УДК510.582

ВИКОРИСТАННЯ МАШИНИ ТЬЮРИНГА ДЛЯ РОЗВ'ЯЗАННЯ КРИПТОГРАФІЧНОЇ ЗАДАЧІ ПОЛІНОМІАЛЬНОЇ СКЛАДНОСТІ

ПЕТРОВА О.О., БУРМЕНСЬКИЙ Р.В.

Пропонується модель процесу обчислення на детермінованій однострічковій машині Тьюринга для реалізації симетричного алгоритму шифрування з використанням полібіанського квадрату. Наводяться етапи кодування даних та програма, що моделює роботу машини Тьюринга для рішення задачі криптографії.

Ключові слова: машина Тьюринга, алгоритм шифрування, квадрат Полібія.

Key words: Turing machine, encryption algorithm, Polybius square.

Вступ

Проблеми рішення задач можна розділити на класи відповідно до складності їх розв'язання. Клас P складається з проблем, які можна вирішити за поліноміальний час, клас NP – із проблем, які можна вирішити за поліноміальний час тільки на недетермінованій машині Тьюринга (МТ). Як відмічається в роботі [1], важливість NP у криптографії полягає в тому, що більшість симметричних алгоритмів і алгоритмів з відкритими ключами можуть бути зламані за недетермінований поліноміальний час. Для даного шифротексту C криптоаналітик просто вгадує відкритий текст X і ключ k, і за поліноміальний час виконує алгоритм шифрування з входами X і k та перевіряє, чи дорівнює результат C. Клас NP включає клас P, оскільки будь–яка проблема, вирішувана за поліноміальний час на детермінованій МТ, буде також вирішена за поліноміальний час на недетермінованій машині Тьюринга, при цьому пропускається етап припущення. Якщо всі NP проблеми вирішуються за поліноміальний час на детермінованій машині, то P = NP.

Більшість задач, цікавих з практичної точки зору, мають поліноміальні алгоритми вирішення. Це означає, що час роботи алгоритму на вході довжини n складає не більше $O(n^k)$ для деякої константи k, яка є незалежною від довжини входу.

Задача називається поліноміальною, тобто відноситься до класу P, якщо існує константа k і алгоритм, що вирішує задачу з $F_a(n)=O(n^k)$, де n – довжина входу алгоритму в бітах.

Таким чином, задачі класу P є уточненням означення «практично вирішуваної» задачі.

Актуальність: в сучасному світі висококваліфікований спеціаліст може отримати доступ практично до будь–якої інформації на комп'ютері. Для запобігання несанкціонованого втручання необхідно використовувати методи захисту інформації, що є основою сучасної криптографії, в якій використовується симетричне та асиметричне шифрування.

Мета роботи: побудова функціональної схеми машини Тьюринга для рішення задачі криптографії.

Для досягнення поставленої мети сформульовані такі завдання:

– ознайомлення з задачами криптографії, які мають поліноміальний алгоритм вирішення;

– розробка моделі процесу обчислення на детермінованій однострічковій МТ;

– аналіз сучасних досліджень шифрування з використанням МТ;

– побудова МТ для реалізації симетричного алгоритму шифрування з використанням полібіанського квадрату.

1. Аналіз попередніх досліджень

Симетричні алгоритми, які іноді називають умовними, представляють собою алгоритми, у яких ключ шифрування, може бути розрахований за ключем дешифрування і навпаки [1]. У більшості симетричних алгоритмів ключі шифрування і дешифрування одні й ті ж. Ці алгоритми, які також називають алгоритмами із секретним ключем або алгоритмами з одним ключем, вимагають, щоб відправник і отримувач узгодили ключ, що використовується перед початком безпечної передачі повідомлень. Безпечність симетричного алгоритму визначається ключем, розкриття ключа означає, що хто завгодно зможе шифрувати і дешифрувати повідомлення. Доки повідомлення, що передаються, повинні бути таємними, ключ повинен зберігатися у секреті. Шифрування і дешифрування з використанням симетричного алгоритму позначається як: EK(M)=C DK(C)=M.

На сьогодні розроблена велика кількість алгоритмів стійкої криптографії. В цьому аспекті цікавим представляється доведення розв'язання криптографічної задачі на МТ.

В [2] автор кодує правила роботи МТ інгібіторною мережею Петрі та відмічає, що програма не є повністю визначеною, оскільки є некоректні конфігурації МТ.

