Web- базирана система за криптиране и декриптиране на блокови транспозиционни криптографски шифри

Виктория Рашкова

Abstract: Web-based Encryption and Decryption System for Block Transposition Cryptographic Ciphers: *Cryptography is the science that seeks to encrypt or decrypt text called plaintext. Encryption and decryption are designed to protect data from unauthorized access. With the development of information technology the need for the protection of personal user data increases. This paper presents a Web-based encryption and decryption system for various types of transposition ciphers. The system provides a short theoretical material for each type of cipher; allows encryption and decryption of multiple transposition ciphers with randomly introduced plaintext; key for encryption / decryption; allows use of ciphers with feature animation.*

Key words: *cryptography, plaintext, cryptography key, encryption, decryption, transposition, block cipher, key length.*

ВЪВЕДЕНИЕ

Информацията винаги е била и остава най-търсената и скъпа стока, което особено засяга съвременното информационно общество. Още в дълбока древност владетелите – императори, ханове, царе и др. са искали да защитят своята кореспонденция, в случай че тя попадне в ръцете на врага. Възниква проблемът със защитата на информацията. За решаването на този проблем древните хора са използвали разнообразни, макар и примитивни методи на защита, като: глинени табелки, върху които се е изписвало съобщението на слоеве; използвали са кодове, при които са означавали някои съгласни и гласни звуци със срички и др. Така възниква и науката криптография. Нейното значение идва от превод на гръцки език (kriptos- тайна и grafus- пиша), т.е. наука за тайнопис, целта на която е да се скрие съдържанието на текста [1]. С навлизането на компютърните комуникации и Internet, криптографията излезе от традиционните си приложения в разузнаването, военното дело и дипломацията и зае трайно място и в гражданския живот. Криптографските шифри кодират даден текст, наречен открит текст, в шифриран вид (шифротекст), използвайки криптографски ключ. Съществуват две основни категории симетрични блокови шифри- субституционни и транспозиционни. Транспозиционните шифри се характеризират с това, че за шифрирането на даден открит текст се използват същите символи, но се разместват в определен ред. Възможно е да се пренаредят отделните символи от открития текст или цели негови думи, но във втория случай нараства вероятността от разбиване на шифъра. При някои транспозиционни шифри процесът на разместване е еднократен (шифри с единична транспозиция). Други използват двоен процес на разместване (шифри с двойна транспозиция). В зависимост от вида на шифъра шифротекстът се извлича по различен начин. Целта на статията е да представи Web-базирана система за криптиране и декриптиране, фокусирайки се само върху транспозиционните криптографски шифри.

ВИДОВЕ ТРАНСПОЗИЦИОННИ ШИФРИ

Съществува голямо разнообразие от транспозиционни шифри, основните от които са:

• ***Зигзагообразен шифър на транспозиция (Rail Fence cipher)*** – при този шифър на транспозиция ключът определя броя на редовете, в които зигзагообразно се записва откритият текст. Броя на колоните зависи от дължината на открития текст. Шифротекстът се определя като се записват последователно всички символи по редове, започвайки от ляво надясно [4], [5]. На фиг. 1 е представен зигзагообразен шифър на транспозиция с открит текст: ТРАНСПОЗИЦИОНЕН

БЛОКОВ ШИФЪР и ключ с отместване 3. Полученият шифротекст е: ТСИНЛВЪРНПЗЦОЕБООШФРАОИНКИ.

Т				С				И				Н				Л				В				Ъ
	Р		Н		П		З		Ц		О		Е		Б		О		О		Ш		Ф		Р
		А				О				И				Н				К				И			

Фигура 1. Пример за шифриране със зигзагообразен шифър на транспоцизия

• ***Транспозиционен шифър с маршрут (Route cipher)*** – при него откритият текст се записва в правоъгълна матрица. Ключът определя броя на редовете в матрицата. Броя на колоните зависи от дължината на открития текст. Този вид шифър има много разновидности, в зависимост от това по какъв маршрут ще се запише шифротекстът. По-долу са представени някои разновидности на този шифър.

- С последователно записване на всички символи по редове от ляво надясно. На фиг. 2 е представен шифърът с открит текст: ТРАНСПОЗИЦИОНЕН БЛОКОВ ШИФЪР и ключ 4. Полученият шифротекст е: ТСИНЛВЪРПЦЕОШРАОИНКИНЗОБОФ.

