FRI-2G.302-1-CSNT-03

SOFTWARE IMPLEMENTATION OF CLASSICAL DIGRAFID CIPHER FOR ENCRYPTING AND DECRYPTING ENGLISH TEXTS IN MATLAB [2]

Assist. Prof. Adriana Borodzhieva, PhD
Department of Telecommunications
"Angel Kanchev" Univesity of Ruse
Phone: 082 888 734
E-mail: aborodzhieva@uni-ruse.bg

Abstract: *The paper presents one of the classical ciphers in cryptography, the digrafid cipher. Most classical ciphers can be practically computed and solved by hand. They are also usually very simple to break with modern technologies. In classical cryptography, the digrafid cipher is a cipher, which combines the bifid and trifid ciphers. It was invented in 1960 by the American Cryptogram Association (ACA). The paper presents MATLAB-based software tool implementing encryption and decryption of English texts using the "classical" digrafid cipher with 27 symbols. The tool will be used in the course "Telecommunication Security" by students of the specialty "Telecommunication Systems" for the Bachelor degree at the University of Ruse but it can be applied in other courses involving issues of cryptographic information protection.*

Keywords: *E-Learning, encryption, decryption, digrafid cipher, English texts, MATLAB.*

ВЪВЕДЕНИЕ

В криптографията, класическият шифър е вид шифър, използван в миналото, който днес вече не се прилага. За разлика от съвременните криптографски алгоритми, повечето класи-чески шифри могат да бъде решени на ръка. Обикновено те са лесни за разбиване с модерните технологии. Терминът класически шифър включва простите системи, използвани от древно-гръцки и римски времена, сложните ренесансови шифри, криптографията от Втората световна война, като машината Енигма и др. За разлика от класическите шифри, съвременната крипто-графия разчита на нови алгоритми и компютри, разработени от 1970 г. насам [1].

В материала се описва шифър DIGRAFID, който комбинира двуразделните (bifid) и триразделните (trifid) шифри. Той е изобретен през 1960 г. от American Cryptogram Association (ACA, Американската асоциация по криптограма). В „класическия" шифър digrafid, една „разбъркана" азбука е записана в мрежа (матрица) с размерност 3 x 9, а втора „разбъркана" азбука е записана в решетка (матрица) с размерност 9 x 3. Таблица от числа, с размерност 3 x 3, е написана от дясно на първата мрежа и над втората мрежа с „разбъркани" азбуки. Първата мрежа има написани в заглавията на колоните цифрите от 1 до 9, а втората мрежа – цифрите от 1 до 9 от дясната страна. Избира се фракциониране (раздробяване) 3 или 4.

Откритият текст (текстът за шифриране) се записва в групи от два символа. За всеки диграф се открива уникално трицифрено число. Цифрите се групират чрез фракциониране, като фракциониране на три се състои от три диграфа в група. След това числата се четат хоризонтално по групи за определяне на диграфите на шифрирания текст [2]. В публикацията е представен MATLAB-базиран софтуерен инструмент за криптиране и декриптиране на английски текстове чрез шифри digrafid и 27-символна азбука (класическия вариант). Целта е да се илюстрират процесите на криптиране и декриптиране при различни ключове и фракциониране. Софтуерният инструмент е предназначен за дисциплината „Телекомуникационна сигурност" за студентите от специалност „Телекомуникационни

[2] Докладът е представен на сесията на 27 октомври 2017 с оригинално заглавие на български език: СОФТУЕРНА РЕАЛИЗАЦИЯ НА „КЛАСИЧЕСКИЯ" DIGRAFID ШИФЪР ЗА КРИПТИРАНЕ И ДЕКРИПТИРАНЕ НА АНГЛИЙСКИ ТЕКСТИВЕ ЧРЕЗ MATLAB

системи”, образователно-квалификационна степен „Бакалавър”, при Русенски университет „Ангел Кънчев”.

ИЗЛОЖЕНИЕ

Криптиране/декриптиране на английски текстове чрез шифър DIGRAFID

Шифърът DIGRAFID използва таблици, в които се „разбъркват” две азбуки. Откритият текст се разделя на диграфи, а диграфите се записват в групи, като броят на диграфите във всяка група е периодът на шифъра. Всеки диграф има уникално трицифрено число от таблиците и те се записват вертикално под съответния диграф [2, 3]. Трицифрените числа се разделят (раздробяват) и новите трицифрени числа се поставят в таблиците, за да се получат диграфите на шифрирания текст. Първата буква на диграфа се намира в хоризонталната азбука, а втората – във вертикалната азбука, а числото на „пресичане” между двете азбуки – между тях [2, 3].

