УДК 338.244.4

ЦИФРОВАЯ ЭКОНОМИКА: НАРУШЕНИЕ ЦЕЛОСТНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ ВЗЛОМОМ ПРОСТЕЙШЕГО ШИФРОВАНИЯ RSA КВАНТОВЫМ КОМПЬЮТЕРОМ НА ПЛАТФОРМЕ IBMQ

DIGITAL ECONOMY: VIOLATION OF INTEGRITY AND PROTECTION OF INFORMATION BY BROKEN SIMPLE RSA WEAKING BY A QUANTUM COMPUTER ON THE IBMQ PLATFORM

Р.М. АЛОЯН, В.В. ШУТЕНКО, Ю.С. АХМАДУЛИНА, Л.С. МИЗГИРЕВ
R.M. ALOYAN, V.V. SHUTENKO, YU.S. AHMADULINA, L.S. MIZGIREV

(Ивановский государственный политехнический университет)
(Ivanovo State Polytechnical University)
E-mail: schutenkovv@gmail.com

В статье рассматривается вариант обеспечения целостности и защиты экономической и финансовой информации путем применения алгоритма шифрования RSA, алгоритма Шора для факторизации целых чисел. Целью исследований является разработка программного обеспечения, базирующегося на алгоритме Шора, и его применения для взлома алгоритма шифрования RSA.

The article considers the option of ensuring the integrity and protection of economic and financial information by applying the RSA encryption algorithm, the Shore algorithm for the factorization of integers. The aim of the research is to develop software based on the Shore algorithm and its application for hacking the RSA encryption algorithm.

Ключевые слова: цифровая экономика, криптография, защита информации, шифрование RSA, алгоритм Шора.

Keywords: digital economy, cryptography, information protection, RSA encryption, Shor algorithm.

В цифровой экономике целостность и защита данных обеспечиваются за счет предотвращения возможности изменения информационного потока в момент выполнения над ним каких-либо финансовых и экономических операций с последующей передачей, хранением и обработкой данных. Фактически это гарантия сохранения данных в первоначально созданном виде.

Угроза нарушения целостности данных наиболее вероятна при попытке злоумышленника изменить номер аккаунта в банковской транзакции, либо при подделке комплекса документов.

Проверка целостности данных в криптографии обеспечивается хеш-функциями, преобразующими последовательность байт произвольного размера в последовательность байт фиксированного размера (число). При изменении информационного потока число, генерируемое хеш-функцией, тоже изменится [1].

Постановка задачи разложения числа на множители обеспечивается в случае подачи на входе составного числа N в двоичной записи и выдачи на выходе двух чисел p, q при условии, что $N = pq$.

Отсутствие полиномиального классического алгоритма решения является мотивацией решения подобной задачи, позволяющей взломать систему шифрования RSA, разрешив одну из основных современных алгоритмических проблем [2]. Лучший из известных классических алгоритмов имеет $O(2\sqrt[3]{n})$ в качестве оценки времени работы, при этом уже сегодня существует квантовый алгоритм, который решает эту задачу за $O(n^2)$.

Задача факторизации произведения двух простых чисел лежит в основе криптографического алгоритма RSA. В данном случае простая операция возведения в степень по модулю N выступит основой для шифрования. Задача факторизации, необходимая для расшифровки, требует вычисления функции Эйлера от числа N, зная разложение числа N на простые множители.

При шифровании RSA открытый и закрытый ключ формируется парой целых чисел. Закрытый ключ сохраняется в секрете, а открытый ключ передается второму участнику, либо публикуется [3].

Генерация ключей в RSA осуществляется следующим образом.

1. Отбираются простые числа p и q с условием $p \neq q$.

2. Вычисляется модуль $N = p * q$.

3. Вычисляется значение функции Эйлера от модуля N: $\phi(N) = (p - 1)(q - 1)$.

4. Выбирается открытая экспонента e, принадлежащая интервалу $1 < e < \phi(N)$ и являющаяся взаимно простой со значением функции $\phi(N)$.