-

Т	С	И	Н	Л	В	Ъ
Р	П	Ц	Е	О	Ш	Р
А	О	И	Н	К	И	
Н	З	О	Б	О	Ф	

Фигура 2. Пример за шифриране с последователно записване на всички символи по редове и използване на транспозиционен шифър с маршрут

- Последователно спираловидно записване - при него се записват последователно всички символи от първи ред. След това се записват последователно всички символи от втори ред в обратна посока (от дясно наляво). След това се записват всички символи от трети ред в права посока и т.н.т. На фиг. 3 е представен шифърът с открит текст: ТРАНСПОЗИЦИОНЕН БЛОКОВ ШИФЪР и ключ 4. Полученият шифротекст е: ТСИНЛВЪРШОЕЦПРАОИНКИФОБОЗН.

-

Т	С	И	Н	Л	В	Ъ
Р	П	Ц	Е	О	Ш	Р
А	О	И	Н	К	И	
Н	З	О	Б	О	Ф	

Фигура 3. Пример за шифриране с последователно спираловидно записване на всички символи по редове и използване на транспозиционен шифър с маршрут

- Спираловидно непоследователно записване на символите от матрицата - при него първо се записват всички символи от първи ред. След това се записват всички символи от последната колона в матрицата, последвани от символите от последния ред, записани в обратна посока. След това се записват всички символи от първата колона в обратен ред, без първият символ от първи ред. и т.н.т. във вид на спирала. На фиг. 4 е представен шифъра с открит текст: ТРАНСПОЗИЦИОНЕН БЛОКОВ ШИФЪР и ключ 4. Полученият шифротекст е: ТСИНЛВЪРФОБОЗНАРПЦЕОШИКНИОА.

Фигура 4. Пример за шифриране със спираловидно непоследователно записване на символите от матрицата и използване на транспозиционен шифър с маршрут

• ***Шифър с колонна транспозиция (Columnar transposition cipher)***– при този шифър откритият текст отново се записва в матрица. Ключът определя броя на колоните в матрицата, а дължината на открития текст определя броя на редовете в матрицата. Символите в ключа се номерират по реда на тяхното срещане в азбуката. В случай, че в ключа има повтарящи се символи, то те се номерират в реда на срещането им. Номера на символа в ключа определя последователността на записване на символите по колони, като първо се записват символите от колона 1, след това от колона 2 и т.н.т. На фиг. 5 е представен шифърът с открит текст: ТРАНСПОЗИЦИОНЕН БЛОКОВ ШИФЪР и ключ: ШИФЪР. Полученият шифротекст е: РООЛШСЦНОЪАЗНОИТПИБВРНИЕКФ.

Ш	И	Ф	Ъ	Р
4	1	3	5	2
Т	Р	А	Н	С
П	О	З	И	Ц
И	О	Н	Е	Н
Б	Л	О	К	О
В	Ш	И	Ф	Ъ
Р				

Фигура 5. Пример за шифриране с шифър с колонна транспозиция

• ***Шифър с двойна транспозиция (Double transposition)*** - той е аналогичен на предходния, но шифротекстът се използва втори път като открит текст и се шифрира отново. При второто шифриране е възможно да се използва и друг вид транспозиционен шифър. Този шифър е по-надежден от шифъра с колонна транспозиция.

• ***Шифър на Московски (Muszkowski cipher)*** – той носи името на своя създател Émile Victor Théodore Myszkowski. Създаден е през 1902 година. Вариант е на шифъра с колонна транспозиция, но в случаите, когато в ключа има повторение на символи, текстът от техните колони не се записва последователно, а паралелно, т.е. първо се записва първият символ от първата повтаряща се колона, след това първият символ от втората повтаряща се колона, след това вторият символ от първата повтаряща се колона и т.н.т. На фиг. 6 е представен шифърът с открит текст: ТРАНСПОЗИЦИОНЕН БЛОКОВ ШИФЪР и ключ: КОЛОНА. Полученият шифротекст е: ПООФТОНКЪАИНВСИЛИРНЗЦЕБОШР.

