QUANTITATIVE CHARACTERISTICS THE SAFE OPERATION OF TELECOMMUNICATION SYSTEMS AND COMPLEX

Falin M.N.

In this paper proposed for the quantitative characteristics of the safe operation of telecommunication systems and complex, according to which the decision can be made about the safety of operation.

Keywords: *telecommunication systems and complex, the operation safety, characteristics of the safe operation.*

Фалин Михаил Николаевич, аспирант Московского государственного технического университета радиотехники, электроники и автоматики. Тел. 8-903-234-76-35. E-mail: mikelbym@gmail.com

УДК 621.391

МОДЕЛИРОВАНИЕ ПАРАЛЛЕЛЬНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ ИНФОРМАЦИИ

Кочеров Ю.Н., Червяков Н.И.

В статье рассмотрены вопросы моделирования параллельных алгоритмов шифрования информации с использованием системы остаточных классов и приведены примеры алгоритмов шифрования RSA, восстановления чисел и моделирования параллельных алгоритмов шифрования в среде Matlab Simulink. Целью статьи является увеличение криптостойкости путем параллельного выполнения различных криптографических алгоритмов или параллельного использования одного алгоритма, но с разными ключами.

Ключевые слова: параллельные алгоритмы, шифрование информации, алгоритм RSA.

Введение

В современном информационном мире информация становится более ценным ресурсом, чем материальные и энергетические ресурсы. Владение точной и достоверной информацией дает преимущество той стороне, которая ею владеет, – особенно если эта информация касается конкурентов. Обладание такой информацией позволяет ее владельцу получить выигрыш: материальный, политический или военный. В современном мире необходимо защищать огромное количество информации, хранимой в базах данных и предаваемой по информационным сетям.

Постановка задачи и моделирование алгоритма шифрования RSA в среде Matlab Simulink

В настоящее время наиболее важную роль играет защита электронной информации от несанкционированного доступа. Для защиты информации используют различные криптографические алгоритмы, такие как RSA, DSA, ГОСТ 28147-89, Шифросистема Эль-Гамаля и многие другие. Надежность криптографических алгоритмов во многом зависит от сложности реализации и от длины ключа шифрования данных. При моделировании в системе Matlab Simulink был использован алгоритм шифрования RSA – криптографический алгоритм с открытым ключом (RSA стал первым алгоритмом такого типа, пригодным и для шифрования и цифровой подписи, сегодня он используется в большом числе криптографических приложений [1]).

Возьмем два больших простых числа p и q. Определим n как результат умножения p на $q: n = p \cdot q$. Выберем случайное число, которое назовем d: это число должно быть взаимно простым (не иметь ни одного общего делителя, кроме единицы, с результатом умножения $(p-1)\cdot(q-1)$).

Определим также число e, для которого является истинным следующее соотношение $(e \cdot d) \bmod (p-1)\cdot(q-1) = 1$. Назовем открытым ключом числа e и n, а секретным – d и n. Задача состоит в том, чтобы зашифровать текст, рассматриваемый как последовательность чисел $M(i)$, по формуле $C(i) = (M(i)^e) \bmod n$. Чтобы расшифровать данные, необходимо выполнить вычисления $M(i) = (C(i)^d) \bmod n$. В результате будет получено множество чисел $M(i)$, которые представляют собой исходный текст.

Следующий пример наглядно демонстрирует алгоритм шифрования RSA.

Зашифруем и расшифруем сообщение «САВ» по алгоритму RSA. Для простоты возьмем небольшие числа, что сократит расчеты.

Выберем $p = 3$ и $q = 11$.

Определим $n = 3 \cdot 11 = 33$.

Найдем $(p-1)\cdot(q-1) = 20$. Пусть d будет равно, например, 3, то есть $d = 3$.

