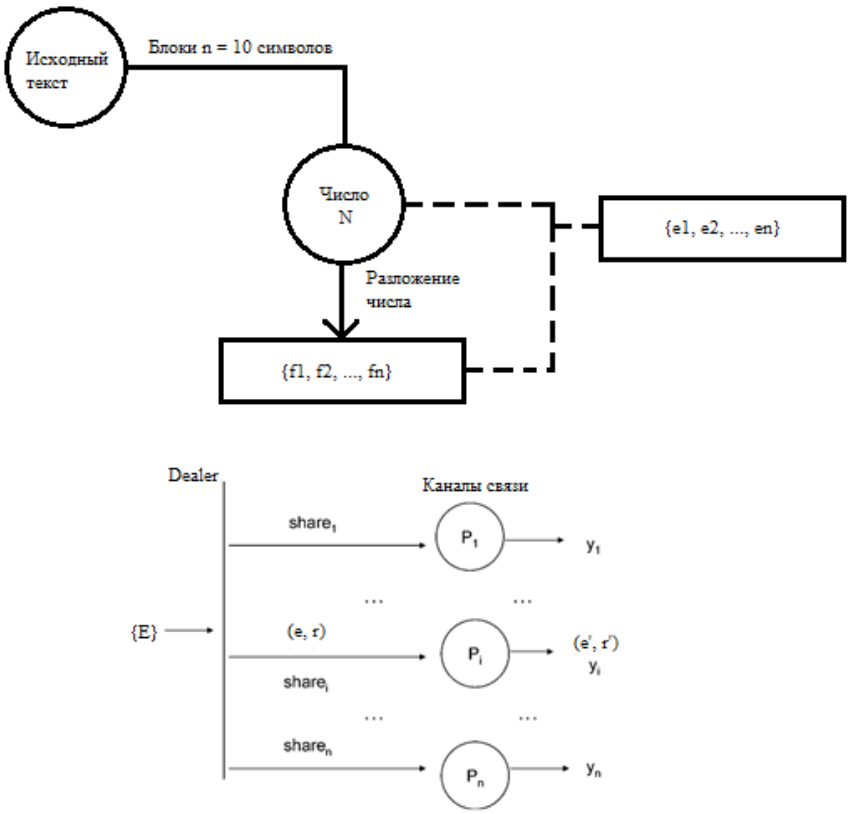

Рисунок 1 – Структурная схема алгоритма шифрования и передачи ключа

Алгоритм дешифрования:

1. С помощью полученного ключа и возрастающей последовательности осуществляется восстановление секрета. Полученная ключевая последовательность делится на блоки длины в 64 бита. Восстановление секрета осуществляется по блокам заданной длины.

2. Производится отображение первого блока ключа на возрастающую последовательность (если элемент e_i ключевой последовательности {E} равен единице, то соответствующий элемент f_i возрастающей последовательности входит в сумму восстановления секрета S и наоборот), в результате чего происходит восстановление первого блока секрета. Если для данного блока ключевой последовательности присутствует дополнительный коэффициент Δ, то его необходимо прибавить к итоговой сумме восстановления.

3. Процесс восстановления секрета осуществляется n-раз, где n – количество блоков информации.

4. Полученное число N (большого порядка) представляется как 60-рязрядное двоичное число, которое делится на 10 шестиразрядных чисел. Полученные числа

переводятся в десятичную систему счисления, каждому числу ставится в соответствие заданный символ.

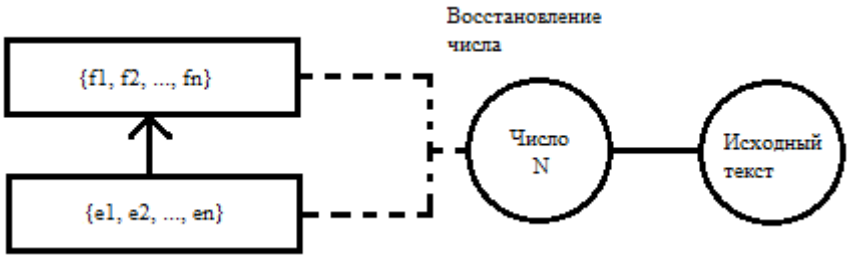

Рисунок 2 – Структурная схема алгоритма дешифрования

На последнем этапе выполнения данной работы был произведен теоретический вывод оценки величины плотности укладки рюкзака, которая была экспериментально получена и приведена в предыдущей работе.