К	О	Л	О	Н	А
2	5	3	5	4	1
Т	Р	А	Н	С	П
О	З	И	Ц	И	О
Н	Е	Н	Б	Л	О
К	О	В	Ш	И	Ф
Ъ	Р				

Фигура 6. Пример за шифриране с шифър на Московски

• ***Транспозиционен шифър с пермутация (Permutation cipher)***– този шифър отново е подобен на шифъра с колонна транспозиция. Той се основава на пермутация и от там идва името му. След като се номерират символите от ключа в

реда на срещането им в азбуката и се попълни последователно откритият текст (фиг. 7а), колоните се пренареждат в нарастващ ред (фиг. 7б). Шифротекстът се получава като се запишат последователно всички символи по редове, а не по колони. На фиг. 7 е представен шифърът с открит текст: ТРАНСПОЗИЦИОНЕН БЛОКОВ ШИФЪР и ключ: ШИФЪР. Полученият шифротекст е: РСАТНОЦЗПИОННИЕЛООБКШЪИВФР

Ш	И	Ф	Ъ	Р
4	1	3	5	2
Т	Р	А	Н	С
П	О	З	И	Ц
И	О	Н	Е	Н
Б	Л	О	К	О
В	Ш	И	Ф	Ъ
Р				

а) първоначална матрица

И	Р	Ф	Ш	Ъ
1	2	3	4	5
Р	С	А	Т	Н
О	Ц	З	П	И
О	Н	Н	И	Е
Л	О	О	Б	К
Ш	Ъ	И	В	Ф
			Р	

б) матрица след пермутацията

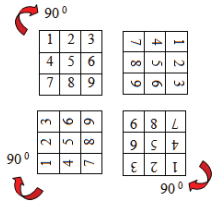
Фигура 7. Пример за шифриране с транпозиционен шифър с пермутация

• ***Шифър с прекъсване (Disrupted transposition)*** – това е най-сложният от представените транспозиционни шифри и най-надеждният. Откритият текст се попълва в табличен вид. Както при шифъра с колонна транспозиция и тук ключът определя броя на колоните в таблицата [2]. Отново символите в ключа се номерират, в зависимост от реда на срещането им в азбуката. При този шифър обаче, откритият текст не се попълва последователно, а с прекъсване, в съответствие с номера на символа в ключа. Символите в първия ред от открития текст се попълват до позиция 1 на ключа и останалите позиции в реда остават празни. На втория ред продължава въвеждането на открития текст до позиция 2 на ключа и отново останалите клетки остават празни и т.н.т. След като се попълни половината от открития текст (или при по-къси ключове се достигне най-голямата позиция) започва попълването на останалата част от открития текст в останалите празни позиции (на фиг. 8 са означени в син цвят). Шифротекстът се получава като се запишат всички символи от таблицата по колони в нарастващ ред на номера на ключа. На фиг. 8 е представен шифърът с открит текст: ТРАНСПОЗИЦИОНЕН БЛОКОВ ШИФЪР и ключ: ШИФЪР. Полученият шифротекст е: РНИВНОООФЪБСЦШЕТАЗИОРЛПКИН.

Ш	И	Ф	Ъ	Р
4	1	3	5	2
Т	Р	Б	Л	О
А	Н	С	П	О
З	И	Ц	К	О
И	В	Ш	И	Ф
О	Н	Е	Н	Ъ
Р				

Фигура 8. Пример за шифриране с шифър с прекъсване

• ***Транспозиционен шифър с въртяща решетка (Grilles cipher)***- шифърът се използва за първи път през 1550 г. за военни цели през Първата световна война [3]. Той използва множество блокове подредени в решетка, като всеки следващ блок представлява завъртане на предходния на 90 градуса, показани на фиг. 9. Откритият текст се попълва по точно определена схема, представена на фиг 10. На фиг. 11 се вижда че попълването на открития текст се извършва на 4 стъпки, като на всяка стъпка се попълват по 9 символа, чиято позиция е предварително определена от ключа. Шифротекстът се получава като се запишат последователно всички символи по редове от ляво надясно.