Выберем число e по формуле: $(e \cdot 3) \bmod 20 = 1$. В нашем случае e будет равно, 7: $(e = 7)$. Представим шифруемое сообщение как последовательность чисел в диапазоне от 0 до 32. Буква $A = 13$, $B = 17$, $C = 19$. Теперь зашифруем сообщение, используя открытый ключ {7,33}:

$$C1 = (13^7) \bmod 33 = 62748517 \bmod 33 = 7;$$

$$C2 = (17^7) \bmod 33 = 410338673 \bmod 33 = 8;$$

$$C3 = (19^7) \bmod 33 = 893871739 \bmod 33 = 13.$$

Теперь расшифруем данные, используя закрытый ключ {3,33}:

$$M1 = (7^3) \bmod 33 = 343 \bmod 33 = 13 \ (\text{A});$$

$$M2 = (8^3) \bmod 33 = 512 \bmod 33 = 17 \ (\text{B});$$

$$M3 = (13^3) \bmod 33 = 2197 \bmod 33 = 19 \ (\text{C}).$$

Данные расшифрованы [2].

Примеры моделирования алгоритмов RSA в Matlab Simulink представлены на рис. 1-2.

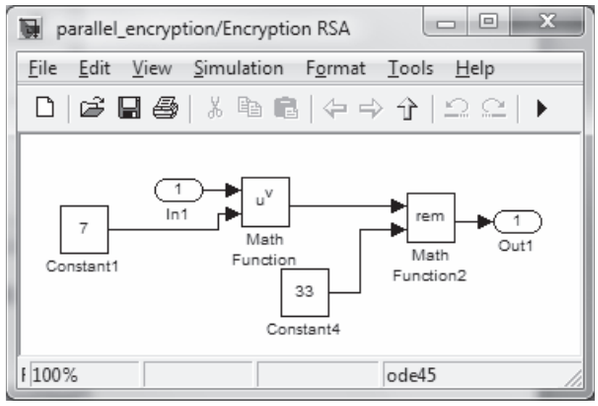

Рис. 1. Пример моделирования шифрования алгоритма RSA

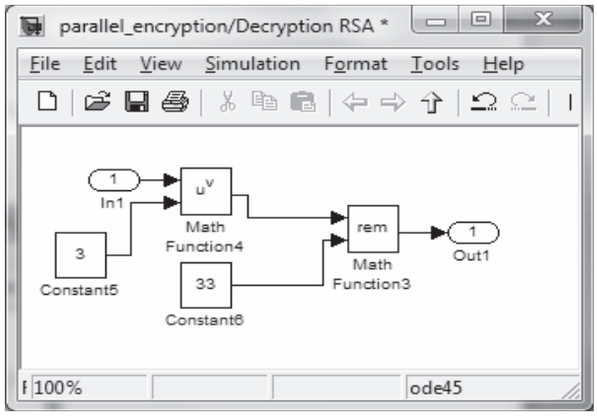

Рис. 1. Пример моделирования дешифрования алгоритма RSA

Использование СОК для разделения информации на модули и восстановления ее

Для параллельного использования нескольких алгоритмов шифрования необходимо представить входную информацию в системе остаточных классов (СОК). Система остаточных классов дает нестандартное представление для чисел и используется для повышения эффективности операций над кодами в остатках. Дело в том, что в данной системе числа представляются своими остатками от деления на выбранную систему оснований и все рациональные операции могут выполняться параллельно над цифрами каждого разряда в отдельности. После представления информации в СОК она шифруется алгоритмами RSA (пример работы алгоритма см. выше).

Для передачи данных после шифрования по одному каналу и разделения входного сигнала на отдельные составляющие используются, соответственно, блок мультиплексора и блок демультиплексора. Основным параметром мультиплексора является число входов, демультиплексора – число выходов [3-4]. Примеры использования мультиплексора и демультиплексора представлены на рис. 3.

На входы мультиплексора подаются два сигнала разной частоты, представленные двумя графиками: мультиплексор коммутирует их на один выход, скоммутированные сигналы в один канал представлены графиком. Далее демультиплексор коммутирует сигнал со входного канала на два выходных сигнала, также представленные графиками.