5. Вычисляется секретная экспонента d, удовлетворяющая условию $de=1(\mathrm{mod}\ \phi(N))$ и являющаяся мультипликативно обратной к числу e по модулю $\phi(N)$.

Сформируем пару ключей: (e, N) – открытый ключ; (d, N) – закрытый ключ.

Указанным алгоритмом зашифруем сообщение "КОТ" путем генерирования пары ключей с последующим шифрованием открытым ключом:

1. Выберем простые числа (небольшие, чтобы упростить вычисления): p = 5 и q = 17.

2. Вычислим модуль $N = pq = 5 \cdot 17 = 85$.

3. Вычислим функцию Эйлера от модуля N: $\phi(N) = (p - 1)(q - 1) = 4 \cdot 16 = 64$.

4. Выберем открытую экспоненту e=11. Получим открытый ключ – (e, N) = (11, 85).

Пусть букве К соответствует цифра 12, О – 16, Т – 20. Следовательно:

$$C1 = 12^{11} \mathrm{mod} 85 = 23$$
$$C2 = 16^{11} \mathrm{mod} 85 = 16$$
$$C3 = 20^{11} \mathrm{mod} 85 = 75$$
$$C(\text{"КОТ"}) = 23, 16, 75$$

Закрытая экспонента не вычислялась, так как задача состояла только в зашифровке сообщения. Для расшифровывания следует вычислить закрытую экспоненту. Поскольку известен только открытый ключ, то невозможно расшифровать сообщение [4].

Данный вариант возможен только с небольшими числами и является тестовым. В реальных системах необходимы большие числа (рис. 1 – число RSA-1024).

```
RSA-1024 = 135066410865995223349603216278805969938881475605667027524485143851526510600
           4859533833940287150571909441798207282164471551373680419703964191743046496589
           8927425623934102086438320211037295872576235850964311056407350150818751067676
           5946292055636855294752135008528794163773285339061097505443349998111500569772
           7236890927563
```

Рис. 1

Максимально эффективными для вычислений такого уровня являются современные квантовые компьютеры IBM, позволяющие проверить работу разрабатываемых экспериментальных программ на реальной системе по схеме удаленного доступа через облачные сферы, запущенные корпорацией IBM.

Основной целью исследования является проектирование математической модели алгоритма разложения целого числа на множители. Для достижения цели реализован алгоритм Шора, факторизующий целые числа, путем сведения задачи факторизации к задаче поиска периода функции.

Выполним поиск периода функции $2^x \mathrm{mod}\ 85$, выполненный в MSExcel, равный 8 (табл. 1 – нахождение периода функции $2^x \mathrm{mod}\ 85$).

Таблица 1

x	2^x	2^xMod 85
1	2	3
1	2	2
2	4	4
3	8	8
4	16	16
5	32	32
6	64	64
7	128	43
8	256	1
9	512	2
10	1024	4
11	2048	8
12	4096	16
13	8192	32
14	16384	64
15	32768	43
16	65536	1

При известном периоде функции факторизация осуществляется на классическом компьютере при помощи алгоритма Евклида за полиномиальное время. Квантовая часть алгоритма факторизации как раз занимается поиском периода функции. А классическая часть алгоритма сначала специальным образом готовит эту функцию, а потом проверяет найденный квантовой частью период на достаточность для решения задачи [5].

Найдем множители N = 85 с использованием функции "=НОД (a (T / 2) ± 1; N)" в MSExcel (табл. 2).

Таблица 2

N =	85
a =	2

Период, T		M1	M2	Проверка
10	2	1	1	1
100	4	5	1	5
110	6	1	1	1
1000	8	17	5	85
1010	10	1	1	1
1100	12	5	1	5
1110	14	1	1	1
10000	16	1	85	85

При условии точного нахождения периода задача считается решенной. В противном случае квантовая часть алгоритма прогоняется повторно, а так как проверка правильности решения для задачи факторизации достаточно несложная (произведение двух чисел с последующим сравнением с третьим), то допускается не учитывать данный блок алгоритма с точки зрения подсчета сложности.