Пример. В класическия digrafid шифър се използват матрици с размерности 3 × 9 и 9 x 3. Чрез задаване на хоризонталните и вертикалните ключови думи без повторение, буквите на ключовите думи се попълват последователно ред по ред в 3 × 9-матрицата и колона по колона в 9 × 3-матрицата. След тях по азбучен ред се добавят останалите букви от азбуката, които не са включени в състава на ключовите думи [2]. Матриците съдържат 27 клетки, така че символът „.” се поставя в последната клетка. Първата „разбъркана” азбука е написана в решетка 3 x 9 въз основа на ключовата дума HORIZONTAL, а втората „разбъркана” азбука е написана в решетка 9 x 3, базирана на ключовата дума VERTICAL. Вдясно от първата решетка на „разбъркана” азбука и над втората решетка на „разбъркана” азбука е записана решетка 3 x 3 с числата от 1 до 9. Първата мрежа с „разбъркана” азбука има написани в заглавията на колоните числата от 1 до 9. Втората мрежа с „разбъркана” азбука има написани отдясно числата от 1 до 9. Използва се фракциониране (раздробяване) 3 или 4.

	1	2	3	4	5	6	7	8	9			
1	H	O	R	I	Z	N	T	A	L	1	2	3
2	B	C	D	E	F	G	J	K	M	4	5	6
3	P	Q	S	U	V	W	X	Y	.	7	8	9

V	D	P	1
E	F	Q	2
R	G	S	3
T	H	U	4
I	J	W	5
C	K	X	6
A	M	Y	7
L	N	Z	8
B	O	.	9
1	2	3	

Раздробяване 3

Открит текст:	D	I	G	R	A	F	I	D	C	I	P	H	E	R
Елемент 1:	3	6	8				4	2	1				4	
Елемент 2:	4	4	2				2	4	8				4	
Елемент 3:	5	3	2				1	5	4				3	
Елемент 1:	3	4	5				4	2	1				4	
Елемент 2:	6	4	3				2	4	5				4	
Елемент 3:	8	2	2				1	8	4				3	
Шифро-текст:	D	Z	E	E	Z	Q	I	D	C	L	B	H	E	R

Раздробяване 4

Открит текст:	D	I	G	R	A	F	I	D	C	I	P	H	E	R
Елемент 1:	3	6	8	4					2	1	4			
Елемент 2:	4	4	2	2					1	8	4			
Елемент 3:	5	3	2	1					5	4	3			
Елемент 1:	3	4	2	3					2	1	5			
Елемент 2:	6	4	2	2					1	8	4			
Елемент 3:	8	4	5	1					4	4	3			
Шифро-текст:	D	Z	E	T	O	J	R	D	O	T	P	H	F	R

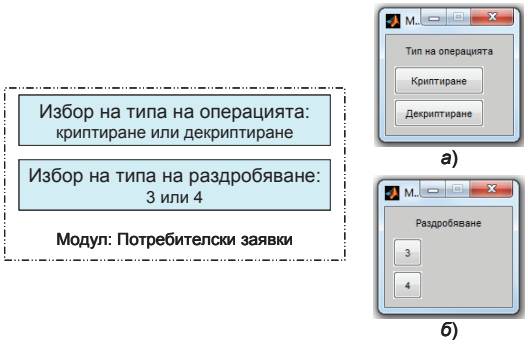
Откритият текст (текстът за шифриране) е DIGRAFID CIPHER (без интервали) и е написан на групи от два символа. За всеки диграф се открива уникално трицифрено число. Например, за диграф DI, това трицифрено число е 345, защото първата буква на диграфа “D” се намира в третата колона (ca = 3) и във втория ред (ra = 2). Втората буква на диграфа “I” се намира в първата колона (cb = 1) и в петия ред (rb = 5). Цифрата в средата (4) се намира във втория ред и в първата колона в решетката 3 x 3 с числата от 1 до 9. Цифрите се групират чрез фракциониране (трикратното разделяне/раздробяване се състои от три диграфа в група, а четирикратното разделяне/раздробяване се състои от четири диграфа в група), след което числата се четат хоризонтално група по група, за да се определят диграфите на шифрирания текст по същия начин [2].