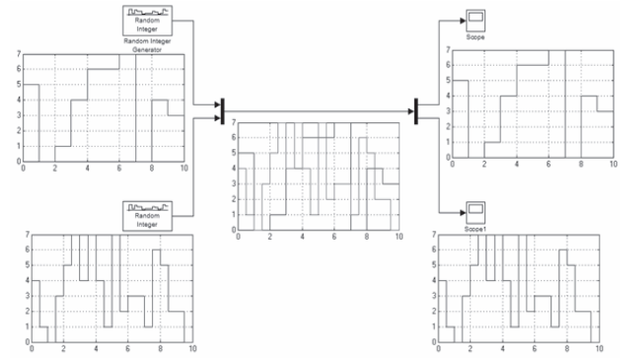

Рис. 3. Пример использования мультиплексора и демультиплексора

После дешифровки данных, чтобы получить исходную информацию, использовалось преобразование СОК → ПСС, где ПСС – позиционная система счисления. При преобразовании СОК → ПСС использовался метод ортогональ-

ных базисов. Преобразование кода числа А, заданного в СОК, в ПСС можно осуществить в соответствии с выражением, записанным в виде $A = (\sum_{i=1}^{n} \alpha_i \mathrm{B}_i) \bmod P_n$, где α_i – значение разрядов числа A по модулю p_i, B_i – ортогональные базисы системы, $P_n = p_1 \cdot p_2 \cdot ... \cdot p_n$ [5].

Следующий пример демонстрирует преобразование из остаточных классов в позиционный код. Возьмем число $A = 103$. Дана система оснований $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, объем диапазона равен $P = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$. Представим число A в системе остаточных классов по системе оснований p, $A = (1, 1, 3, 5, 4)$.

Для расчета ортогональных базисов найдем величины P_i:

$$P_1 = \frac{P}{p_1} = \frac{2310}{2} = 1155;\ P_2 = \frac{P}{p_2} = \frac{2310}{3} = 770;$$

$$P_3 = \frac{P}{p_3} = \frac{2310}{5} = 462;\ P_4 = \frac{P}{p_4} = \frac{2310}{7} = 330;$$

$$P_5 = \frac{P}{p_5} = \frac{2310}{11} = 210.$$

Ищем веса базисов: $1155 \cdot m_1 = 1(\mathrm{mod}\,2)$, методом подбора находим $m_1 = 1$; $770 \cdot m_2 = 1(\mathrm{mod}3)$, методом подбора находим $m_2 \equiv 2$; $462 \cdot m_3 = 1(\mathrm{mod}5)$, методом подбора находим $m_3 \equiv 3$; $330 \cdot m_4 = 1(\mathrm{mod}7)$, методом подбора находим $m_4 \equiv 1$; $210 \cdot m_5 = 1(\mathrm{mod}11)$, методом подбора находим $m_5 \equiv 1$.

Далее вычислим сами базисы:

$$B_1 = m_1 \cdot P_1 = 1 \cdot 1155 = 1155;$$

$$B_2 = m_2 \cdot P_2 = 2 \cdot 770 = 1540;$$

$$B_3 = m_3 \cdot P_3 = 3 \cdot 462 = 1386;$$

$$B_4 = m_4 \cdot P_4 = 1 \cdot 330 = 330;$$

$$B_5 = m_5 \cdot P_5 = 1 \cdot 210 = 210.$$

Далее, имея значения базисов, вычислим значения числа A:

$$A = |1 \cdot 1155 + 1 \cdot 1540 + 3 \cdot 1386 + 5 \cdot 330 + 4 \cdot 210|_{2310} = |9343|_{2310} = 103.$$

Из расчета видно, что переведенное из СОК число идентично исходному числу.

Моделирование параллельных алгоритмов шифрования в среде Mathlab simulink

На рис. 4 приведен пример модели параллельных алгоритмов шифрования при моделировании в среде Matlab Simulink.

