			позитивне – наявність інвестиційного резерву (графік фінансування не виконується)
ІТПВ	Індекс точності планування вартості	ІТПВ=ФВ/ПО	Індекс вище 1 – неточність при плануванні вартості, менше або дорівнює 1 – точність планування вартості

Список використаних джерел:

1. Милощевич Д. Набор инструментов для управления проектами / Драган З. Милошевич: Пер. с англ. Мамонтова Е.В.; Под ред. Неизвестного С. И. – М.: Компания АйТи; ДМК Пресс, 2008. – 729 с.

Бурменський Р.В.
студент;
Петрова О.О.
кандидат технічних наук, доцент,
Харківський національний університет будівництва та архітектури

РЕАЛІЗАЦІЯ КРИПТОГРАФІЧНОГО АЛГОРИТМУ МАШИНОЮ ТЬЮРИНГА

В статті розглядається алгоритм захисту інформаційних ресурсів за допомогою алгоритму шифрування методом квадрату Полібія, реалізований на машині Тьюринга (МТ). Машиною Тьюринга називається формалізм, запропонований для поняття алгоритму англійським математиком, логіком, криптографом та інженером Аланом Тьюрингом.

Авторами в роботах [1, с. 215; 2, с. 139] була розглянута структура МТ та вирішені задачі:

– побудови МТ, яка виконує алгебраїчне додавання N натуральних цілих чисел, заданих у десятковій системі числення;

– побудови МТ, яка виконує множення числа в десятковій системі числення на 11.

Криптографічний алгоритм або шифр – це математична формула, що описує процеси шифрування і розшифрування. Основне призначення криптографічних алгоритмів – це захист інформації.

На сьогоднішній день існує велика кількість криптографічних алгоритмів, що відрізняються як своїми загальними характеристиками, так і принципами, на яких базується їх робота. Основною властивістю криптографічних алгоритмів є їх надійність.

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 її 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 квадрату Полібія.

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

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 [3].

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 квадрату Полібія в таблиці розміром 6x6 (рис. 1).

	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. 1. Квадрат Полібія

Джерело: розроблено авторами

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 символам, наведеним в таблиці (рис. 1) отримаємо сукупність символів «O,MA».

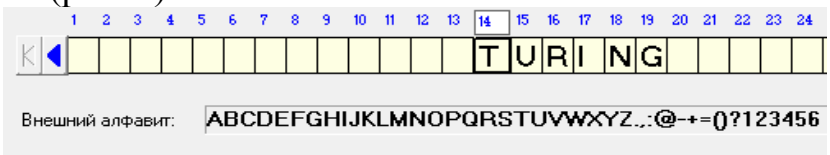
Четвертий метод використання квадрату Полібія було реалізовано в програмному інтерпретаторі машини Тьюринга ALGO 2000 [4].

Розроблена авторами програма, що моделює шифрування тексту методом квадрату Полібія, працює за наступним принципом: у стані q_0 МТ переглядає символ у клітині, на якій розташована головка, після чого, у разі 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 квадрату 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. 2).

