Обучаващ модул с графичен потребителски интерфейс за криптиране и декриптиране при използване на двутаблични вертикални и хоризонтални шифри, базирани на шифъра на Playfair

Пламен Маноилов, Адриана Бороджиева

Abstract: Training Module with Graphical User Interface for Encrypting and Decrypting Using Two-Square Vertical and Horizontal Ciphers Based on Playfair Cipher: *The paper describes the developed training module with graphical user interface for encryption and decryption of texts in English or Bulgarian, which will be used in the course "Telecommunications Security" included as compulsory in the curriculum of the specialty "Telecommunication Systems" for the "Bachelor" educational qualification degree in University of Ruse "Angel Kanchev". The training module is implemented using MATLAB and GUIDE.*

Key words: *Encryption, decryption, two-square ciphers, graphical user interface, MATLAB, GUIDE.*

ВЪВЕДЕНИЕ

През 1854 г. английският физик Wheatstone описва специален субституционен шифър. Неговият приятел, Playfair, препоръчва шифъра на висши правителствени и военни чиновници. Днес този шифър е известен като шифър на Playfair. За пръв път е използван през Кримската война. През Първата световна война все още намира приложение в британската армия, но от средата на 1915 г. немските криптаналитици го разбиват безпроблемно. Модифициран вариант на Playfair (т.нар. двутабличен Playfair) се използва за някои части на немската армия в Африка чак до есента на 1944 г. Обект на изследване в публикацията са именно двутабличните шифри, базирани на шифъра на Playfair [1].

Двутабличният шифър на Playfair е разработен за облекчаване на процесите на криптиране/декриптиране на дълги текстове при използване на четиритабличен шифър. Техниката криптира двойки букви (диграфи) и по такъв начин попада в категорията на шифрите, известни като полиграфни субституционни шифри. Те добавят значителна мощ за криптирането, в сравнение с монографните субституционни шифри, които обработват единични символи. Използването на диграфи прави двутабличните шифри по-неподатливи на атаки на честотния анализ, тъй като анализът трябва да се направи върху 676 възможни диграфа, а не само върху 26 символа за монографното заместване. Честотният анализ на диграфи е възможен, но значително по-труден, и обикновено изисква по-дълъг шифриран текст, за да е ефективен [2].

Двутабличният шифър има две разновидности – вертикална и хоризонтална. Вертикалната се състои от две разположени една над друга матрици с размерност 5 x 5, а хоризонталната – от две разположени една до друга матрици. Всяка една от матриците съдържа буквите от английската азбука (обикновено се пропуска буквата "Q" или буквите "I" и "J" се разполагат в една и съща клетка, с цел намаляване на азбуката, за да се побере в матрицата с размерност 5 x 5). За българската азбука се използват матрици с размерност 6 x 5 (или 5 x 6). За да се генерират „квадратите", в клетките на матрицата първо се попълват буквите на дадена ключова дума или фраза (като отпадат дублиращите се букви), след което се попълват останалите клетки с останалите букви от азбуката по азбучен ред. Ключът може да бъде написан в първите редове от таблицата, от ляво на дясно, или по някакъв друг модел. Ключовата дума, заедно с правилата за попълване на матрицата, представлява ключът на шифъра. Алгоритъмът на двутабличния шифър дава възможност за използване на два отделни ключа, по един за всяка от двете матрици. Използването на ключова дума при създаването на матриците облекчава прилагането на шифъра, но намалява неговата сигурност [2]. При шифрирането на текст с използване на двутаблични шифри се спазват следните правила:

• За вертикалните двутаблични шифри първата буква от диграфа на открития текст се намира в горната матрица, а втората буква от диграфа – в долната.

• За хоризонталните двутаблични шифри първата буква от диграфа на открития текст се намира в лявата матрица, а втората буква от диграфа – в дясната.

• След като се намерят символите на диграфа на открития текст, се образува правоъгълник. В противоположните му ъгли се намира диграфът на криптирания текст.