Първоначално разработеният софтуерен инструмент показва изображения в отделни графични прозорци с цел разясняване на теоретичния материал. В публикацията са дадени екранни снимки на примери за криптиране/декриптиране на текстове на английски език. В

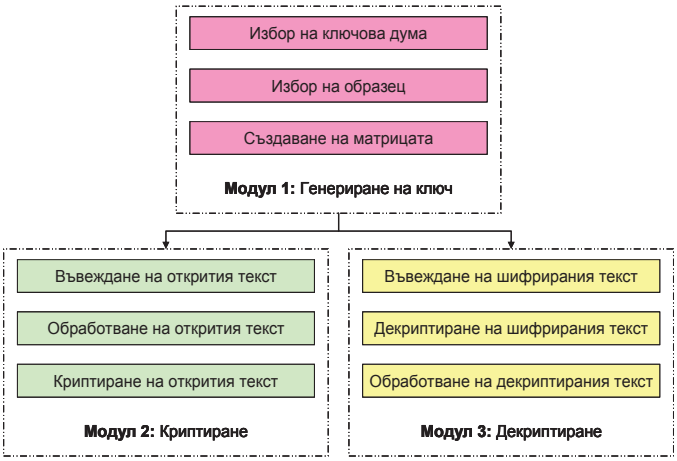
бъдеще алгоритъмът, представен в доклада, ще бъде модифициран за криптиране и декриптиране на английски текстове с по-голям брой символи в използваната азбука, както и на български текстове.

MATLAB-базирано приложение за криптиране и декриптиране на английски текстове с класическия шифър DIGRAFID

В публикацията са описани етапът на проектирането и принципът на действие на софтуерен инструмент за осъществяване на процесите на криптиране и декриптиране при използване на класическия шифър digrafid. Представени са архитектурата на системата и модулите за генериране на ключове и криптиране/декриптиране. Софтуерният инструмент е разработен в MATLAB и ще се прилага в учебния процес по дисциплината „Телекомуникационна сигурност”. Софтуерният инструмент позволява на потребителя да избира от меню тип на операцията (криптиране или декриптиране – фиг. 1, а) и тип на фракционирането (3 или 4, фиг. 1, б). Софтуерният инструмент се състои от три модула: 1) Модул 1 – Генериране на ключа; 2) Модул 2 – Криптиране; 3) Модул 3 – Декриптиране. Архитектурата на системата и структурите на модулите за генериране на ключ, криптиране и декриптиране са представени на фиг. 2.



Фиг. 1. Обработване на потребителски заявки



Фиг. 2. Архитектура на системата

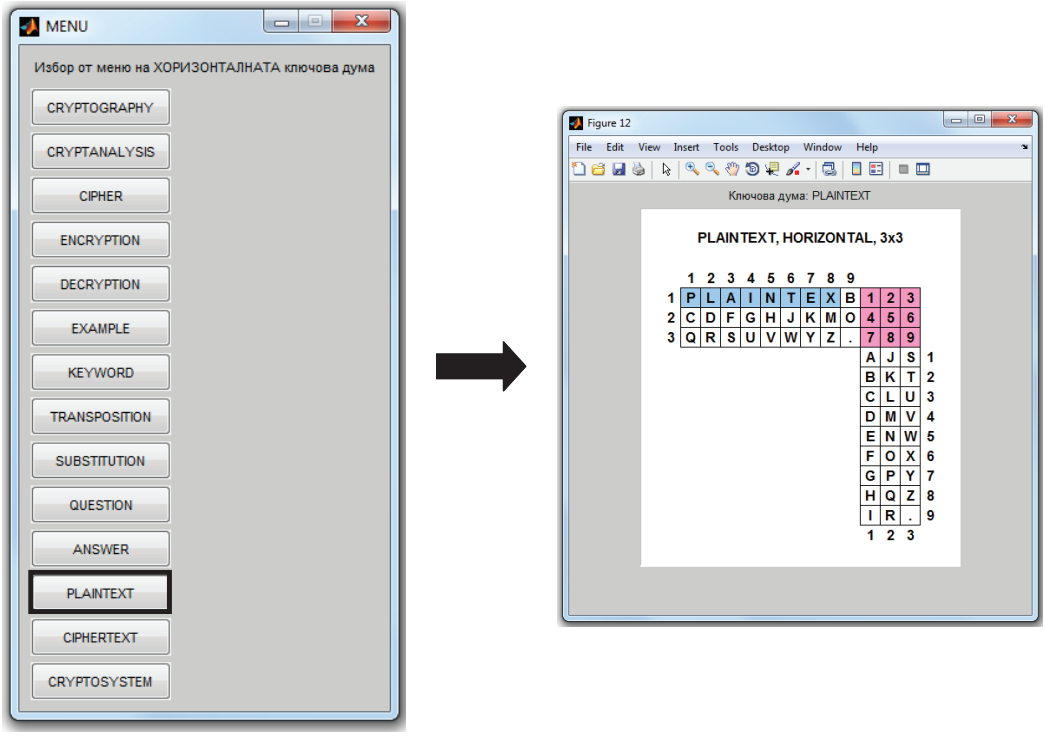
Модул 1 – Генериране на ключа. Най-напред потребителят избира ключови думи или фрази за изграждане на хоризонталната и вертикалната матрици (фиг. 3). Тук потребителят може да избира от 14 ключови думи. След това матриците се формират и в графични прозорци се изобразяват картинки на матриците, които ще се използват (например, когато ключовата дума PLAINTEXT е избрана за хоризонталната матрица и ключовата дума CIPHERTEXT е избрана за вертикалната матрица).