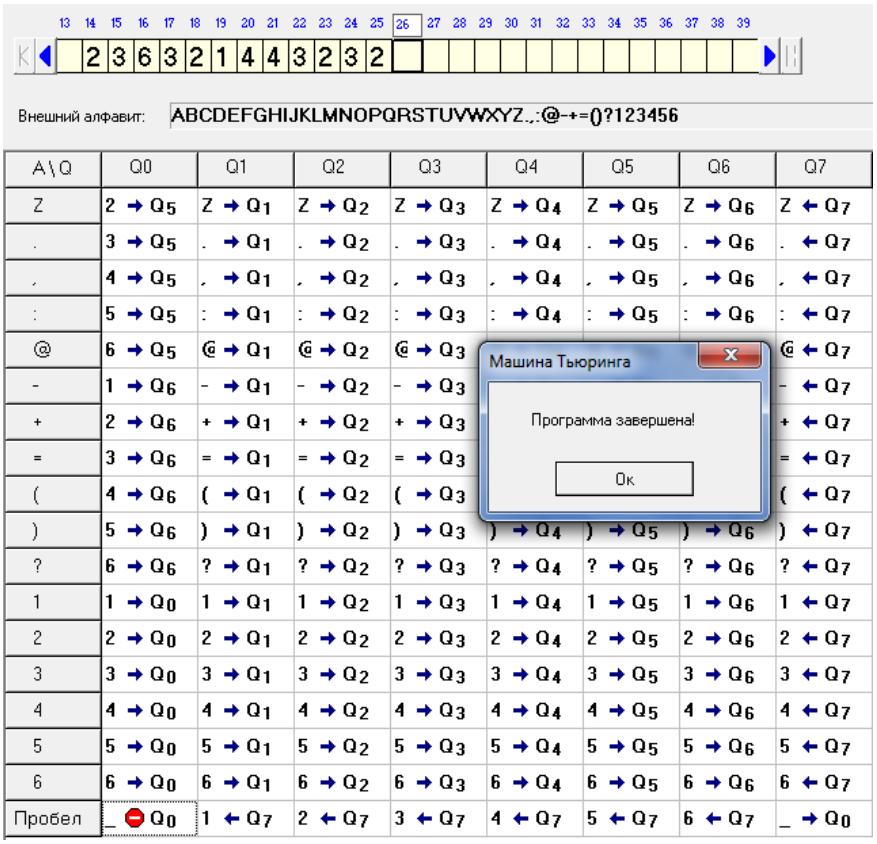


A\Q	Q2	Q3	Q4	Q5	Q6	Q7
A	A → Q2	A → Q3	A → Q4	A → Q5	A → Q6	A ← Q7
B	B → Q2	B → Q3	B → Q4	B → Q5	B → Q6	B ← Q7
C	C → Q2	C → Q3	C → Q4	C → Q5	C → Q6	C ← Q7
D	D → Q2	D → Q3	D → Q4	D → Q5	D → Q6	D ← Q7
E	E → Q2	E → Q3	E → Q4	E → Q5	E → Q6	E ← Q7
F	F → Q2	F → Q3	F → Q4	F → Q5	F → Q6	F ← Q7
G	G → Q2	G → Q3	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. 2. Фрагмент протоколу побудованої МТ

Джерело: розроблено авторами

Результат шифрування слова «TURING» методом квадрату Полібія наведено на рис. 3.



A\Q	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
Z	2 → Q5	Z → Q1	Z → Q2	Z → Q3	Z → Q4	Z → Q5	Z → Q6	Z ← Q7
.	3 → Q5	. → Q1	. → Q2	. → Q3	. → Q4	. → Q5	. → Q6	. ← Q7
,	4 → Q5	, → Q1	, → Q2	, → Q3	, → Q4	, → Q5	, → Q6	, ← Q7
:	5 → Q5	: → Q1	: → Q2	: → Q3	: → Q4	: → Q5	: → Q6	: ← Q7
@	6 → Q5	@ → Q1	@ → Q2	@ → Q3				@ ← Q7
-	1 → Q6	- → Q1	- → Q2	- → Q3				- ← Q7
+	2 → Q6	+ → Q1	+ → Q2	+ → Q3				+ ← Q7
=	3 → Q6	= → Q1	= → Q2	= → Q3				= ← Q7
(	4 → Q6	(→ Q1	(→ Q2	(→ Q3				(← Q7
)	5 → Q6	) → Q1	) → Q2	) → Q3	) → Q4	) → Q5	) → Q6	) ← Q7
?	6 → Q6	? → Q1	? → Q2	? → Q3	? → Q4	? → Q5	? → Q6	? ← Q7
1	1 → Q0	1 → Q1	1 → Q2	1 → Q3	1 → Q4	1 → Q5	1 → Q6	1 ← Q7
2	2 → Q0	2 → Q1	2 → Q2	2 → Q3	2 → Q4	2 → Q5	2 → Q6	2 ← Q7
3	3 → Q0	3 → Q1	3 → Q2	3 → Q3	3 → Q4	3 → Q5	3 → Q6	3 ← Q7
4	4 → Q0	4 → Q1	4 → Q2	4 → Q3	4 → Q4	4 → Q5	4 → Q6	4 ← Q7
5	5 → Q0	5 → Q1	5 → Q2	5 → Q3	5 → Q4	5 → Q5	5 → Q6	5 ← Q7
6	6 → Q0	6 → Q1	6 → Q2	6 → Q3	6 → Q4	6 → Q5	6 → Q6	6 ← Q7
Пробел	_ → Q0	1 ← Q7	2 ← Q7	3 ← Q7	4 ← Q7	5 ← Q7	6 ← Q7	_ → Q0

