Механика Транспорт Комуникации

Научно списание

ISSN 1312-3823

том 11, брой 3, 2013 г.

статия № 0869

http://www.mtc-aj.com

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

Адриана Бороджиева
aborodjieva@ecs.uni-ruse.bg

Русенски университет „Ангел Кънчев”, 7017 Русе, ул. „Студентска” № 8 БЪЛГАРИЯ

Ключови думи: *Криптиране, декриптиране, двутаблични и четиритаблични шифри, графичен потребителски интерфейс, MATLAB, GUIDE.*

Резюме: *В публикацията се описва разработен обучаващ модул с графичен потребителски интерфейс за криптиране и декриптиране на текстове на английски или български език, който ще намира приложение в учебния процес по дисциплината „Телекомуникационна сигурност”, включена като задължителна в учебния план на специалност „Телекомуникационни системи”, за образователно-квалификационната степен „бакалавър”, в Русенски университет „Ангел Кънчев”. Обучаващият модул е реализиран чрез MATLAB и средата за разработване на графични потребителски интерфейси GUIDE. Приложението позволява при избор от падащо меню на ключови думи за построяване на „квадратите” на шифрирания текст, да се илюстрират процесите на криптиране/декриптиране на открит/шифриран текст, въведен в текстово поле от потребителя, при използване на двутаблични или четиритаблични шифри, базирани на шифъра на Playfair. В графичния прозорец се извеждат „квадратите” въз основа на които се осъществява криптирането/декриптирането. Реализирани са и двете разновидности на двутабличните шифри – хоризонтална и вертикална. 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. С разработения обучаващ модул се цели повишаване на интереса на студентите, изучаващи дисциплината „Телекомуникационна сигурност”.*

ВЪВЕДЕНИЕ

През 1854 г. английският физик Charles Wheatstone описва специален субституционен шифър. Приятелят на Wheatstone, Lyon Playfair, препоръчва шифъра на висши правителствени и военни чиновници. Днес този шифър е известен като шифър на Playfair. За пръв път той е използван през Кримската война. През Първата световна война все още намира приложение в британската армия, но от средата на 1915 г. немските криптаналисти 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 и четиритабличните шифри, базирани на шифъра на Playfair [1].

Двутабличният шифър на Playfair е разработен за облекчаване на процесите на криптиране/декриптиране на дълги текстове, вместо използването на четиритабличен шифър, описан по-долу. 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 суб¬сти¬ту¬ционни шифри, които обработват единични символи. Използването на ди¬графи 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 много по-голям шифриран текст, за да бъде полезен [2].

Двутабличният шифър има две разновидности – хоризонтална и вертикална. Вертикалната се състои от две матрици, като всяка една от тях съдържа по 5 реда и по 5 стълба, а матриците са разположени една над друга. Хори¬зон¬талната също се състои от две матрици, като всяка една от тях съдържа по 5 реда и по 5 стълба, но матриците са разположени една до друга. 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 6 реда и 5 стълба (или 5 реда и 6 стълба). За да се генерират „квадратите”, първо се попълват в клетките на матрицата 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 (пропуска се буквата “Q” или буквите “I” и “J” се разполагат в една и съща клетка за намаляване на английската азбука с цел да се побере в матрицата с размерност 5 x 5). Ключът може да бъде написан в първите редове от таблицата, от ляво на дясно, или по някакъв друг модел, например, като спирала, започваща в горния ляв ъгъл и завършваща в центъра. Ключовата дума, заедно с правилата за попълване на таблицата с размерност 5 x 5, представлява ключа на шифъра. Алгоритъмът на двутабличния шифър дава възможност за използване на два отделни ключа, по един за всяка от двете матрици на шифрирания текст. Използването на ключова дума при създаването на матриците облекчава прилагането на шифъра, но намалява неговата сигурност [2]. При шифрирането на текст с използването на двутаблични шифри се спазват следните правила:

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

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

♦ След като се намерят символите на диграфа на откритият текст, се образува правоъгълник, като в противоположните му ъгли се намира диграфът на криптирания текст.

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

Четиритабличният шифър на Playfair е аналогичен на двутабличния шифър на Playfair. Разликата е в това, че тук се използват четири матрици с размерност 5 x 5, подредени в квадрат. Като цяло, горната лява и долната дясна матрици са „квадратите на окрития текст" и всяка от тях съдържа „стандартната азбука". Горната дясна и долната лява матрици са „квадратите на шифрирания текст" и съдържат смесена последователност на буквите от азбуката [3]. За българската азбука се използват „квадрати" с размерност 6 x 5 или с размерност 5 x 6.

Алгоритъмът за криптиране съдържа следните стъпки:

♦Разделя се съобщението за криптиране на диграфи.

♦Намира се първата буква от диграфа в горната лява матрица на откритият текст.

♦Намира се втората буква от диграфа в долната дясна матрица на откритият текст.

♦Първата буква на криптирания диграф е в същия ред като първата буква на откритият текст и в същата колона като втората буква на откритият текст. Ето защо е в горната дясна матрица на шифрирания текст.