Исполнение алгоритма:

1. Выбор случайного числа a < N.
2. Расчет НОД (a, N) при помощи алгоритма Евклида.
3. В случае, если НОД (a, N) ≠ 1, то существует нетривиальный делитель числа M, так что алгоритм завершается.
4. В противном случае необходимо использовать квантовую подпрограмму поиска периода функции $f(x) = a^x \bmod N$.
5. Если найденный период T нечетный, то вернуться на шаг 1 и выбрать другое число a.
6. Если $a^{(T/2)} \equiv M - 1 \pmod N$, то вернуться на шаг 1 и выбрать другое число a.
7. Определить два значения НОД $(a^{(T/2)} \pm 1, N)$, являющиеся нетривиальными делителями числа N.

Приведем описание квантовой части алгоритма (рис. 2).

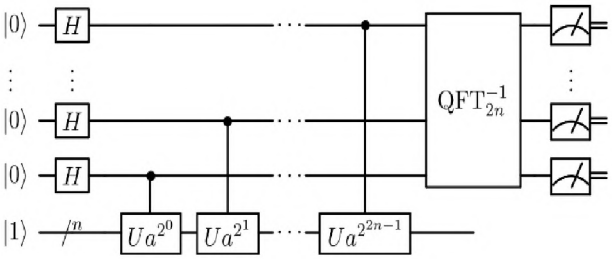

Рис. 2

Вычислительная схема формируется двумя квантовыми регистрами X и Y. Первоначально каждый из них состоит из совокупности кубитов в нулевом булевом состоянии |0>.

В регистре X размещаются аргументы x функции f (x), а в регистре Y размещаются значения функции f (x) с периодом T, подлежащим вычислению.

Реализация квантового вычисления осуществляется в четыре шага.

На первом шаге с помощью операции Адамара первоначальное состояние |0> регистра X переводится в равновероятную суперпозицию всех булевых состояний N. Второй регистр Y остается в состоянии |0>.

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x,0\rangle$$

На втором шаге с помощью унитарного преобразования U_f переводится |x, 0> в |x, f (x)>.

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x,0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x,a^x \bmod N\rangle$$

Над состоянием первого регистра производится квантовое преобразование Фурье.

Выполняется измерение регистра X.

На оставшейся части алгоритма используется классический компьютер.

На рис. 3 представлены фрагменты разработанного кода программы, вычисляющей множители и расшифровывающей сообщение. В результате работы на экран выводятся рассчитанные множители и расшифрованное сообщение.

В этом примере функции decrypt() были переданы следующие аргументы:

Открытый ключ: (11, 85);

Сообщение: "1л?:,x2"

```
def Oracle():
    qc.cx(qr[2], qr[6])
    qc.cx(qr[3], qr[7])


def findPQ(a, N):

    qc.h(qr[0])
    qc.h(qr[1])
    qc.h(qr[2])
    qc.h(qr[3])

    Oracle()

    qc.h(qr[0])
    qc.cu1(pi/2, qr[0], qr[1])
    qc.h(qr[1])
    qc.cu1(pi/4, qr[0], qr[2])
    qc.cu1(pi/2, qr[1], qr[2])
    qc.h(qr[2])
    qc.cu1(pi/8, qr[0], qr[3])
    qc.cu1(pi/4, qr[1], qr[3])
    qc.cu1(pi/2, qr[2], qr[3])
    qc.h(qr[3])

    qc.measure(qr[0], cr[0])
    qc.measure(qr[1], cr[1])
    qc.measure(qr[2], cr[2])
    qc.measure(qr[3], cr[3])
```

Квантовая часть программы

```
result = qp.execute(['Shor'])
res = result.get_counts('Shor')

mult_list = []
for k in res.keys():
    p = int(k, 2)
    print(p)
    if p % 2 == 0:
        k1 = a**(p/2) - 1
        k2 = a**(p/2) + 1
        mult_list.append((gcd(k1, N), gcd(k2, N)))
    else:
        print("Period is odd, skipping")

print("mult_list: {}".format(mult_list))
return mult_list
```