Модул 2 – Криптиране. Потребителят въвежда открития текст (текста за шифриране). Той се съхранява в стринговата променлива s. След това откритият текст се обработва в три етапа: 1) премахване на интервалите в открития текст (Обработка 1); 2) преобразуване на малките букви в главни букви в открития текст (Обработка 2); 3) вмъкване на нов символ, ако е необходимо – ако броят на символите в открития текст е нечетно число, тогава в края на низа се вмъква символът „.” за възможността за разделяне на символите на текста на диграфи (Обработка 3). Процесът на криптиране се изпълнява, използвайки зависимостите в таблица 1.

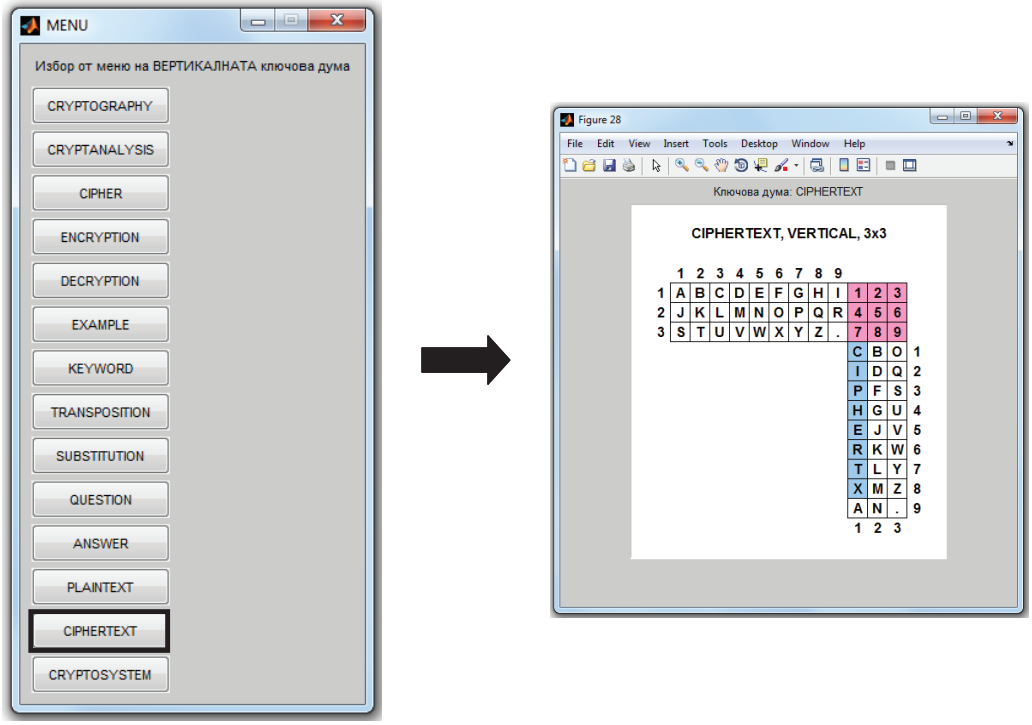
Модул 3 – Декриптиране. Декриптирането на съобщенията се осъществява, като се прилагат аналогични правила съгласно зависимостите в таблица 2.

С цел по-лесно асимилиране на преподавания материал от студентите, софтуерният инструмент позволява да се визуализира в графичен прозорец принципа на действие на

шифъра DIGRAFID, прилаган в процеса на криптиране. Картинка, илюстрираща принципа на действие на шифъра DIGRAFID, е показана на фигура 4.



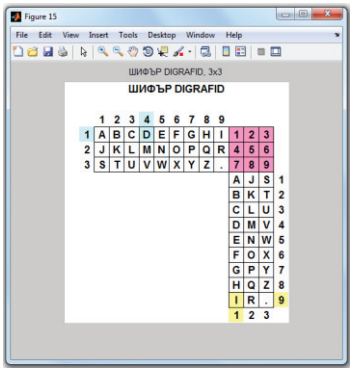
а) Хоризонтална ключова дума

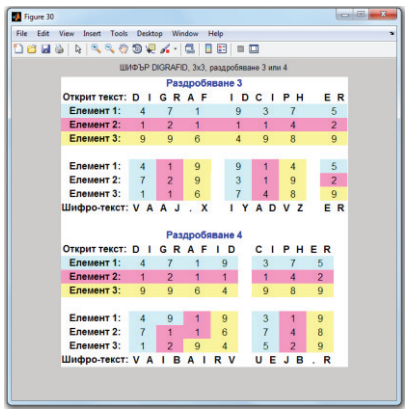


б) Вертикална ключова дума

Фиг. 3. Модул 1 „Генериране на ключа”