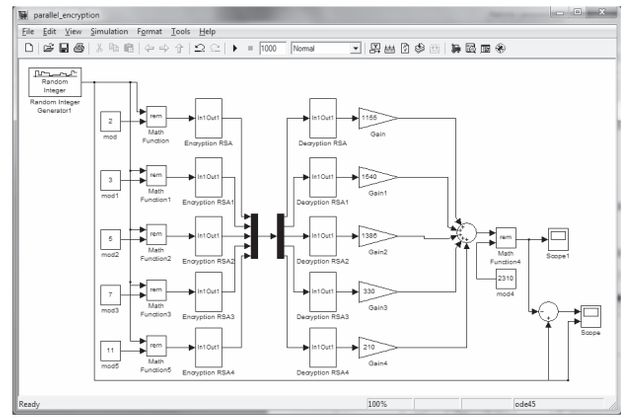

Рис. 4. Модель параллельных алгоритмов шифрования

При моделировании в среде Matlab исходная информация разбита на пять модулей $p = (2,3,5,7,11)$. Каждый модуль зашифрован алгоритмом RSA.

Алгоритм, представленный на рис. 4, можно условно разбить на пять частей. В первой части входной сигнал представляется в СОК по системе оснований $p = (2,3,5,7,11)$. Во второй части информация, представленная в СОК, параллельно шифруется алгоритмами RSA. В третьей части сигнал после шифрования для передачи данных по одному каналу коммутируется мультиплексором в один канал, и для дешифровки данных скомутированный сигнал разделяется демультиплексором на пять каналов. В четвертой части сигнал дешифруется. В пятой части сигнал восстанавливается из СОК. Проверка на правильность выполнения путем вычитания входной и выходной информации.

Рассмотрим пример использования параллельных алгоритмов шифрования.

Зашифруем сообщение «ABC», используя параллельные алгоритмы шифрования. Представим сообщения как последовательность чисел $A = 13, B = 17, C = 19$. Представим сообщение в СОК по системе оснований

$$p = (2,3,5,7,11);\quad A = (1,1,3,6,2);$$

$$B = (1,2,2,3,6);\quad C = (1,1,4,5,8).$$

Зашифруем сообщение, представленное в СОК, используя для каждого модуля свой ключ. Для числа по модулю 2 мы будем использовать открытый ключ {7,33} и закрытый {3,33}, для модуля числа 3 открытый ключ {11,91} и закрытый {59,91}, для модуля числа 5 открытый ключ {17,65} и закрытый {113,65}, для модуля числа 7 открытый ключ {5,34} и закрытый {13,34} и для модуля числа 11 открытый ключ {29,437}

и закрытый {41,437} – пример расчета ключей см. выше. При моделировании в среде Matlab Simulink, так как значения переменных при возведении в степень выходили за область определения, во всех алгоритмах шифрования использовались одинаковые ключи шифрования: открытый ключ {7,33} и закрытый {3,33}.

Теперь зашифруем сообщения, используя данные ключи:

$$C_A1 = (1^7) \bmod 33 = 1;\ C_B1 = (1^7) \bmod 33 = 1;$$
$$C_C1 = (1^7) \bmod 33 = 1;\ C_A2 = (1^{11}) \bmod 91 = 1;$$
$$C_B2 = (2^{11}) \bmod 91 = 46;\ C_C2 = (1^{11}) \bmod 91 = 1;$$
$$C_A3 = (3^{17}) \bmod 65 = 48;\ C_B3 = (2^{17}) \bmod 65 = 32;$$
$$C_C3 = (4^{17}) \bmod 65 = 49;\ C_A4 = (6^5) \bmod 34 = 24;$$
$$C_B4 = (3^5) \bmod 34 = 5;\ C_C4 = (5^5) \bmod 34 = 31;$$
$$C_A5 = (2^{29}) \bmod 437 = 243;\ C_B5 = (6^{29}) \bmod 437 = 302;$$
$$C_C5 = (8^{29}) \bmod 437 = 12.$$

