Список використаних джерел:

1. Малков С.Ю. Математическое моделирование исторической динамики: подходы и модели. М.: РГСУ. 2004. 188 с.

2. Caltagirone S., Pendergast A., Betz C. The diamond model of intrusion analysis. DTIC Document, Tech. Rep. 2013. 21 P.

3. Hutchins E. M., Cloppert M. J., and Amin R. M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research. 2011. Vol. 1. P. 80-82.

4. Schneier B. Attack trees. Dr. Dobbs journal. 1999. Vol.24. No. 12. P. 21-29.

Ключові слова: інформаційна безпека, кібербезпека, модель, динамічні системи, нелінійність, методи, кібератаки.

Ключевые слова: информационная безопасность, кибербезопасность, модель, динамичные системы, нелинейность, методы, кибератаки.

Keywords: information security, cybersecurity, model, dynamic systems, nonlinearity, methods, cyber attacks.

Орлов Сергей Вячеславович

Національний університет «Одеська юридична академія»,
старший преподаватель кафедры информационных технологий

ПРОБЛЕМА УДЛИНЕНИЯ ТЕКСТА В СИСТЕМАХ ШИФРОВАНИЯ НА ОСНОВЕ КОНЕЧНОГО АВТОМАТА И АВТОМАТА С МАГАЗИННОЙ ПАМЯТЬЮ

Удлинение текстов при шифровании является одной из важных характеристик любой системы шифрования. Шифрование контента все большего объема характерно для современных технологий. Это не только обмен видео, в том числе потокового, но и реализация блок чейн технологий и многое другое. В связи с этим все более важной характеристикой систем шифрования становиться ее способность не очень сильно увеличивать объем информации при шифровании.

Рассмотрим систему шифрования построенной на основе контекстно свободной и регулярной грамматик предложен-

ную в работе [1]. В ней предлагается использовать для шифрования каждой из букв регулярную грамматику. Известно, что каждой регулярной грамматике можно поставить в соответствие конечный автомат [2]. Достаточно просты правила для преобразования регулярных грамматик в конечные автоматы. Эффективная реализация подобной системы шифрования предполагает использование именно конечных автоматов при кодировании символов. Например, детерминированный конечный автомат для кодирования буквы «А», в виде таблицы переходов, может выглядеть следующим образом:

Табл. 1

Конечный автомат для кодирования «А»

$КА_1$-автомат кодирования буквы «А»							
«А”	a	b	c	d	e	f	g
S_0	S_3	S_0		S_2		S_3	
S_1			S_5		S_2		«Допустить»
S_2		S_3			S_1	S_5	
S_3	S_0	S_4					S_0
S_4			S_5	S_2	S_3		S_1
S_5			S_2	S_0			

Этими автоматами будут генерироваться регулярные языки L(КАi). При таком алгоритме шифрования одна буква в исходном тексте будет зашифрована строкой из нескольких символов. В данном случае из множества {a, b, c, d, e, f, g}. Для приведенного автомата удлинение зашифрованного текста может быть и 10 раз. Так как в автомате есть возвраты в предыдущие состояния. Известно, что проблема кодирования, декодирования регулярных языков Р-полная. Взлом подобного шифра тоже является Р-полной задачей. Крипто стойкость такой системы шифрования не высокая. Поэтому в работах [1; 3] предлагается проводить отсеивание части полученных кодирующих строк при помощи контекстно свободной грамматики.

На самом деле удобнее, на практике, воспользоваться автоматом с магазинной памятью. Так как известно, что каждой контекстно свободной грамматике можно поставить в соответствии автомат с магазинной памятью. Полученный, таким образом, язык позволяет добиться устойчивости к взлому на уровне NP-полных задач [4].

Для контролируемого и гарантированного удлинения текста менее чем в 2 раза предлагается кодировать символы алфавита в двоичной системе при помощи таблиц переходов ограниченного размера. При этом будем строить матрицу переходов таким образом, чтобы в ней не было возвратов в предыдущие состояния. Например, матрица для кодирования «А» может выглядеть в этой системе следующим образом **КА1*** – конечный автомат кодирования буквы **«А»**:

Табл. 2.

Конечный автомат для двоичного кодирования «А», с контролируемым удлинением

«А»	0	1
S_1	S_2	
S_2	S_5	S_3
S_3	S_4	S_5
S_4	S_5	
S_5		S_6
S_6		Допустить

В соответствии с этой таблицей переходов символ «А» может быть закодирован любой бинарной строкой, словом из языка L(**КА1***), который может быть описан множеством {0011,01111,010011}. Предложим кодировать остальные буквы алфавита подобными автоматами, придерживаясь следующих правил:

1. Количество строк состояний в КА возьмем минимум – 6.