Процесът на криптиране започва с избора на хоризонтални и вертикални ключови думи. Те се използват за създаване на матриците, необходими за осъществяване на криптирането. Изборът се извършва чрез меню (фиг. 3), което съдържа четиринадесет ключови думи. Фиг. 3 показва матриците на хоризонталната ключова дума PLAINTEXT (фиг. 3 а) и вертикалната ключова дума CIPHERTEXT (фиг. 3 б). Буквите в синьо са буквите на ключовата дума. След тях се допълват останалите букви на английската азбука.





Фиг. 4. Принцип на действие при използване на шифър digrafid

Алгоритъмът за криптиране на английски текстове, използвайки шифъра DIGRAFID, реализиран в разработения скрипт, съдържа следните стъпки:

1. Избор на хоризонтална и вертикална ключови думи от меню за съставяне на матриците (фиг. 3). Създадените матрици се съхраняват в променливите MA и MB.

2. Въвеждане на открития текст на английски език от клавиатурата с възможност за интервали; откритият текст се съхранява в променливата s.

3. След това откритият текст се обработва в три етапа: 1) елиминиране на интервалите в открития текст (Обработка 1); 2) преобразуване на малките букви в главни в открития текст (Обработка 2); 3) вмъкване на нов символ, ако е необходимо – ако броят на символите в открития текст е нечетно число, в края на низа се вмъква символът „.” за възможността за разделяне на символите на текста на диграфи (Обработка 3). Процесът на криптиране се изпълнява, използвайки зависимостите в таблица 1.

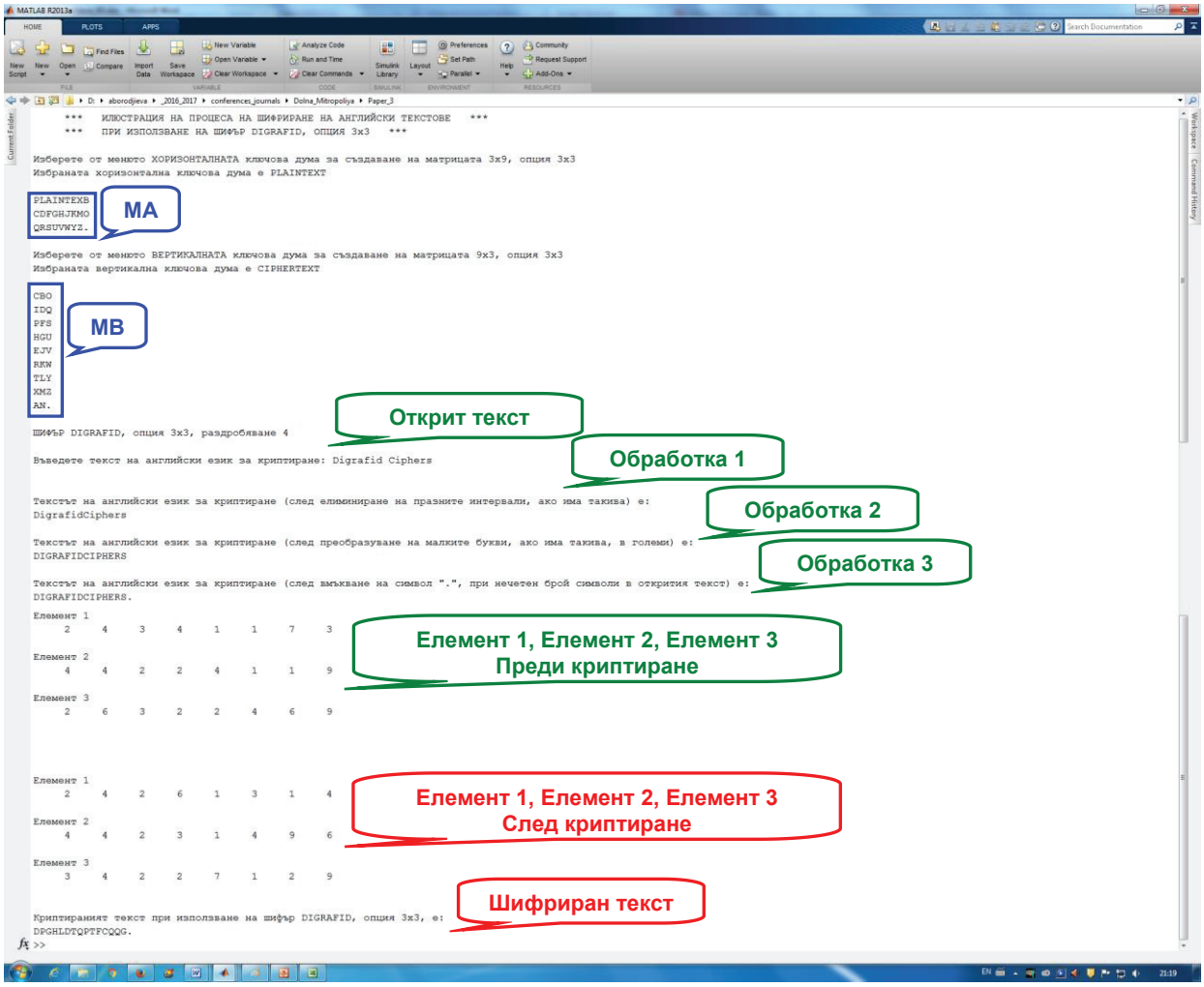
4. Криптиране на обработения текст. Определяне на елементите на символите в открития текст: Елемент 1, Елемент 2 и Елемент 3.

