DOI: 10.17117/na.2015.11.03.258

<http://ucom.ru/doc/na.2015.11.03.258.pdf>

Поступила (Received): 25.11.2015

Магомедова П.Х.

К вопросу о надежности простых методов кодирования

Magomedova P.H.

To the question about the reliability of simple encoding methods

Обсуждается современное состояние знаний о вычислительной сложности задач на предположении NP-полноты которых базируется криптостойкость алгоритмов шифрования открытым ключом. Рассмотрены программистские аспекты надежности алгоритма шифрования методом XOR. Для простого случая приведена реализация дешифрования

Ключевые слова: задача, криптостойкость, шифрование, злоумышленник, алгоритм

Discusses the current state of knowledge about computational complexity on the assumption NP-completeness underlying the cryptographic strength of the encryption algorithms public key. Discussed the programming aspects of the reliability of encryption algorithm XOR. For the simple case of an implementation of the decryption

Key words: task, cryptographic strength, encryption, attacker, algorithm

Магомедова Пирдас Хабибовна

Кандидат экономических наук, доцент
Дагестанский государственный университет
г. Махачкала, ул. М. Гаджиева, 43 А

Magomedova Pirdas Habibovna

Candidate of Economic Sciences, Associate Professor
Dagestan state university
Makhachkala, M. Gadzhieva st., 43 A

1. Введение. Доверие к стойкости криптосистем с открытым ключом базируется на предположении о труднорешаемости некоторых задач. Прежде всего – задачи о составном числе и задачи дискретного логарифмирования. Задача о составном числе приведена в [1, с. 373] в списке открытых задач, т.е. задач, NP-полнота которых предполагается, но не доказана; с тех пор о принципиальных продвижениях в выяснении вычислительной сложности этой задачи в литературе не сообщается. В то же время появились публикации о возможности эффективного решения задачи дискретного логарифмирования с применением квантовых вычислений. Так, в [2] сообщается, что с их использованием дискретный логарифм может быть «теоретически» вычислен за полиномиальное время.

Хотя приведенные в литературе сведения о полиномиальной разрешимости задачи дискретного логарифмирования не позволяют однозначно судить о практической реализуемости утверждения [2], подобные результаты мотивируют более пристальное внимание к различным аспектам известных и относительно простых способов шифрования.

2. Некоторые практические аспекты шифрования методом XOR. В нашем сообщении рассматриваются программистские аспекты метода шифрования,

известного как *шифрование с помощью случайных чисел* [3, с.181-183]. Предварительно напомним, что своеобразие (и привлекательность) шифрования методом хог заключается в том, что повторное шифрование этим методом с тем же ключом восстанавливает исходное сообщение (и применение метода хог для последовательных слов исходного и зашифрованного сообщений восстанавливает значение ключа).

Чтобы не отвлекаться на второстепенные для наших целей детали, рассмотрим задачу в следующем упрощенном варианте.

Пусть А и В договорились о шифровании сообщений методом хог с использованием ключа из файла "key.txt". Затем А создал в MS Excel 2016 файл "FileToEncode.xlsx" и зашифровал его методом хог с ключом из файла "key.txt". Результат шифрования А сохранил в файле "encoded.txt", который он отправил В по открытому каналу. Злоумышленник С перехватил файл "encoded.txt". При этом С известно, что исходный документ подготовлен в MS Excel 2016 и зашифрован методом хог, однако у него нет доступа к ключу. Спрашивается, в состоянии ли С расшифровать содержимое файла "encoded.txt"?

Ответ положителен. MS Excel 2016, как и многие другие редакторы, помещает в начало файла "FileToEncode.xlsx" служебную информацию (далее – «префикс Р»), не имеющую связи с содержанием документа. Злоумышленник С создаст, используя MS Excel 2016, произвольный документ и сохранит его, скажем, в файле "RandomDocument.xlsx". Префикс Q этого файла идентичен префиксу Р файла "FileToEncode.xlsx", результат Р1 шифрования которого ему известен из перехваченного файла "encoded.txt". Следовательно, применение операции хог к последовательным байтам префиксов Р1 и Q позволит восстановить искомый ключ в повторяющихся копиях. После чего С применит ключ к "encoded.txt" и восстановит исходный файл "FileToEncode.xlsx".

Приведенный ниже *рабочий* (хотя и упрощенный из соображений краткости) код на С# позволит выполнить имитацию действий А и С не только с целью проверить изложенную идею на практике, но и понаблюдать за интересными числовыми результатами, не все из которых отмечены в тексте сообщения. Функция Encrypt, обращения к которой составляют тело основной функции Main, приведена ниже: ее параметрами выступают имена файлов, содержащих исходный для кодирования методом хог документ, результат и ключ кодирования соответственно.

```
static void Main(string[] args)
{
    //Шифруем файл FileToEncode.xlsx ключом из файла key.txt
    Encrypt ("FileToEncode.xlsx", "encoded.txt", "key.txt");

    //Пытаемся угадать ключ, шифруя другим.xlsx-документом
    Encrypt ("encoded.txt", "guess.txt", "RandomDocument.xlsx");

    //Проверяем корректность шифрования, используя исходный ключ
    Encrypt ("encoded.txt", "decoded.xlsx", "key.txt");
}
```

```
static void Encrypt (string inputPath, string outputPath, string keyPath)
{
    byte[] input = File.ReadAllBytes(inputPath);
    byte[] key = File.ReadAllBytes(keyPath);

    byte[] result = new byte[input.Length];

    for (int i = 0; i < input.Length; ++i)
    {
        result[i] = (byte)(input[i] ^ key[i % key.Length]);
    }

    File.WriteAllBytes(outputPath, result);
}
```

Список используемых источников:

1. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982. 416 с.
2. Вялый М.Н. Квантовые компьютеры и квантовые вычисления.
URL: http://cs.mipt.ru/docs/comp/rus/develop/other/quantum_comp.
3. Новиков Н.А. Дискретная математика для программистов. СПб.: Питер, 2001. 304 с.

© 2015, Магомедова П.Х.

К вопросу о надежности простых методов
кодирования

© 2015, Magomedova P.H.

To the question about the reliability of simple
encoding methods