· http://ucom.ru/na · ISSN 2411-7609 · Science Almanac ·

DOI: 10.17117/na.2017.03.03.072 http://ucom.ru/doc/na.2017.03.03.072.pdf
Поступила (Received): 23.03.2017

Димитриев А.П.
Модель шифрования с учетом повреждения данных на основе сетей Петри

Dimitriev A.P.
Model of encryption with account data damage based on Petri nets

Для ранее разработанной криптографической системы алгоритм шифрования является симметричным блочным на основе аналитических преобразований. Для системы построена математическая модель на основе сети Петри. Рассмотрен вопрос о надежности хранения информации при шифровании. Предложена модификация метода, направленная на увеличение средней длины восстанавливаемого участка после сбоя на носителе данных. Для ее моделирования построена сеть Петри, записанная при помощи полинома

Ключевые слова: *блочное шифрование, сеть Петри, повреждение данных*

For previously developed cryptographic system, encryption algorithm is a symmetric block based on analytical transformations. For this system, developed a mathematical model based on Petri nets. Considered the issue of reliability of data storage when encrypting. Proposed modification of the method aimed at increasing the average length of the site being restored after a failure on a data carrier. For it modeling is built Petri net, that wrote by polynomial

Key words: *block cipher, Petri net, data corruption*

Димитриев Александр Петрович
Кандидат технических наук, доцент
Чувашский государственный университет им. И.Н. Ульянова
г. Чебоксары, Московский пр., 15

Dimitriev Alexander Petrovich
Candidate of Technical Sciences, Associate Professor
Chuvash state university named I.N. Ulyanov
Cheboksary, Moskovskiy ave., 15

На основе принципов защиты базы данных, применяемых в [7, с. 44], разработана криптографическая система [2, с. 64], [3, с. 65], [4, с. 40], [5, с. 41], [10, с. 139]. Применяемый для нее алгоритм шифрования является симметричным блочным на основе аналитических преобразований [6, с.2].

Возникает вопрос о надежности хранения зашифрованных данных. На практике нередко происходит их повреждение. Это характерно, например, для ситуаций появления сбойных блоков на жестком диске. Последующая дешифрация сталкивается с проблемой, состоящей в том, что начиная с места повреждения в файле она невозможна.

Цель работы – разработать подход к улучшению возможности восстановления поврежденных данных после шифрования. Для этого сначала разработаем математическую модель системы.

Математическую модель предлагается построить на основе сетей Петри, которые иногда применяются для моделирования шифрования [9, с. 70], [11, с.

· http://ucom.ru/na · ISSN 2411-7609 · Science Almanac ·

1372], [12, с. 317]. Предположим, что исходный текст можно разбить на блоки одинаковой длины. Зашифрованный текст, обозначаемый {*S*}, будет состоять из блоков такой же длины, как у исходного текста.

Предлагаемая модель для алгоритма шифрования [5, с. 41] изображена на рис. 1.

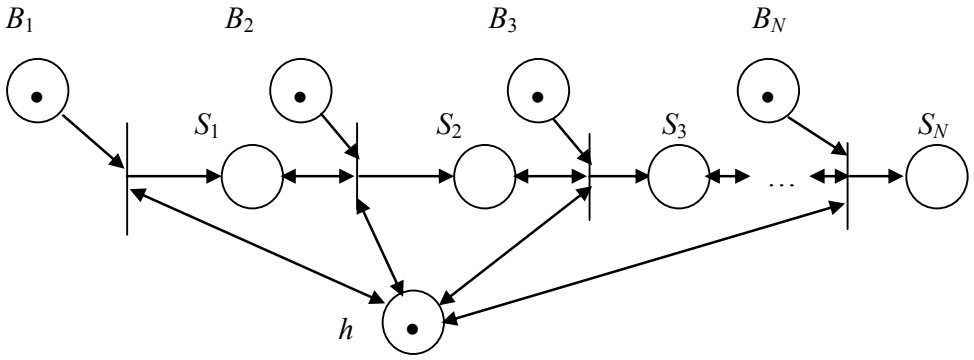

Рис. 1. Модель исходного алгоритма шифрования

В данной модели используются следующие обозначения:

– N – количество блоков, на которые разбивается исходный текст.

– B_i – позиция, которая в исходном состоянии содержит в качестве метки i-й блок исходного текста, $i = \overline{1, N}$;

– S_i – позиция, которая в конечном состоянии должна содержать в качестве метки *i*-й блок {*S*}, $i = \overline{1, N}$;

– *h* – позиция, хранящая хэш-функцию от пароля.

Начальная маркировка следующая: $h(1)$, $B_i(1)$, $i = \overline{1, N}$. Срабатывание любого перехода означает операцию по шифрованию содержимого соответствующего блока. Модель в определенной степени условна, для получения следующих блоков {*S*} используются более сложные преобразования, направленные против взлома [1, с. 193].