Таблица 1. Зависимости, използвани при криптирането

Случай	Преди трансформацията (преди криптиране)	След трансформацията (след криптиране)	Забележка
3x3 (3x9, 9x3)			
I	$\begin{pmatrix} E1_1 & E1_2 & E1_3 & E1_4 \\ E2_1 & E2_2 & E2_3 & E2_4 \\ E3_1 & E3_2 & E3_3 & E3_4 \end{pmatrix}$	$\begin{pmatrix} E1_1 & E1_4 & E2_3 & E3_2 \\ E1_2 & E2_1 & E2_4 & E3_3 \\ E1_3 & E2_2 & E3_1 & E3_4 \end{pmatrix}$	раздробяване 4 (цели блокове)
II	$\begin{pmatrix} E1_1 & E1_2 & E1_3 \\ E2_1 & E2_2 & E2_3 \\ E3_1 & E3_2 & E3_3 \end{pmatrix}$	$\begin{pmatrix} E1_1 & E2_1 & E3_1 \\ E1_2 & E2_2 & E3_2 \\ E1_3 & E2_3 & E3_3 \end{pmatrix}$	раздробяване 4 (частични блокове) раздробяване 3 (частични блокове)
III	$\begin{pmatrix} E1_1 & E1_2 \\ E2_1 & E2_2 \\ E3_1 & E3_2 \end{pmatrix}$	$\begin{pmatrix} E1_1 & E2_2 \\ E1_2 & E3_1 \\ E2_1 & E3_2 \end{pmatrix}$	раздробяване 4 (частични блокове) раздробяване 3 (частични блокове)
IV	$\begin{pmatrix} E1_1 \\ E2_1 \\ E3_1 \end{pmatrix}$	$\begin{pmatrix} E1_1 \\ E2_1 \\ E3_1 \end{pmatrix}$	раздробяване 4 (частични блокове) раздробяване 3 (частични блокове)

5. Визуализиране на криптирания текст, съхраняван в стринговата променлива scr.

Фиг. 5 илюстрира процеса на криптиране на английския текст Digrafid Ciphers, съдържащ малки и главни букви, и интервали, използвайки шифър DIGRAFID, раздробяване 4, хоризонтална ключова дума: PLAINTEXT, вертикална ключова дума: CIPHERTEXT.



Фиг. 5. Криптиране на английски текст чрез шифър DIGRAFID, раздробяване 4
Хоризонтална ключова дума: PLAINTEXT, Вертикална ключова дума: CIPHERTEXT,
Открит текст: Digrafid Ciphers; Криптиран текст: DPGHLDTQPTFCQQG.

Декриптирането на съобщенията се осъществява, като се прилагат обратните правила, използвани в процеса на криптиране.

Алгоритъмът за декриптиране на текстове на английски език, използвайки шифър DIGRAFID, реализиран в скрипта на MATLAB, включва следните стъпки:

1. Избор на хоризонтална ключова дума и вертикална ключова дума от меню с ключови думи за съставяне на матриците (фиг. 3).

2. Въвеждане на шифрирания текст на английски език от клавиатурата с възможност за интервали; шифрираният текст се съхранява в променливата s.