Пусть $\{d_1, d_2, \dots d_n\}$ – исходная совокупность документов («общая память»), $\{k_1, k_2, \dots k_n\}$ – ключ формирования возрастающей последовательности в заданном поле Галуа. Сумму всех элементов исходных документов обозначим как $d = \sum d_i$.

$d_e = \sum (e_i * d_i)$ – элемент формируемой возрастающей последовательности $\{f_1, f_2, \dots f_n\}$, где d_e участвует в формировании элемента f_i, если соответствующий элемент ключа k_i равен единице и наоборот.

Обозначим f_n^0 – классический ряд Фибоначчи. С помощью документов из «общей памяти» формируется возрастающая (в поле Галуа GF_p, где p-простое и $p \sim 2^{64}$) последовательность «типа Фибоначчи» $\{f_1, f_2, \dots f_n\}$, где $f_1 = 1$, $f_2 = d_1 * k_1$, $f_3 = d_2 * k_2 + f_2 + f_1$, $f_4 = d_3 * k_3 + f_3 + f_2 + f_1$, …, $f_n = d_{n-1} * k_{n-1} + f_{n-1} + \sum f_i$, $\{k_1 \dots k_n\}$ – ключ формирования $\{f_1 \dots f_n\}$, где $k_i = 1$ – элемент d_i участвует в формировании последовательности или $k_i = 0$ – не участвует. Или $f_1 = 1$, $f_2 = d_{e1}$, $f_3 = d_{e2} + f_2 + f_1$, …, $f_n = f_n^0 + f_{n-1}^0 * d_{en}$.

Отсюда получаем следующую оценку величины плотности укладки для описанной ранее рюкзачной криптосистемы на основе SMT LSS broadcast: $\frac{n}{log_2 (f_n^0 + f_{n-1}^0 * \text{den})} \leq \frac{n}{log_2 f_n} \leq \frac{n}{log_2 f_n^0}$. Так как плотность укладки рюкзака равна $d = \frac{n}{log_2 f_n}$, то получаем $\frac{n}{log_2 (f_n^0 * (|d|+1))} \leq d \leq \frac{n}{log_2 f_n^0}$.

В итоге получается следующая теоретическая оценка плотности рюкзака для заданной криптосистемы, которая полностью соответствует ранее полученной экспериментальной оценке:

$$\frac{n}{[\,log_2 f_n^0 + log_2\,(d+1)\,]} \leq d \leq \frac{n}{log_2 f_n^0} \quad (1).$$

В дальнейшем планируется работа по корректированию алгоритмов шифрования и дешифрования информации. После выполнения всех необходимых корректировок и изменений планируется их практическая реализация.

Литература

1. *Coster M. J., Joux A., LaMacchia B. A.*, et al. Improved low-density subset sum algorithms // Computational Complexity. 1992. No. 2. P. 111–128.

2. *Lagarias J. C., A. M. Odlyzko* – Solving low-density subset problems, Proc. 24th Annual IEEE Symp. on Found, of Corp. Science, pp. 1-10, 1983.

3. *Odlyzko A. M. and Lagarias J. C.* Solving Low-Density Subset Sum Problems // J. Association Computing Machinery. 1985. V. 32. No.1. P. 229–246.

4. *Черемушкин А.В.* Криптографические протоколы: основные свойства и уязвимости. М.: 2009, 36с.

5. *К. Шеннон.* Работы по теории информации и кибернетике. // ИИЛ, Москва 1963, 829с.

6. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си // М.: "Триумф", 2002.

7. *Под редакцией Ященко*. Введение в криптографию. Новые математические дисциплины. // МЦНМО Санкт-Петербург, 2001, 288с.