• При вертикалните шифри, когато двете букви от диграфа в открития текст са в една и съща колона, в криптирания текст се записва същият диграф. За хоризонталните шифри, когато двете букви от диграфа в открития текст са в един и същ ред, буквите от диграфа в шифрирания текст се записват в обратен ред. В областта на криптографията това се нарича прозрачност. Слабост на двутабличните шифри е, че около 20 % от диграфите ще бъдат прозрачни [2].

В [3] са представени разработени скриптове на MATLAB, които позволяват шифрирането и дешифрирането на текстове на английски или български език чрез двутаблични и четиритаблични шифри, базирани на шифъра на Playfair. В [4] се описва обучаващ модул с графичен потребителски интерфейс, с който е илюстрирано действието на приложението за четиритаблични шифри. В тази публикация се представя неговото функциониране за шифрирането и дешифрирането на текстове на английски или български език чрез двутаблични вертикални и хоризонтални шифри, базирани на шифъра на Playfair.

ОБУЧАВАЩ МОДУЛ С ГРАФИЧЕН ПОТРЕБИТЕЛСКИ ИНТЕРФЕЙС ЗА КРИПТИРАНЕ И ДЕКРИПТИРАНЕ С ИЗПОЛЗВАНЕ НА ДВУТАБЛИЧНИ ШИФРИ, БАЗИРАНИ НА ШИФЪРА НА PLAYFAIR

Обучаващият модул с графичен потребителски интерфейс за криптиране и декриптиране с използване на двутаблични и четиритаблични шифри, базирани на шифъра на Playfair, е реализиран в MATLAB и средата за разработване на графични потребителски интерфейси GUIDE (Graphical User Interface Development Environment). На фиг. 1 е показан външният вид на обучаващия модул с графичен потребителски интерфейс. Неговата функционалност е описана по-долу чрез пример на двутабличен вертикален шифър.

Обучаващият модул съдържа в горната си част четири панела: 1) за избор на език за шифриране и/или дешифриране на текстове между двете опции български и английски (фиг. 1, блок 1); 2) за избор на шифъра за шифриране и/или дешифриране между двете опции двутабличен и четиритабличен (фиг. 1, блок 2); 3) за избор на разновидността на прилагания двутабличен шифър между двете опции вертикална и хоризонтална (фиг. 1, блок 3); селектираната опция в този панел е от значение само при избран двутабличен шифър; 4) за избор на двата ключа за построяване на „квадратите" на шифрирания текст, като изборът се извършва въз основа на падащи менюта с 14 опции за избор (фиг. 1, блок 4). Обучаващият модул предлага постъпково шифриране и дешифриране с цел по-лесно усвояване на преподавания материал от студентите.

Алгоритъмът за *шифриране на текстове на английски/български език* чрез двутабличен шифър, базиран на шифъра на Playfair, заложен в разработения обучаващ модул (фиг. 1, панел „КРИПТИРАНЕ"), съдържа следните стъпки:

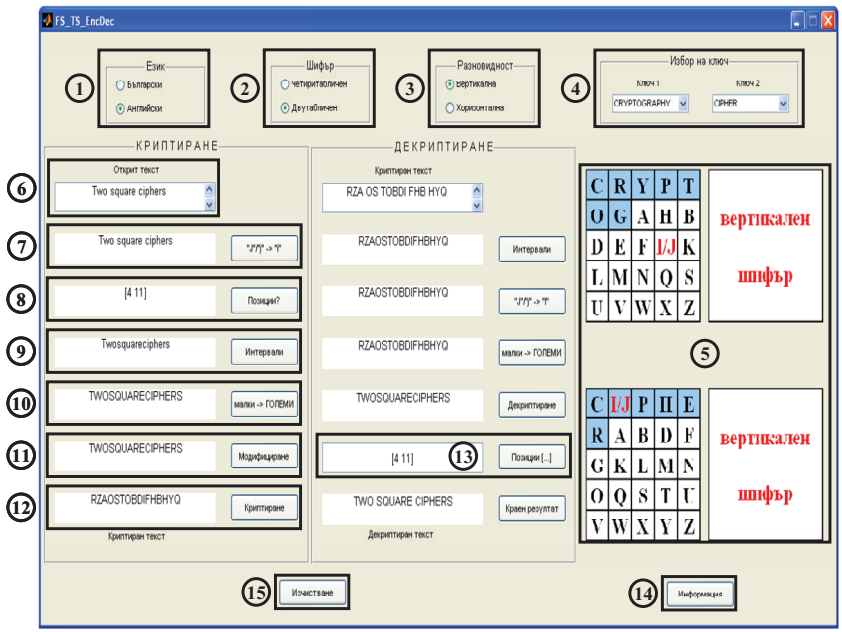
1. Избор от меню (фиг. 1, блок 4) на ключова дума за съставяне на първия квадрат (горен за вертикалния вариант и ляв за хоризонталния вариант). Създадената матрица на първия квадрат се съхранява в променливата MA1.

2. Избор от меню (фиг. 1, блок 4) на ключова дума за съставяне на втория квадрат (долен за вертикалния вариант и десен за хоризонталния вариант). Създадената матрица на втория квадрат се съхранява в променливата MA2.

3. Извеждане на матриците MA1 и MA2 в графичните оси на приложението (фиг. 1, блок 5), като MA1 и MA2 се извеждат една под друга за вертикалния вариант и една до друга за хоризонталния вариант.

4. Въвеждане от клавиатурата на текста за криптиране (открития текст) в текстовото поле на английски/български език (фиг. 1, блок 6) с възможност за празни интервали между думите, който ще се съхранява в стринговата променлива *s*.

5. Претърсване на стринговата променлива *s* за наличието на буквите "*J*" и "*J*", и заменянето им с буквата "*I*", организирано чрез цикъл по отношение на променливата *i* = 1:*length*(*s*), където *length*(*s*) определя дължината на стринга *s*. При този цикъл се прави проверка дали *s*(*i*) = '*j*' или *s*(*i*) = '*J*', и ако това условие е изпълнено, тогава се извършва субституцията *s*(*i*) = '*i*'. Тази обработка на текста се активира при натискането на бутона "j"/"J" -> "i" и е налична само за текстове на английски език. Резултатът се извежда в съответното текстово поле (фиг. 1, блок 7).



Фигура 1. Външен вид на обучаващия модул с графичен потребителски интерфейс

6. Откриване на позициите в стринговата променлива *s*, където има празни интервали. Тези позиции се съхраняват във вектор-ред *k*, на който първоначално е присвоено празно множество. Тази операция отново се организира чрез цикъл по отношение на променливата *i* = 1:*length*(*s*), където *length*(*s*) определя дължината на стринга *s*. При този цикъл се прави проверка дали *s*(*i*) = ' ' (интервал) и ако това условие е изпълнено, тогава векторът *k* се допълва с номера на поредния интервал (*i*) чрез инструкцията *k* = [*k i*]. Тази обработка на текста се активира при натискането на бутона „Позиции?", а резултатът под формата на вектора *k* се извежда в съответното текстово поле (фиг. 1, блок 8).

7. Елиминиране на празните интервали в стринга *s*. За съхраняване на междинните резултати от тази операция се използва стринговата променлива *str*, чиято първоначална стойност е празен стринг: *str* = [' ']. Впоследствие в нея се записва