Рис. 3. Результат шифрування

Джерело: розроблено авторами

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

До переваг запропонованого методу шифрування належать:

– можливість довільного заповнення таблиці символами, що може ускладнити дешифрування без наявної у отримувача таблиці Полібія на відміну від метода 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 квадрату Полібія не призведе до успіху.

При цьому обраний метод шифрування є досить простим, оскільки реалізація більш складних алгоритмів шифрування потребує більшої кількості станів МТ, що є досить проблематичним у плані громіздкості програми для МТ, тому доречнішим для реалізації більш досконалих алгоритмів шифрування буде використання мов програмування.

Список використаних джерел:

1. 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.

2. Петрова О. О., Бурменський Р. В. Функціональна схема машини Тьюринга для множення числа на 11 // Матеріали VII-ої Українсько-польської науково-практичної конференції «Електроніка та інформаційні технології» (ЕлІТ – 2015), Львів–Чинадієво, 2015. – С. 139–141.
3. http://thereichenbachblog.tumblr.com/typesofcipher
4. http://teach.sc585.spb.ru/inf/2011/11/21/эмулятор-машины-поста-algo-2000/

Духович Д.М.
студент,
Науковий керівник: **Вовк Р.Б.**
кандидат технічних наук, доцент,
доцент кафедри програмного забезпечення автоматизованих систем,
Івано-Франківський національний технічний університет нафти і газу

ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ЗАСОБІВ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ В НАВЧАЛЬНОМУ ПРОЦЕСІ

Освітній процес в Україні на сьогоднішній час переживає не найкращі часи, оскільки в більшості випадків використовуються застарілі схеми та програми навчання, які беруть свій початок ще з часів СРСР з недосконалою системою викладання і слабкою прив'язкою до реальних потреб виробництва. Для покращення даної ситуації необхідно здійснювати впровадження абсолютно нових підходів до викладання в навчальних закладах, наприклад застосування різноманітних засобів та систем віртуальної реальності в підготовці фахівців різних галузей.

Віртуальна реальність – це комплекс програмного та апаратного забезпечення, що імітує відчуття сенсорних систем користувача за допомогою візуальної та звукової інформації та дозволяє зануритись в абстрактний світ з використанням спеціалізованих систем [1]. З кожним днем системи віртуальної реальності набувають все більшого поширення. Основною сферою, в якій вони застосовуються є ігрова індустрія, проте можливостей застосування систем віртуалізації існує набагато більше. Зокрема, дані системи можна впровадити в навчальний процес та значно підвищити якість навчання за рахунок інтерактивності між користувачем та навчальним матеріалом. Відомо, що людина сприймає близько 80 відсотків інформації, яка надходить з навколишнього середовища завдяки зоровому аналізатору [2]. Візуальний контакт надає можливість людині краще зрозуміти досліджуваний об'єкт. Водночас звичайного споглядання за об'єктом недостатньо, у випадку, якщо його розглядають з точки зору навчання, тобто намагаються зрозуміти принцип його роботи чи концепцію створення. Для візуального вивчення нових предметів можна використовувати такі пристрої, як «Google Cardboard» [3], «Oculus Rift» [4], «OSVR» [5], а також систему доповнення реальності «Kinect