Итак, зашифрованное сообщение примет вид

$$C_A = (1,1,48,24,243);\ C_B = (1,46,32,5,302);$$
$$C_C = (1,1,49,31,12).$$

Далее расшифруем сообщение:

$$M_A1 = (1^3) \bmod 33 = 1;\ M_B1 = (1^3) \bmod 33 = 1;$$
$$M_C1 = (1^3) \bmod 33 = 1;\ M_A2 = (1^{59}) \bmod 91 = 1;$$
$$M_B2 = (46^{59}) \bmod 91 = 2;\ M_C2 = (1^{59}) \bmod 91 = 1;$$
$$M_A3 = (48^{113}) \bmod 65 = 3;\ M_B3 = (32^{113}) \bmod 65 = 2;$$
$$M_C3 = (49^{113}) \bmod 35 = 4;\ M_A4 = (24^{13}) \bmod 34 = 6;$$
$$M_B4 = (5^{13}) \bmod 34 = 3;\ M_C4 = (31^{13}) \bmod 34 = 5;$$
$$M_A5 = (243^{41}) \bmod 437 = 2;\ M_B5 = (302^{41}) \bmod 437 = 6;$$
$$M_C5 = (12^{41}) \bmod 437 = 8.$$

Расшифрованное сообщение примет вид

$$M_A = (1,1,3,6,2) = A;\ M_B = (1,2,2,3,6) = B;$$
$$M_C = (1,1,4,5,8) = C.$$

Таким образом, после расшифровки мы получили исходное сообщение.

Восстановим расшифрованное сообщение преобразованием СОК → ПСС (пример преобразования СОК → ПСС см. выше).

$$A = \left|1 \cdot 1155 + 1 \cdot 1540 + 3 \cdot 1386 + 6 \cdot 330 + 2 \cdot 210\right|_{2310} =$$
$$= \left|9253\right|_{2310} = 13.$$
$$B = \left|2 \cdot 1155 + 2 \cdot 1540 + 2 \cdot 1386 + 3 \cdot 330 + 6 \cdot 210\right|_{2310} =$$
$$= \left|9257\right|_{2310} = 17.$$
$$C = \left|1 \cdot 1155 + 1 \cdot 1540 + 4 \cdot 1386 + 5 \cdot 330 + 8 \cdot 210\right|_{2310} =$$
$$= \left|11569\right|_{2310} = 19.$$

Сравним данные, зашифрованные простым алгоритмом RSA, и данные, полученные при использовании параллельных алгоритмов шифрования. В примере для шифрования использовались одинаковые сообщения «ABC», при использовании алгоритма RSA мы получили следующее сообщение $C1 = 7, C2 = 8, C3 = 13$. При использовании параллельных алгоритмов шифрования мы получили сообщение

$$C_A = (1,1,48,24,243);\ C_B = (1,46,32,5,302);$$
$$C_C = (1,1,49,31,12).$$

Выводы

Данные, зашифрованные при помощи параллельных алгоритмов шифрования, имеют достаточно сложную структуру. Получение исходной информации из зашифрованной усложняется необходимостью взломать каждый алгоритм отдельно. Исследования выполнены при поддержке гранта РФФИ 12-07-00482-а.

Литература

1. http://www.anti-malware.ru/rsa
2. http://www.e-nigma.ru/stat/rsa/
3. http://subscribe.ru/archive/tech.digitchip01/200212 /19092116.html
4. Черных И.В. Simulink: инструмент моделирования динамических систем // http://www.knigka.info/2008/10/03/simulink-instrument-modelirovanija.html
5. Модулярные параллельные вычислительные структуры нейропроцессорных систем. Под. ред. Н.И. Червякова. М.: Физматлит, 2003. – 288 с.
5. http://www.cybersecurity.ru/crypto/85133.html

MODELING OF PARALLEALGORITMS FOR ENCRYPTION INFORMATION

Kocherov Y.N., Chervyakov N.I.