частта от стринга *s*, до мястото на първата позиция с интервал: *str* = *strcat*(*str*,*s*(1:*k*(1))). Следва натрупване на частите от стринга *s*, между позициите на първия и втория интервал, между позициите на втория и третия интервал и т.н. (между позициите на предпоследния и последния интервал), като се елиминират всички празни интервали в стринга. Това отново се организира чрез цикъл по отношение на променливата *i* = 1:*length*(*k*)-1, където *k* е вектор-ред, съдържащ позициите на празните интервали в *s*: *str* = *strcat*(*str*,*s*((*k*(*i*)+1):(*k*(*i*+1)-1))). И накрая, трябва да се натрупат крайните символи на стринга *s* след позицията на последния интервал, като резултатът се съхранява отново в стринговата променлива *s*, и се реализира чрез реда: *s* = *strcat*(*str*,*s*((*k*(*length*(*k*))+1):*length*(*s*))). Тази обработка на текста се активира при натискането на бутона „Интервали", а резултатът се извежда в съответното текстово поле (фиг. 1, блок 9).

8. Преобразуване на малките букви, ако има такива, в големи, чрез инструкцията *upper* и съхраняване на резултата отново в променливата *s*. Тази обработка на текста се активира при натискането на бутона „малки->ГОЛЕМИ", а резултатът се извежда в съответното текстово поле (фиг. 1, блок 10).

9. Модифициране на текста за криптиране (ако е нужно). За целта се проверява дали броят на символите в текста за криптиране (след елиминирането на празните интервали) е нечетен: *mod*(*length*(*s*),2) = 1. Ако условието е изпълнено, в края на стринга *s* се прибавя някоя от нискочестотните букви в английския език, в случая буквата '*Z*': *s* = *strcat*(*s*,'*Z*'); за текстове на български език е предвидено въвеждането на нискочестотната буква *'Ь'*. Тази обработка на текста се активира при натискането на бутона „Модифициране", а резултатът се извежда в съответното текстово поле (фиг. 1, блок 11).

10. Криптиране на обработения текст с използване на двутаблични шифри, базирани на шифъра на Playfair. В случая, стрингът *s* се разделя на двубуквени блокове. За всяка двойка символи се определят реда *ra* и колоната *ca*, в които се намира *i*-тият символ на стринга в матрицата MA1, и реда *rb* и колоната *cb*, в които се намира (*i* + 1)-вият символ на стринга в матрицата MA2 чрез инструкцията *find*. Криптирането на диграфите на открития текст се извършва за всяко *i* = 1:2:*length*(*s*)-1 чрез инструкциите:

- при вертикален вариант:

ra_n = *ra*; *ca_n* = *ca*; *rb_n* = *rb*; *cb_n* = *cb* (при *ca* = *cb*);
ra_n = *ra*; *ca_n* = *cb*; *rb_n* = *rb*; *cb_n* = *ca* (при *ca* ~= *cb*);

- при хоризонтален вариант:

ra_n = *rb*; *ca_n* = *cb*; *rb_n* = *ra*; *cb_n* = *ca* (при *ra* = *rb*);
ra_n = *rb*; *ca_n* = *ca*; *rb_n* = *ra*; *cb_n* = *cb* (при *ra* ~= *rb*).

В тези инструкции с *ra_n* и *ca_n* са означени съответно реда и колоната на първия символ в шифрирания текст, а с *rb_n* и *cb_n* – реда и колоната на втория символ в шифрирания текст. Шифрираните символи се вземат от указаните редове и колони съответно в матриците MA1 и MA2:

- при вертикален вариант:

scr = *strcat*(scr,*MA*1(*ra_n*,*ca_n*),*MA*2(*rb_n*,*cb_n*));

- при хоризонтален вариант:

scr = *strcat*(*scr*,*MA*2(*ra_n*,*ca_n*),*MA*1(*rb_n*,*cb_n*)); при *ra* = *rb*;
scr = *strcat*(*scr*,*MA*2(*rb_n*,*cb_n*),*MA*1(*ra_n*,*ca_n*)); при *ra* ~= *rb*.

Междинните резултати се съхраняват в променливата *scr*, която съдържа и крайния резултат от шифрирането на английския/българския текст. Тази обработка на текста се активира при натискането на бутона „Криптиране", а резултатът (криптираният текст), съхранен в стринговата променлива *scr*, се извежда в съответното текстово поле (фиг. 1, блок 12).