♦Втората буква на криптирания диграф е в същия ред като втората буква на откритият текст и в същата колона като първата буква на откритият текст. Ето защо е в долната лява матрица на шифрирания текст.

Методът на криптиране включва намирането на другите два ъгъла на правоъгълник, определен от двете букви в диграфа на откритият текст. Криптираният диграф са буквите в другите два ъгъла, като първо се изписва горната дясна буква.

Дешифрирането работи по същия начин, но в обратен ред. Диграфите на шифрирания текст се разделят, като първият символ „отива" в горната дясна матрица, а вторият символ – в долната лява матрица. След това се намират другите ъгли на правоъгълника. Те представляват диграфите на декриптирания текст, който съвпада с откритият текст, като първо се изписва елементът в горната лява матрица [3].

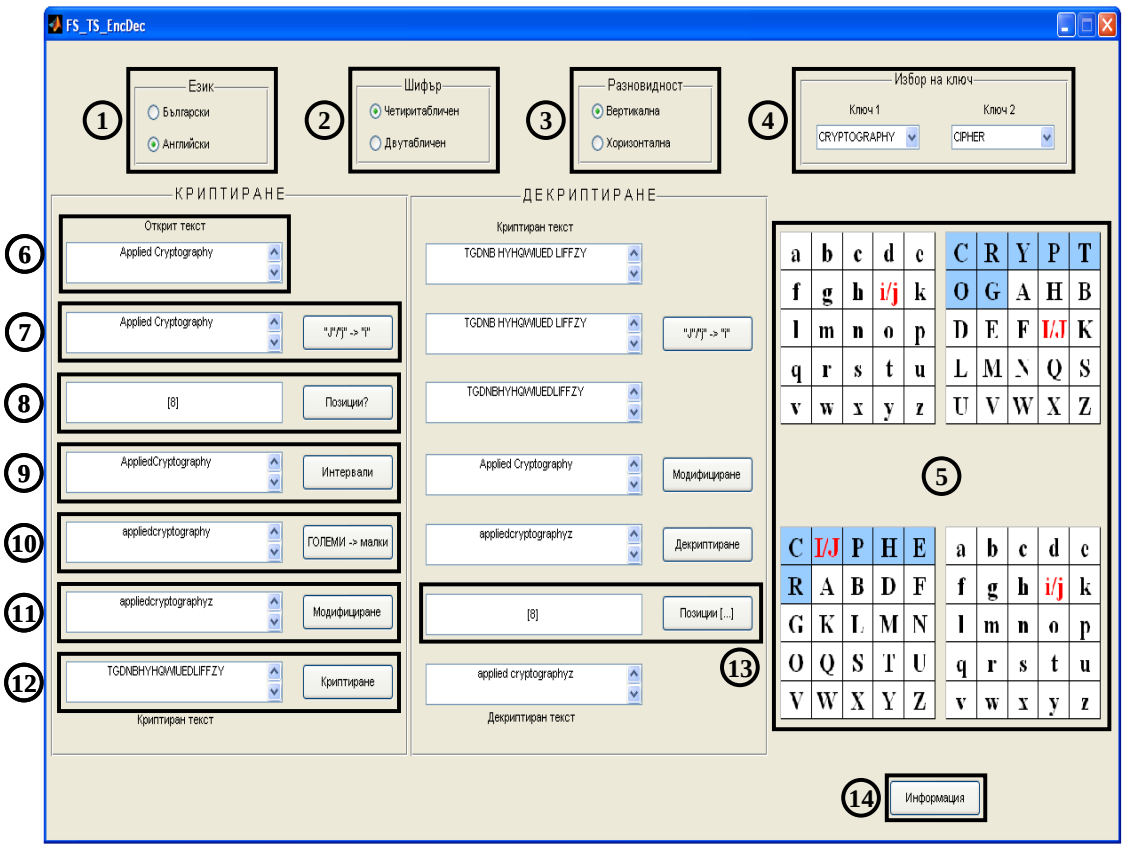
В [4] са представени разработени скриптове на MATLAB, които позволяват шифрирането и дешифрирането на текстове на английски или български език чрез двутаблични и четиритаблични шифри, базирани на шифъра на Playfair. В тази публикация се описва обучаващ модул с графичен потребителски интерфейс, който е предназначен за тази цел. Модулът ще намира приложение в учебния процес по дисциплината „Телекомуникационна сигурност", включена като задължителна в учебния план на специалност „Телекомуникационни системи", за образователно-квалификационната степен „бакалавър", в Русенски университет „Ангел Кънчев".

ОБУЧАВАЩ МОДУЛ С ГРАФИЧЕН ПОТРЕБИТЕЛСКИ ИНТЕРФЕЙС ЗА КРИПТИРАНЕ И ДЕКРИПТИРАНЕ С ИЗПОЛЗВАНЕ НА ДВУТАБЛИЧНИ И ЧЕТИРИТАБЛИЧНИ 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 чрез MATLAB и средата за разработване на графични потребителски интерфейси GUIDE (**G**raphical **U**ser **I**nterface **D**evelopment **E**nvironment). На фиг. 1 е показан външният вид на обучаващия модул с графичен потребителски интерфейс, като неговата функционалност е описана по-долу чрез примери.