3. След това шифрираният текст се обработва в три етапа: 1) елиминиране на интервалите в шифрирания текст (Обработка 1); 2) преобразуване на малките букви в главни в шифрирания текст (Обработка 2); 3) вмъкване на нов символ, ако е необходимо – ако броят на символите в шифрирания текст е нечетно число, в края на низа се вмъква символът „.” за възможността за разделяне на символите на текста на диграфи (Обработка 3).

4. Декриптиране на обработения текст, като се прилагат обратните правила, използвани в процеса на криптиране. Процесът на декриптиране се изпълнява, като се използват зависимостите в таблица 2.

5. Визуализиране на декриптирания текст, съхранен в низовата променлива sdcr.

Някои резултати при използване на шифъра DIGRAFID с хоризонтална ключова дума PLAINTEXT и вертикална ключова дума CIPHERTEXT са дадени в таблица 3.

Таблица 2. Зависимости, използвани при декриптирането

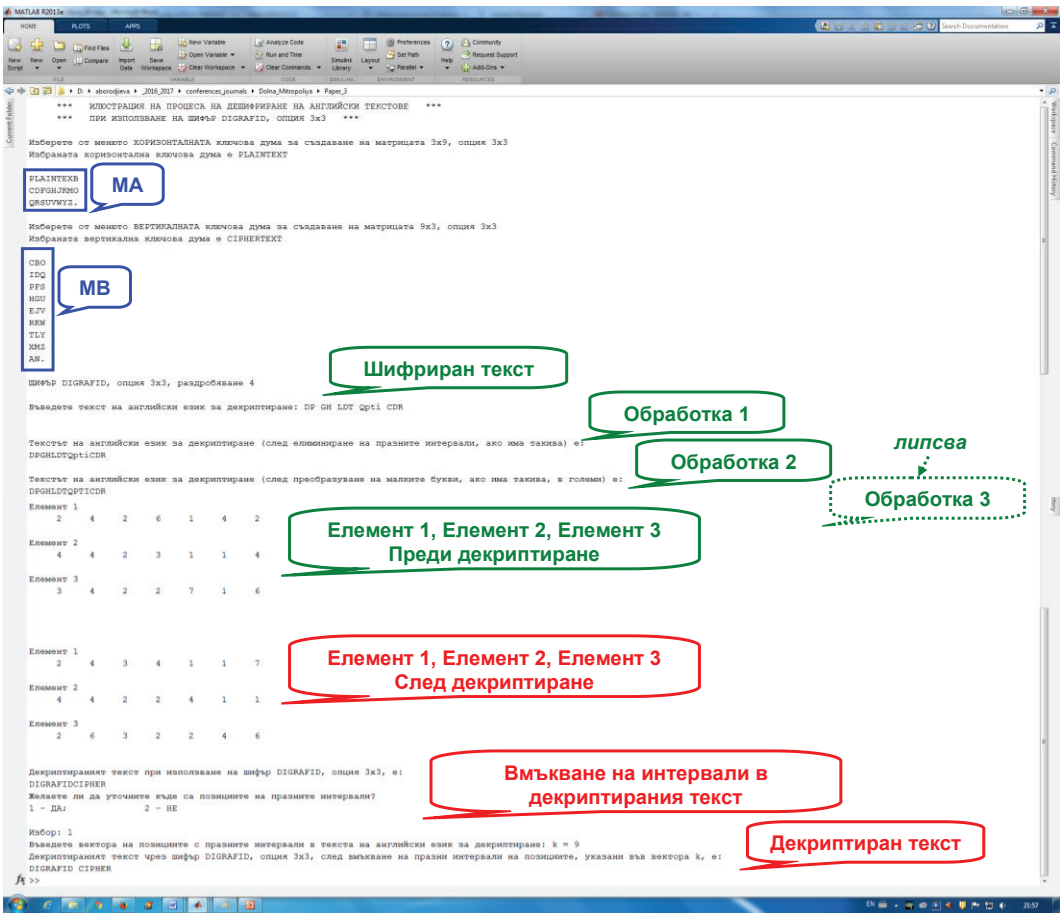
Случай	Преди трансформацията (преди декриптиране)	След трансформацията (след декриптиране)	Забележка
3x3 (3x9, 9x3)			
I	$\begin{pmatrix} E1_1 & E1_2 & E1_3 & E1_4 \\ E2_1 & E2_2 & E2_3 & E2_4 \\ E3_1 & E3_2 & E3_3 & E3_4 \end{pmatrix}$	$\begin{pmatrix} E1_1 & E2_1 & E3_1 & E1_2 \\ E2_2 & E3_2 & E1_3 & E2_3 \\ E3_3 & E1_4 & E2_4 & E3_4 \end{pmatrix}$	раздробяване 4 (цели блокове)
II	$\begin{pmatrix} E1_1 & E1_2 & E1_3 \\ E2_1 & E2_2 & E2_3 \\ E3_1 & E3_2 & E3_3 \end{pmatrix}$	$\begin{pmatrix} E1_1 & E2_1 & E3_1 \\ E1_2 & E2_2 & E3_2 \\ E1_3 & E2_3 & E3_3 \end{pmatrix}$	раздробяване 4 (частични блокове) раздробяване 3 (частични блокове)
III	$\begin{pmatrix} E1_1 & E1_2 \\ E2_1 & E2_2 \\ E3_1 & E3_2 \end{pmatrix}$	$\begin{pmatrix} E1_1 & E2_1 \\ E3_1 & E1_2 \\ E2_2 & E3_2 \end{pmatrix}$	раздробяване 4 (частични блокове) раздробяване 3 (частични блокове)
IV	$\begin{pmatrix} E1_1 \\ E2_1 \\ E3_1 \end{pmatrix}$	$\begin{pmatrix} E1_1 \\ E2_1 \\ E3_1 \end{pmatrix}$	раздробяване 4 (частични блокове) раздробяване 3 (частични блокове)