По аналогичен начин могат да се опишат алгоритмите за дешифриране чрез двутаблични шифри.

В [3] са дадени блок-схеми на алгоритми, реализиращи обработката при шифрирането и дешифрирането на български и английски текстове.

На фиг. 1 е приложена снимка на разработения обучаващ модул. Избран е текст за шифриране *Two square ciphers* (три думи, разделени с интервал) и ключовите думи *CRYPTOGRAPHY* и *CIPHER* за съставяне на матриците на шифрирания текст при използване на двутабличен вертикален шифър, базиран на шифър на Playfair. Впоследствие полученият шифриран текст *RZAOSTOBDIFHBHYQ* се дешифрира чрез панела „ДЕКРИПТИРАНЕ" (фиг. 1), при което се получава декриптиран текст, съвпадащ с използвания открит текст. В този панел е предвидена опция за задаване на вектора *k* (фиг. 1, блок 13), указващ позициите на празните интервали (например, между думите в израз или изречение), които се отстраняват в процеса на шифриране.

Предвидена е възможност в отделен графичен прозорец да се извежда информация относно прилагания шифър и илюстрация на принципа на действие на шифъра, при желание от страна на потребителя [4]. Тази опция се активира при натискането на бутон „Информация" (фиг. 1, блок 14). Съществува възможност и за изчистване на полетата на панелите „КРИПТИРАНЕ" и „ДЕКРИПТИРАНЕ" при натискане на бутон „Изчистване" (фиг. 1, блок 15).

ЗАКЛЮЧЕНИЕ

В публикацията се описва обучаващ модул с графичен потребителски интерфейс, предназначен за шифриране и дешифриране на текстове на български и английски език с използване на двутаблични хоризонтални и вертикални шифри, базирани на шифъра на Playfair. Модулът ще намира приложение в учебния процес по дисциплината „Телекомуникационна сигурност", включена като задължителна в учебния план на специалност „Телекомуникационни системи", за образователно-квалификационна степен „Бакалавър", в Русенски университет „Ангел Кънчев". С разработения обучаващ модул се цели повишаване на интереса на студентите, изучаващи дисциплината. Процесите на шифриране и дешифриране се реализират постъпково, с цел по-лесно усвояване и осмисляне на материала от студентите.

ЛИТЕРАТУРА

[1] Playfair cipher, http://en.wikipedia.org/wiki/Playfair_cipher

[2] Two-square cipher, http://en.wikipedia.org/wiki/Two-square_cipher

[3] Borodzhieva, A. Software Tool for Implementing Encryption and Decryption Processes Using Classical Ciphers. International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE-2012), 5 – 6 October 2012, University of National and World Economy, Conference Proceedings, Sofia, Bulgaria, pp. 458 – 463.

[4] Бороджиева, А. Обучаващ модул с графичен потребителски интерфейс за криптиране и декриптиране с използване на двутаблични и четиритаблични шифри, базирани на шифъра на Playfair. XXI международна научна конференция „Транспорт 2013", организирана от Висше транспортно училище „Тодор Каблешков", 10 – 13 октомври 2013 г., Варна, курортен комплекс „Св. св. Константин и Елена", Academic journal "Mechanics, Transport, Communications", Volume 11, Issue 3/2013, Part 3, PhD Student Session, pp. DS-196 – DS-202, ISSN: 1312-3823.

За контакти:

Доц. д-р Пламен Маноилов, Катедра „Информатика и информационни технологии", Русенски университет „Ангел Кънчев", тел.: 082-888 646, e-mail: pmanoilov@ecs.uni-ruse.bg.

Гл. ас. д-р Адриана Бороджиева, Катедра „Телекомуникации", Русенски университет „Ангел Кънчев", тел.: 082-888 734, e-mail: aborodjieva@ecs.uni-ruse.bg.