В роботі [3] розглядається побудова МТ, що шифрує текст за допомогою таблці відповідності. Кожній літері латинського алфавіту зіставляється відповідний бінарний код. У шифротекст додаються «сміттєві символи», що ускладнюють процес дешифрування, але шифротекст дуже легко піддається розшифровці. Для цього необхідно виокремити з нього бінарні числа і розшифрувати код за таблицею відповідності.

Автором Чернушко М.М. у роботі [4] була розглянута «…задача реалізації за допомогою МТ алгоритму симетричного шифрування методом перестановки та алгоритму шифрування методом одноалфавітної підстановки». При використанні шифрування методом одноалфавітної підстановки автор розглядав алфавіт, який складається тільки з символів «АБВГДЕ», що суттєво звужує діапазон слів, які підлягають шифруванню.

В наведеній у даній статті функціональній схемі МТ подолано це обмеження і є можливість шифрування слів з усіх літер англійського алфавіту та деяких спеціальних символів.

Як бачимо, кожен із запропонованих алгоритмів шифрування, реалізований на МТ, має свої переваги та недоліки.

2. Основний матеріал

МТ є найбільш загальною математичною моделлю «детермінованого перетворювача слів», тобто моделлю, за допомогою якої може бути обчислена будь–яка функція з множини слів в одному алфавіті в множину слів в іншому алфавіті. Кожна окрема МТ здатна виконувати тільки один алгоритм, для визначення якого можна користуватись терміном «програма МТ» – набір інструкцій, які спрощені до однотипної схеми. Всі МТ відрізняються своїми програмами [5].

МТ має в розпорядженні кінцеве число знаків (символів): $a_1, a_2, ..., a_m$, що утворюють зовнішній алфавіт, в якому кодуються відомості, що подаються в машину, а також ті, які виробляються в ній. В МТ обробка інформації, як і в комп'ютері, виконується в логічному блоці, який може перебувати в одному з кінцевої кількості станів: $q_1, q_2, ...q_n$. Блок має два вхідних канали: через один із них на кожній стадії роботи машини (в кожному такті) надходить знак з клітинки, яку оглядають, через інший – знак q_i того стану, який приписується блоку на даний такт. Через вихідний канал блок посилає в клітинку, яку оглядає, відповідний «перепрацьований» знак a_j, що є однозначною функцією від сигналів $a_j q_i$, поданих на вхід (рис. 1).

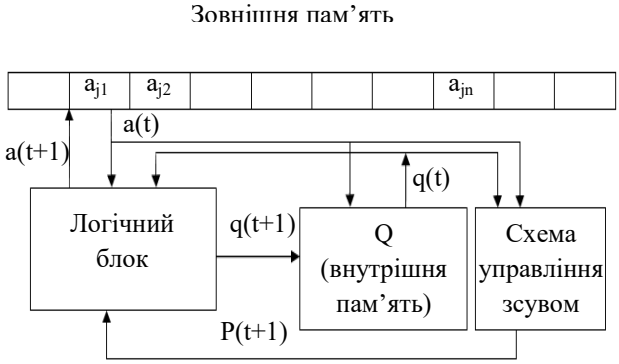


Рис. 1. Обробка інформації в МТ

Логічний блок реалізує функцію, яка ставить у залежність кожній парі знаків: a_i, q_n (кількість таких пар складає $k*m$) трійку знаків: a_j, D, q_t. Таку логічну функцію зручно подавати у вигляді прямокутної таблиці, стовпчики якої занумеровані знаками стану, а рядки – знаками зовнішнього алфавіту. В кожній клітинці таблиці записано відповідну вихідну трійку знаків. Таку таблицю можна називати функціональною схемою машини [5].

В роботах [6,7] наведено схематичне зображення детермінованої однострічкової машини Тьюринга, описано стуктуру МТ та розроблено протоколи програм МТ для рішення задач обчислювальної математики.

В даній статті наведено функціональну схему МТ для симетричного алгоритму шифрування методом квадрата Полібія.

Квадрат Полібія є загальною моноалфавітною підстановкою, яка проводиться за допомогою випадково заповненої алфавітом квадратної таблиці. Класичний полібіанський квадрат – таблиця, що складається з 5 рядків і 5 стовпців, заповнена випадковим чином буквами грецького алфавіту і пробілом. При шифруванні в таблиці знаходять букву відкритого тексту і записують у шифртекст букву, розташовану нижче від неї в тому ж стовпці. Якщо літера вихідного тексту знаходиться в нижньому рядку таблиці, то їй відповідає буква першого рядка з цього ж стовпця.