Рассмотрим случай повреждений данных одного блока: $B_i \rightarrow B_i'$. В разработанном ранее алгоритме [4, с. 40] возможна расшифровка файла только до B_i'. Если вероятность повреждения блока $p(B_i \rightarrow B_i') = 1/N \; \forall i \in [1, N]$, то в среднем удается восстановить почти половину файла. Точнее, первую половину за вычетом ½ размера блока, т.е. среднее суммарное количество восстанавливаемых данных $R = l(B_i) \cdot (N-1)/2$.

Предлагаемая далее модель имеет целью увеличение *R*. Если *N* заранее известно, то данные в файле можно представить в виде иерархии блоков. Пусть каждый блок, кроме блоков последнего уровня, порождает три блока. Всего *N*=13: один блок первого уровня, три – второго и девять – третьего. Тогда модель шифрования на основе представления сети Петри в виде полинома [8, с. 57] имеет следующий вид:

$$hp_1B_1t^0hp^1{}_1p^1{}_2p^1{}_3S_1 + \sum_{i=1}^{3} hp_i^1 B_{i+1} t_i^1 hS_{i+1} p_{3i-2}^2 p_{3i-1}^2 p_{3i}^2 + \sum_{i=1}^{9} hp_i^2 B_{i+4} t_i^2 hS_{i+4},$$

причем начальная маркировка $B_i(1)$, $i = \overline{1, N}$.

· http://ucom.ru/na · ISSN 2411-7609 · Science Almanac ·

Срабатывание переходов модели означает генерацию S_i из B_i, используя h. Рассчитаем R для данного примера.

Вероятность $p(B_i \rightarrow B_i') = 1/13 \ \forall i \in [1, 13]$. Если происходит повреждение блока первого уровня, доля поврежденной части относительно всего размера файла $l_1 = 1$. Когда повреждается один из блоков второго уровня, теряются данные только его самого и его трех потомков, т.е. $l_2 = 4/13$. Повреждение блока третьего уровня приводит к потере $l_3 = 1/13$. По формуле полной вероятности:

$$R = 1 - (1/13)\cdot(l_1 + 3l_2 + 9l_3) \approx 0{,}8.$$

Это значительно больше значения, полученного в предыдущей модели, что иллюстрирует преимущество данного подхода. При увеличении числа уровней иерархии, которое возникает при увеличении размера исходного текста, соотношение между значениями R для предлагаемой и исходной моделей становится еще больше.

Таким образом, предлагаемая модель шифрования увеличивает среднее количество восстанавливаемых после повреждения данных.

Список используемых источников:

1. Димитриев А.П. Схема работы криптосистемы на основе задачи размещения и ее новая версия // Научный альманах. 2014. № 1 (1). С. 191-195.
2. Димитриев А.П. Алгоритм инициализации для криптосистемы // Наука и образование в жизни современного общества. Ч. 1. Тамбов: Консалтинговая компания Юком. 2015. С. 64 65.
3. Димитриев А.П. Алгоритм сдвига для криптосистемы // Наука и образование в жизни современного общества. Ч. 1. Тамбов: Консалтинговая компания Юком. 2015. С. 65-67.
4. Димитриев А.П. Алгоритм дешифрования на основе задачи размещения // Современные тенденции в образовании и науке. Ч. 2. Тамбов: Консалтинговая компания Юком, 2014. С. 40-41.
5. Димитриев А.П. Алгоритм шифрования на основе задачи размещения (тезисы РИНЦ) // Современные тенденции в образовании и науке. Ч. 2. Тамбов: Консалтинговая компания Юком. 2014. С. 41-43.
6. Димитриев А.П. Константы для алгоритма шифрования на основе задачи размещения // APRIORI. 2014. № 6. 7 с. URL: http://apriori-journal.ru/seria2/6-2014/Dimitriev1.pdf
7. Димитриев А.П. Чувашско-русский переводчик: программная реализация // Прикладная информатика. 2011. № 6 (36). С. 43-46.
8. Желтова Л.В., Желтов В.П. Моделирование систем и дискретные математические модели. Чебоксары: ЧГУ им. И.Н. Ульянова, 1995. 124 с.
9. Сизоненко А.Б., Меньших В.В. Использование сетей Петри для моделирования способов распараллеливания алгоритмов защиты информации в системах с массивно-параллельными сопроцессорами // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика. 2014. № 3. С. 65-74.
10. Dimitriev A. Modification of a cryptographic system using the formulation of the travelling salesman problem // Interactive Systems: Problems of Human // Computer Interaction. Ulyanovsk: USTU, 2015. P. 139-141.
11. Hussein A. Lafta. Message Encrypted Modelling Using Petri Nets // Journal of Babylon University/Pure and Applied Sciences. 2012. No. (5). Vol. (20). P. 1367-1378. URL: http://www.iasj.net/iasj?func=fulltext&aId=77263
12. Rodriguez H., Carvajal R., Ontiveros B., Soto I. and Carrasco R. Using Petri Net for Modeling and Analysis of a Encryption Scheme for Wireless Sensor Networks. DOI: 10.5772/7508. // Petri Nets Applications. 2010. 762 p.

Модель шифрования с учетом повреждения данных на основе сетей Петри

Model of encryption with account data damage based on Petri nets