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 страна на студентите.



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

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

1. Избор от меню на ключова дума за съставяне на втория (горен, десен) квадрат (фиг. 1, блок 4). Създадената матрица се съхранява в променливата MA2.

2. Избор от меню на ключова дума за съставяне на третия (долен, ляв) квадрат (фиг. 1, блок 4). Създадената матрица се съхранява в променливата MA3.

3. Дефиниране на матриците на открития текст, съдържащи „стандартната” английска азбука и съхранявани в променливите MA1 и MA4. Матриците MA1, MA2, MA3 и MA4 се извеждат в графичните оси на приложението (фиг. 1, блок 5).

4. Въвеждане от клавиатурата на текста за криптиране (откритият 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).

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*) = ' ' (празен интервал) и ако това условие е изпълнено, тогава векторът *k* се допълва с номера на поредния празен 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 празен интервал: *str* = *strcat*(*str*,*s*(1:*k*(1))). Следва натрупване на частите от стринга *s*, между позициите на първия и втория празен интервал, между позициите на втория и третия празен интервал и т.н. (между позициите на предпоследния и последния празен 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 стринга *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 празен интервал, като резултатът се съхранява отново в стринговата променлива *s*, и се реализира чрез командата: *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 големите букви, ако има такива, в малки, чрез инструкцията *lower* и съхраняване на резултата отново в променливата *s*. Тази обработка на текста се активира при натискането на бутона „ГОЛЕМИ->малки”, 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 четиритабличен шифър, базиран 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 MA4 чрез инструкцията *find*. Криптирането на диграфите на открития текст се извършва чрез инструкциите: *ra_n* = *ra*; *ca_n* = *cb*; *rb_n* = *rb*; *cb_n* = *ca*; за всяко *i* = 1:2:*length*(*s*)-1. 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 MA2 и MA3. Междинните резултати се съхраняват в променливата *scr*, която съдържа и крайният 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).

Трябва да се отбележи, че стъпките 5, 6, 7 и 8 могат да разменят местата си при софтуерната реализация на предложения алгоритъм. По аналогичен начин могат да се опишат алгоритмите за дешифриране чрез четиритабличен шифър, както и за шифриране и дешифриране на текстове чрез двутаблични шифри (в двете му разновидности).

В [4] могат да се намерят блок-схеми на алгоритмите, реализиращи обработката, която се извършва при шифрирането и дешифрирането на български и английски текстове.

На фиг. 1 е приложена снимка на разработения обучаващ модул, като е избран текст за шифриране *Applied Cryptography* (две думи, разделени с празен интервал) и ключовите думи *CRYPTOGRAPHY* и *CIPHER* за съставяне на матриците на шифрирания текст при използване на четиритабличен шифър, базиран на шифър на Playfair. Впоследствие полученият в резултат шифриран текст *TGDNBHYHQWIUEDLIFFZY* 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 един 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).

ЗАКЛЮЧЕНИЕ

В тази публикация се описва обучаващ модул с графичен потребителски интерфейс, който е предназначен за шифриране и дешифриране на текстове на български и английски език с използване на четиритаблични и двутаблични 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-квалификационната степен „бакалавър”, в Русенски университет „Ангел Кънчев”.С разработения обучаващ модул се цели повишаване на интереса на студентите, изучаващи дисциплината „Телекомуникационна сигурност”. Процесите на шифриране и дешифриране се реализират постъпково с цел по-лесното усвояване и осмисляне от студентите на преподавания материал, като те могат постъпково да проследяват етапите, а не само да визуализират резултатите от шифрирането/дещифрирането.

ЛИТЕРАТУРА:

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

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

[3] http://en.wikipedia.org/wiki/Four-square_cipher

[4] 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.

TRAINING MODULE WITH GRAPHICAL USER INTERFACE FOR ENCRYPTING AND DECRYPTING USING TWO-SQUARE AND FOUR-SQUARE CIPHERS BASED ON PLAYFAIR CIPHER

Adriana Borodzhieva
aborodjieva@ecs.uni-ruse.bg

University of Ruse "Angel Kanchev", 7017 Ruse, 8 Studentska Street
BULGARIA

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

Abstract: *This publication 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 (Graphical User Interfaces Development Environment). The application allows to choose keywords from the pop-menu for constructing the "squares" of the ciphertext, to illustrate the process of encryption/decryption of plaintext/cipher-text entered in the text box by the user using two-square or four-square ciphers based of Playfair cipher. The "squares" used for encryption/decryption are displayed in the graphical axes. Both varieties of the two-square ciphers are implemented – horizontal and vertical. There is an opportunity information about the applications of the ciphers as well as the principle of operation of the cipher to be displayed in a separate graphical window, if desired by the user. The developed training module aims to increase students' interest in studying the course "Telecommunication security".*