Існує декілька методів використання квадрата Полібія.

1. Суть першого методу полягає в тому, що замість кожної літери в слові використовується відповідна їй літера знизу (A = F, B = G).

2. В другому методі зазначаються відповідні кожній літері цифри з таблиці: першою пишеться цифра по вертикалі, другою – по горизонталі (A = 11, B = 21).

3. Третій метод базується на попередньому методі, при цьому записаний попарно первісний код здвигається вліво на одну позицію, в другий раз розділяється попарно, в результаті чого отримується шифр [8].

4. Четвертий метод аналогічний другому методові, але на відміну від нього шифр розділяється на 2 блоки: цифри по вертикалі пишуться в лівому блоці, а по горизонталі – в правому.

В запропонованій роботі концепцію полібіанського квадрата реалізовано з використанням англійських літер та спеціальних знаків на основі четвертого методу використання квадрата Полібія в таблиці розміром 6x6 (рис. 2).

	1	2	3	4	5	6
1	A	B	C	D	E	F
2	G	H	I	J	K	L
3	M	N	O	P	Q	R
4	S	T	U	V	W	X
5	Y	Z	.	,	:	@
6	-	+	=	(	)	?

Рис. 2. Квадрат Полібія

Для кращого розуміння шифрування цим методом наведемо приклад: слово CODE шифрується двома блоками цифр 3345 1311. Якщо розділити код попарно 33 45 13 11, то згідно з символами, наведеними в таблиці (рис. 2), отримаємо сукупність символів «O,MA».

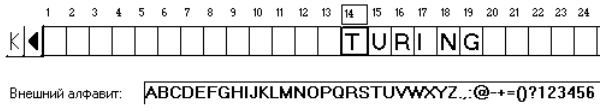
Четвертий метод використання квадрата Полібія було реалізовано в програмному інтерпретаторі машини Тьюринга ALGO 2000 [9].

Розроблена авторами програма, що моделює шифрування тексту методом квадрата Полібія, працює за таким принципом: у стані q_0 МТ переглядає символ у клітині, на якій розташована головка, після чого, якщо цей символ наявний у квадраті Полібія, головка записує відповідну йому цифру шифру по вертикалі у поточну клітину та переходить у відповідний стан $q_1 – q_6$, де індекс q вказує на цифру шифру по горизонталі. У разі, якщо в стані q_0 не було знайдено символу, що входить до квадрата Полібія (головка дійшла до кінця символьної послідовності), то робота МТ завершується.

У станах $q_1 – q_6$ головка МТ переміщується у кінець символьної послідовності до порожньої клітини та ставить відповідну індексу стану q цифру шифру по горизонталі, після чого МТ переходить у стан q_7.

У стані q_7 головка МТ переміщується у початок символьної послідовності, після чого МТ переходить у початковий стан q_0.

Для перевірки роботи запропонованого алгоритму було введено прізвище Алана Тьюринга (рис. 3).



A\Q	Q2	Q3	Q4	Q5	Q6	Q7
A	A → Q2	A → Q3	A → Q4	A → Q5	A → Q6	A ← Q7
B	B → Q2	B → Q3	B → Q4	B → Q5	B → Q6	B ← Q7
C	C → Q2	C → Q3	C → Q4	C → Q5	C → Q6	C ← Q7
D	D → Q2	D → Q3	D → Q4	D → Q5	D → Q6	D ← Q7
E	E → Q2	E → Q3	E → Q4	E → Q5	E → Q6	E ← Q7
F	F → Q2	F → Q3	F → Q4	F → Q5	F → Q6	F ← Q7
G	G → Q2	G → Q3	G → Q4	G → Q5	G → Q6	G ← Q7
H	H → Q2	H → Q3	H → Q4	H → Q5	H → Q6	H ← Q7
I	I → Q2	I → Q3	I → Q4	I → Q5	I → Q6	I ← Q7
J	J → Q2	J → Q3	J → Q4	J → Q5	J → Q6	J → Q7
K	K → Q2	K → Q3	K → Q4	K → Q5	K → Q6	K ← Q7
L	L → Q2	L → Q3	L → Q4	L → Q5	L → Q6	L ← Q7
M	M → Q2	M → Q3	M → Q4	M → Q5	M → Q6	M ← Q7
N	N → Q2	N → Q3	N → Q4	N → Q5	N → Q6	N ← Q7
O	O → Q2	O → Q3	O → Q4	O → Q5	O → Q6	O ← Q7
P	P → Q2	P → Q3	P → Q4	P → Q5	P → Q6	P ← Q7
Q	Q → Q2	Q → Q3	Q → Q4	Q → Q5	Q → Q6	Q ← Q7
R	R → Q2	R → Q3	R → Q4	R → Q5	R → Q6	R ← Q7

Рис. 3. Фрагмент протоколу побудованої МТ

Результат шифрування слова «TURING» методом квадрата Полібія наведено на рис. 4.