Классическая часть программы

```
...
mult_list: [(5.0, 17.0), (85, 1.0), (1.0, 5.0), (1.0, 5.0)]
The message is: Экзамен
N = N * 1, skipping
N = N * 1, skipping
N = N * 1, skipping
[Finished in 43.5s]
```

Результат работы программы

Рис. 3

ВЫВОДЫ

Проведенные исследования и выполненные расчеты свидетельствуют, что алгоритм Шора представляет прямую угрозу для системы шифрования RSA. В настоящее время количество кубитов недостаточно для взлома реальных систем, но с развитием квантовых технологий ситуация вполне может измениться.

ЛИТЕРАТУРА

1. *Алоян Р.М., Филимонова Н.М., Петрухин А.Б., Капустина Н.В.* Управление логистическими факторами риска в процессе организации производства // Изв. вузов. Технология текстильной промышленности. – 2017, № 4. С. 94...97.

2. *Алоян Р.М., Шутенко В.В.* Разработка информационного сопровождения оценки качества государственных образовательных услуг, предоставляемых вузом // Изв. вузов. Технология текстильной промышленности. – 2016, № 5. С. 5...10.

3. *Алоян Р.М., Татиевский П.Б., Федосеев В.Н.* Практика использования информационно-аналитических технологий (ИАТ) для принятия управленческих решений в режиме "On-Line" // Интеграл – М.: ООО НПЦ "Энергоинвест", 2013, № 1-2. С. 56...58.

4. *Андреева О.Р., Зайцева И.А., Шутенко В.В.* Выбор приоритетных направлений инновационного развития социальной сферы на основе использования метода анализа иерархий // Современные наукоемкие технологии. Региональное приложение. – Иваново: ИГХТУ, 2013, № 4 (36). С. 16...23.

5. *Андреева О.Р., Зайцева И.А., Шутенко В.В.* Оценка качества подачи тепловой энергии на основе метода анализа иерархий в программной системе "Mpriority" // Современные наукоемкие технологии. Региональное приложение. – Иваново: ИГХТУ, 2014, № 1. С. 30...37.

REFERENCES

1. Alojan R.M., Filimonova N.M., Petruhin A.B., Kapustina N.V. Upravlenie logisticheskimi faktorami riska v processe organizacii proizvodstva // Izv. vuzov. Tehnologija tekstil'noj promyshlennosti. – 2017, № 4. S.94...97.

2. Alojan R.M., Shutenko V.V. Razrabotka informacionnogo soprovozhdenija ocenki kachestva gosudarstvennyh obrazovatel'nyh uslug, predostavljaemyh vuzom // Izv. vuzov. Tehnologija tekstil'noj promyshlennosti. – 2016, № 5. S. 5...10.

3. Alojan R.M., Tatievskij P.B., Fedoseev V.N. Praktika ispol'zovanija informacionno-analiticheskih tehnologij (IAT) dlja prinjatija upravlencheskih reshenij v rezhime "On-Line" // Integral – M.: OOO NPC "Jenergoinvest", 2013, № 1-2. S. 56...58.

4. Andreeva O.R., Zajceva I.A., Shutenko V.V. Vybor prioritetnyh napravlenij innovacionnogo razvitija social'noj sfery na osnove ispol'zovanija metoda analiza ierarhij // Sovremennye naukoemkie tehnologii. Regional'noe prilozhenie. – Ivanovo: IGHTU, 2013, № 4 (36). S. 16...23.

5. Andreeva O.R., Zajceva I.A., Shutenko V.V. Ocenka kachestva podachi teplovoj jenergii na osnove metoda analiza ierarhij v programmnoj sisteme "Mpriority" // Sovremennye naukoemkie tehnologii. Regional'noe prilozhenie. – Ivanovo: IGHTU, 2014, № 1. S.30...37.

Рекомендована кафедрой информационных систем и технологий. Поступила 25.10.17.