2. Функции выхода, «Допустить» может быть расположены начиная с 4 строки состояния.

3. Функции переходы можно не менять для каждого нового символа слишком часто (для автоматизации генерации таблиц перехода).

4. В таблице переходов будут отсутствовать переходы на предыдущие состояния.

5. Пустые клетки конечного автомата означают выход – «Отвергнуть».

6. Сгенерированные конечными автоматами языки L(КАi) не должны пересекаться, содержать одинаковые слова для кодировки разных символов.

Например, букву «Б» можно закодировать конечным автоматом следующего вида:

Табл. 3.

Конечный автомат для двоичного кодирования «Б», с контролируемым удлинением

«Б»	0	1
S_1	S_2	
S_2	S_5	S_3
S_3	S_4	S_5
S_4	S_5	
S_5		Допустить

В соответствии с этой таблицей переходов символ «Б» может быть закодирован следующими бинарными строками, словами из множества L(**КА2***) = {001,0111,01001}. Очевидно, что эти языки, множества не пересекаются.

Для шифрования букв латинского алфавита потребуется 5 бит, а кириллицы 6 бит. Очевидно, что после шифрования

строка может быть длиннее на бит лишь в редких случаях. Максимальное удлинение зашифрованного текста в приведенном примере будет 1/6. Иногда зашифрованный текст может быть даже короче исходного. Однако при наличии кодирующего множества, языка L(**KAi***) хотя бы размером в 2 слова для каждой буквы мы гарантировано получим удлинение зашифрованного текста хотя бы на 1 бит. Иначе невозможно будет добиться не пересекающихся кодирующих множеств для всех символов алфавита. Поэтому, для реализации системы шифрования как правило потребуется таблица переходов с большим количеством состояний-строк.

В вышеприведенной системе шифрования, при существенном уменьшении коэффициента расширения зашифрованного текста может понизиться крипто стойкость. Очевидно возможность кодировать один и тот же символ разными битовыми словами повышает крипто стойкость системы шифрования. Корреляция крипто стойкости и коэффициента удлинения зашифрованного текста для данной системы шифрования недостаточно изучена. Предполагается, что уже при небольшом коэффициенте расширения, например, 1,5 или 2 она не существенна.

Список использованных источников:

1. Кондакова С. В., Орлов С. В, «Пример построения возможно односторонней функции на основе контекстно-свободной и регулярных грамматик», сборник научных трудов «Науковий часопис НПУ імені М. П. Драгоманова. Серія 1. Фізико-математичні науки», вып.13(2), 2012, С. 77–84.

2. Джон Хопкрофт, Раджив Мотвани, Джеффри Ульман. Введение в теорию автоматов, языков и вычислений, Introduction to Automata Theory, Languages, and Computation. – М.: «Вильямс», 2002, 528с

3. Орлов С. В., Система шифрования на основе контекстно зависимых и регулярных грамматик, 3 международная конференция «Компьютерная алгебра иинформационные технологии», ОНУ, Украина, 20–25 августа 2018 г., С. 113–116.

4. М. Герри, Д. Джонсон, «Вычислительные машины и трудно разрешимые задачи», М.: Мир, 1982., 419 с.

Ключові слова: кінцеві автомати, автомати з магазинною пам'яттю, система шифрування.
Ключевые слова: конечные автоматы, автоматы с магазинною памятью, система шифрования.
Keywords: finite-state machine, pushdown automaton, encryption system.

Онацкий Алексей Витальевич
Национальный университет «Одесская юридическая академия»,
преподаватель кафедры кибербезопасности,
кандидат технических наук, доцент

Поляков Дмитрий Владимирович
Одесская национальная академия связи им. А. С. Попова,
студент 7 курса специальности 125 – Кибербезопасность

Дубовой Ярослав Владимирович
Одесская национальная академия связи им. А. С. Попова,
студент 6 курса специальности 125 – Кибербезопасность

ПРОТОКОЛ АУТЕНТИФИКАЦИИ НА ОСНОВЕ КРИПТОСИСТЕМЫ NTRU

Протоколы аутентификации можно рассматривать как вид интерактивного доказательства знания. Интерактивное доказательство – понятие теории сложности вычислений, составляющее основу понятия доказательства с нулевым разглашением (zero-knowledge proof – ZKP) [1…3]. Широкое распространение получили криптографические протоколы ZKP на базе ассиметричного шифрования, наиболее известными являются: Fiat–Shamir, Schnorr, Okamoto, Guillou–Quisquater, Brickell–McCurley, Feige–Fiat–Shamir [1 … 3].

Целью работы является разработка протокола ZKP на основе криптосистемы NTRU (Nth-degree TRUncated polynomial