A\Q	Q0	Q1	Q2	Q3	Q4	Q5
X	6 → Q4	X → Q1	X → Q2	X → Q3	X → Q4	X → Q5
Y	1 → Q5	Y → Q1	Y → Q2	Y → Q3	Y → Q4	Y → Q5
Z	2 → Q5	Z → Q1	Z → Q2	Z → Q3	Z → Q4	Z → Q5
.	3 → Q5	. → Q1	. → Q2	. → Q3	. → Q4	. → Q5
,	4 → Q5	, → Q1	, → Q2	, → Q3	, → Q4	, → Q5
:	5 → Q5	: → Q1	: → Q2	: → Q3	: → Q4	: → Q5
@	6 → Q5	@ → Q1	@ → Q2	@ → Q3	@ → Q4	@ → Q5
-	1 → Q6	- → Q1	- → Q2	- → Q3	- → Q4	- → Q5
+	2 → Q6	+ → Q1	+ → Q2	+ → Q3	+ → Q4	+ → Q5
=	3 → Q6	= → Q1	= → Q2	= → Q3	= → Q4	= → Q5
(	4 → Q6	(→ Q1	(→ Q2	(→ Q3	(→ Q4	(→ Q5
)	5 → Q6	) → Q1	) → Q2	) → Q3	) → Q4	) → Q5
?	6 → Q6	? → Q1	? → Q2	? → Q3	? → Q4	? → Q5
1	1 → Q0	1 → Q1	1 → Q2	1 → Q3	1 → Q4	1 → Q5
2	2 → Q0	2 → Q1	2 → Q2	2 → Q3	2 → Q4	2 → Q5

Рис. 4. Результат шифрування

Для представлення інформації в текстовому вигляді отриманий шифр розбивається попарно: 23 63 21 44 32 32 і отриманим парам цифр знаходяться відповідні літери в таблиці. Результатом шифрування слова «TURING» буде сукупність літер «NRBVII».

Висновки

На основі результатів досліджень запропонована функціональна схема машини Тьюринга, яка доводить алгоритм розв'язання запропонованої криптографічної задачі поліноміальної складності. Наведено структуру розробленої МТ, розглянуто операції, які вона виконує, виконано програмне моделювання роботи МТ для реалізації криптографічного алгоритму.

До переваг запропонованого методу шифрування належать:

–можливість довільного заповнення таблиці символами, що може ускладнити дешифрування без наявної у отримувача таблиці Полібія на відміну від методу шифру Цезаря та шифру із кодовим словом;

–неможливість дешифрування «на льоту» на відміну від шифру одноалфавітною підстановкою чи перестановкою та відносна складність визначення шифру, оскільки дешифрування тексту за трьома першими методами квадрата Полібія не приведе до успіху;

– квадрат Полібія має однакову кількість рядків та стовпців, що не завжди виконується для таблиці відповідності, а отже, неможливо одразу визначити, який індекс літери шифротексту відповідає рядку, а який – стовпцю.

З огляду на простоту правил побудови запропоновані коди можна ефективно використовувати для захисту індивідуальних користувачів. При цьому обраний метод шифрування є досить простим, оскільки реалізація більш складних алгоритмів шифрування є проблема-

тичною у плані громіздкості програми для МТ. Тому доречнішим для реалізації більш досконалих алгоритмів шифрування буде використання мов програмування.