Таблица 3. Резултати при криптиране и декриптиране при използване на шифъра DIGRAFID

Открит текст	Криптиран текст	Декриптиран текст	Случай
3x3, раздробяване 3			
Cryptography	QRUPTOIVIRTY	CRYPTOGRAPHY	II
Applied Cryptography	AHPBSELBUOQTBBVCUUY.	APPLIEDCRYPTOGRAPHY.	III
Course in Applied Cryptography	CPWTCVIOLIBYIDCANTQQCLKAQCOA	COURSEINAPPLIEDCRYPTOGRAPHY.	IV
3x3, раздробяване 4			
Digrafid Ciphers	DPGHLDTQPTFCQQG.	DIGRAFIDCIPHERS.	I
Questions	QR.SCGANS.	QUESTIONS.	II
Cryptography	QRGTFRARFBTY	CRYPTOGRAPHY	III
Digrafid Cipher	DPGHLDTQPTICDR	DIGRAFIDCIPHER	IV

Фиг. 6 илюстрира процеса на декриптиране на шифриран текст (на английски език) DP GH LDT Qpti CDR, съдържащ малки и главни букви, и интервали, чрез шифър DIGRAFID, раздробяване 4, хоризонтална ключова дума: PLAINTEXT, вертикална ключова дума: CIPHERTEXT.

Приложението, разработено за дешифриране на английски текстове, позволява на потребителя, ако желае, да укаже позициите на празните интервали. В командния прозорец се появява меню за избор с две опции. В този случай потребителят избира първия вариант ("1") и въвежда вектора на позициите на интервалите на английски език за дешифриране: k = 9. Декриптираният текст, след вмъкване на интервалите, посочени в вектора k, е: DIGRAFID CIPHER.



Фиг. 6. Декриптиране на английски текст чрез шифър DIGRAFID, раздробяване 4
Хоризонтална ключова дума: PLAINTEXT, Вертикална ключова дума: CIPHERTEXT,
Криптиран текст: DP GH LDT Qpti CDR; Декриптиран текст: DIGRAFID CIPHER (k = 9)

ИЗВОДИ

В публикацията се описва един от прилаганите в класическата криптография шифър DIGRAFID. Представено е в детайли MATLAB-базирано приложение, реализиращо процесите на криптиране и декриптиране на английски текстове с шифър DIGRAFID, с раздробяване 3 и 4. Илюстрирани са процесите на криптиране и декриптиране на думи и изрази на английски език, като са представени множество примери, получени чрез разработеното приложение.

Материалът намира приложение в учебния процес по дисциплината „Телекомуникационна сигурност”, включена като задължителна в учебния план на специалност „Телекомуникационни системи”, образователно-квалификационна степен „Бакалавър”, при Русенски университет „Ангел Кънчев”, но може да се прилага и в други дисциплини, засягащи криптографските методи за защита на информацията.

Бъдещата работа по темата предвижда модифициране на алгоритъма и на разработеното MATLAB-базирано приложение с цел реализиране на процесите на криптиране и декриптиране на английски и/или български текстове с шифър DIGRAFID, с раздробяване 3 и 4, и с произволно раздробяване, както и с по-голям брой на символите в използваната азбука.

REFERENCES

Classical cipher. https://en.wikipedia.org/wiki/Classical_cipher (Accessed on 19.09.2017).

Digrafid Cipher. http://www.thonky.com/kryptos/digrafid-cipher (Accessed on 19.09.2017).

Digrafid Cipher. http://www.cryptogram.org/downloads/aca.info/ciphers/Digrafid.pdf (Accessed on 19.09.2017).