This article discusses the questions of modeling of parallel encryption algorithms of the information with usage of system of residual classes. It also presents the examples of RSA encryption algorithms, restoration of numbers and modeling of parallel algorithms of enciphering in the environment of Matlab Simulink. The purpose of the given article is magnifications cryptographic strength by parallel performance of various cryptographic algorithms or parallel use of one algorithm, but with different keys.

Keywords: *parallel algorithms, information enciphering, algorithm RSA.*

Червяков Николай Иванович, Заслуженный деятель науки и техники РФ, доктор технических наук, профессор Кафедры «Прикладная математика и информатика» Ставропольского государственного университета. Тел. (8-865) 275-35-64. E-mail: kfmf-primath@stavsu.ru

Кочеров Юрий Николаевич, аспирант Кафедры «Информационные системы, электропривод и автоматика» Невинномысского технологического института – филиала Северо-Кавказского государственного технического университета. Тел. (8-865) 543-55-08; 8-918-866-91-93. E-mail: kocherov_yra@mail.ru

УПРАВЛЕНИЕ И ПОДГОТОВКА КАДРОВ ДЛЯ ОТРАСЛИ ИНФОКОММУНИКАЦИЙ

УДК 007.51

ОРГАНИЗАЦИЯ ПЛАНИРОВАНИЯ И УПРАВЛЕНИЯ ХОЗЯЙСТВЕННО-ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТЬЮ ПРЕДПРИЯТИЯ С ИСПОЛЬЗОВАНИЕМ КОНЦЕПЦИИ СБАЛАНСИРОВАННОЙ СИСТЕМЫ ПОКАЗАТЕЛЕЙ

Дилигенский Н.В., Матвеева Е.А.

В статье рассматриваются проблемы планирования и управления хозяйственно-экономической деятельностью предприятий. Для решения проблем организации деятельности предлагается использовать концепцию сбалансированной системы показателей (ССП). На основе концепции ССП разработана структура модели управления хозяйственно-экономической деятельностью.

Ключевые слова: стратегическое планирование, оперативное планирование, организация деятельности, сбалансирования система показателей.

Введение

Перспективы развития производственных систем в современных условиях интеграции в мировую экономику при быстром изменении спроса обусловлены необходимостью выпуска конкурентоспособной продукции как по техническим, так и по стоимостным характеристикам. Наиболее эффективные производственные системы в условиях нестабильной рыночной конъюнктуры должны быть адаптивными к постоянным переменам в среде функционирования, что приводит к многообразию номенклатуры производимой продукции.

Стремление к удовлетворению запросов рынка привело к резкому росту численности предприятий с мелкосерийным типом производства и многономенклатурной продукцией хозяйствующих субъектов, управление которыми имеет существенную специфику и сложность.

Эффективность работы всего предприятия в целом определяющим образом зависит от процессов планирования и управления основным производством на всех стадиях и уровнях, от получения заказа до отгрузки продукции, во взаимосвязи с ресурсным, материальным, финансовым и кадровым обеспечением. Совершенствование планирования и управления основным производством требует индивидуального подхода к каждому объекту, диктуемого спецификой выпускаемой продукции, типом производства, техническим оснащением, уровнем организации труда и производства и квалификацией сотрудников. Правильно спроектированная производственная система обладает сбалансированным комплексом результатов деятельности и факторов их достижения.

Постановка задачи

Специфические особенности предприятий с мелкосерийным типом производства: выпуск продукции с разнообразной номенклатурой изготовляемых деталей и узлов; многообразие технологических процессов обработки; большое количество и малая повторяемость выполняемых операций обработки по плановому периоду; высокая степень взаимосвязей и взаимозависимостей между различными подразделениями на всех стадиях производства - порождают многофакторные проблемы управления при решении задач планирования, организации и регулирования на межцеховом и внутрицеховом уровнях сбора и переработки больших объемов информации в сжатые сроки с высокими требованиями к достоверности получаемых результатов. Для устранения проблем