Література: 1. *Левина А.Б.* Моделирование криптосистем. Санкт-Петербург: НИУ ИТМО, 2013. 82 с. **2**. *Зайцев Д.А.* Ингибиторная сеть Петри, исполняющая произвольную заданную машину Тьюринга / Д.А. Зайцев // Систем. дослідж. та інформ. технології. 2012. № 2. С. 26-41. **3.** *Z. Saqib, M. A. Shahid, M. U. Ashraf.* Encryption and Decryption Using Automata Theory/ International Journal of Multidisciplinary Sciences and Engineering, Vol. 6, No. 4, April 2015. P. 14-21. **4.** *Чернушко М.М.* Применение машины Тьюринга для реализации алгоритмов шифрования [Текст] / М. М. Чернушко // Технические науки: теория и практика: материалы II междунар. науч. конф. Чита: Молодой ученый, 2014. С. 19-22. **5.** *Трахтенброт Б.А.* Алгоритмы и машинное решение задач. М.: Государственное издательство технико-теоретической литературы, 1957. 96 с. **6.** *Петрова О.О., Бурменський Р.В.* Моделювання машини Тьюринга обчислення додатку чисел // Всеукраїнська студентська наукова конференція «Наукова Україна» (з міжнародною участю), м. Дніпропетровськ, 2015. С. 215-218. **7.** *Петрова О., Бурменський Р.* Функціональна схема машини Тьюринга для множення числа на 11 // Матеріали VII Українсько-польської науково-практичної конференції «Електроніка та інформаційні технології» (ЕлІТ-2015), Львів-Чинадієво-2015. С.139-141. **8.** *Tumblr*. 14 способов шифрования. [Електронний ресурс]. Режим доступу: http://thereichenbachblog.tumblr.com/typesofcipher **9.** Эмулятор машины Поста (ALGO 2000). [Електронний ресурс]. Режим доступу: http://teach.sc585.spb.ru/inf/2011/11/21/эмулятор-машины-поста-algo-2000/

Транслитерированный список литературы:

Література: 1. *Levina A.B.* Modelirovanie kriptosistem. Sankt-Peterburg: NIU ITMO, 2013. 82 s. **2.** *Zajcev D.A.* Ingibitornaja set' Petri, ispolnjajushhaja proizvol'nuju zadannuju mashinu T'juringa / D.A. Zajcev // Sistem. doslidzh. ta inform. tehnologiї. 2012. № 2. S. 26-41. **3.** *Z. Saqib, M. A. Shahid, M. U. Ashraf.* Encryption and Decryption Using Automata Theory/ International Journal of Multidisciplinary Sciences and Engineering, Vol. 6, No. 4, April 2015. C. 14-21. **4.** *Chernushko M. M.* Primenenie mashiny T'juringa dlja realizacii algoritmov shifrovanija [Tekst] / M. M. Chernushko // Tehnicheskie nauki: teorija i praktika: materialy II mezhdunar. nauch. konf. Chita: Molodoj uchenyj, 2014. S. 19-22. **5.** *Trahtenbrot B.A.* Algoritmy i mashinnoe reshenie zadach. M.: Gosudarstvennoe izdatel'stvo tehniko-teoreticheskoj literatury, 1957. 96 s. **6.** *Petrova O.O., Burmens`ky`j R.V.* Modelyuvannya mashy`ny` T`yury`nga obchy`slennya dodatku chy`sel // Vseukrayins`ka students`ka naukova konferenciya «Naukova Ukrayina» (z mizhnarodnoyu uchastyu), m. Dnipropetrovs`k, 2015. S. 215-218. **7.** *Petrova O., Burmens`ky`j R.* Funkcional`na sxema mashy`ny` T`yury`nga dlya mnozhennya chy`sla na 11 // Materialy` VII Ukrayins`kopol`s`koyi naukovo-prakty`chnoyi konferenciyi «Elektronika ta informacijni texnologiyi» (ElIT -2015), L`viv-Chy`nadiyevo-2015. S.139-141. **8.** *Tumblr*. 14 sposobov shifrovanija. [Електронний ресурс]. http://thereichenbachblog.tumblr.com/typesofcipher **9.** Эмулятор машины Поста (ALGO 2000). [Електронний ресурс]. http://teach.sc585.spb.ru/inf/2011/11/21/эмулятор-машины-поста-algo-2000/

Надійшла до редколегії 12.11.2015

Рецензент: д-р техн. наук Гіль М.І.

Петрова Олена Олександрівна, канд. техн. наук, доцент каф. Економічної кібернетики та інформаційних технологій Харківського національного університету будівництва та архітектури. Наукові інтереси: штучний інтелект, експертні системи. Адреса: Україна, 20322. Харків, вул. Сумська, 40, тел. +38 098 8499 076.

Бурменський Рустам Валерійович, студент Харківського національного університету будівництва та архітектури. Наукові інтереси: програмування, тривимірне комп'ютерне моделювання. Захоплення та хоббі: читання наукової літератури про інформаційні технології та космос. Адреса: Україна, 61204. Харків, пр. Перемоги, 62Г, тел. +38 0974352219.