Фигура 9. Ротация на 90 0

10	1	19	2	11	3
20	12	28	13	4	29
14	21	5	30	22	15
31	6	16	23	7	32
17	24	33	18	34	8
25	35	26	9	27	36

Фигура 10. Схема на запълване

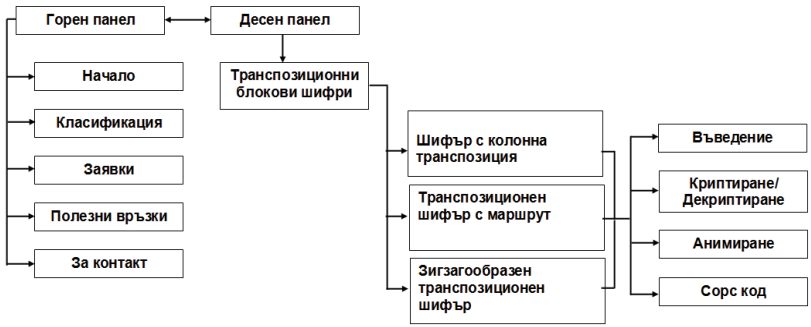
а) стъпка 1 б) стъпка 2 в) стъпка 3 г) стъпка 4

Фигура 11. Постъпково шифриране на транспозиционен шифър с решетка на Grilles

На фиг. 11 е представен постъпково шифърът с открит текст: ТРАНСПОЗИЦИОНЕН БЛОКОВ ШИФЪР С РЕШЕТКА. Ключът тук е последователността на попълване на открития текст, показана на фиг. 10. Полученият шифротекст е: ЦТКРИАООРННЕЕВСШШНЕПБИОТЛФКОАЗЪРИС.

СЪЗДАВАНЕ НА WEB-БАЗИРАНАТА СИСТЕМА

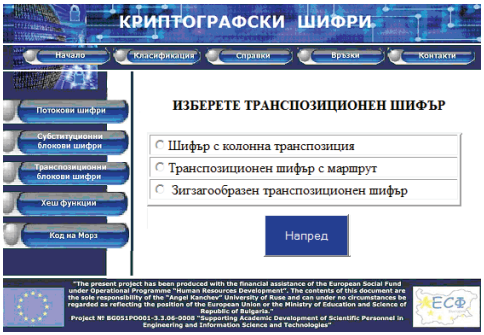
Web-базираната система е създадена с програма DreamWeaver. Използвани са езиците за програмиране HTML, CSS, PHP за създаването на сайта; JavaScript за програмирането на криптографските шифри и MySQL за създаването на базата данни. Инсталиран е WAMP Server, който работи с операционна система Windows и съчетава в себе си Apache, MySQL и PHP. За анимирането на изображенията, които онагледяват криптирането и декриптирането на различните транспозиционни шифри е използвана програма KoolMoves. Структурата на сайта е представена на фиг.12.



Фигура 12. Структура на сайта

Сайтът се състои от два панела: горен- предоставящ възможност за навигация на сайта, съответно за: начална страница; класификационна схема; заявки, за

извличане на информация от базата данни; полезни връзки и страница за контакт. Десният панел представя възможност за избор на вид криптографски шифър, като статията се фокусира само върху транспозиционните шифри.



Фигура 13. Прозорец за избор на транспозиционен шифър

При избор на връзка “Транспозиционни блокови шифри” в основния прозорец за визуализиране на информацията в сайта се показват 3 от основните видове транспозиционни шифри (показани са на фиг. 13). При избор на кой да е от тях системата предоставя възможност за: визуализиране на теоретичните основи на шифъра (бутон Въведение), преминаване към автоматично криптиране/ декриптиране (бутон Криптиране); анимиране на шифъра (бутон Анимация) или визуализиране на сорс кода на шифъра (бутон Сорс код).

При избор на бутон Заявки потребителят може да извлече информация от базата данни относно използваните до момента криптографски ключове; въведените открити текстове и получените шифротекстове за даден вид транспозиционен шифър.

ЗАКЛЮЧЕНИЕ

Системата притежава следните предимства: лесен и удобен интерфейс; избор на работен език- български или английски език; представяне на основните теоретични знания за всеки от транспозиционните шифри; възможност за онагледяване на алгоритмите със анимация (flash); възможност за въвеждане на произволен открит текст / шифротекст; възможност за въвеждане на произволен криптографски ключ; системата съхранява входните и изходни данни в база данни и позволява извеждане на справка по даден критерий.

Недостатъци: представени са само 3 от транспозиционните криптографски шифри; системата на този етап позволява криптиране / декриптиране само с използване на английската азбука.

"Настоящият документ е изготвен с финансовата помощ на Европейския социален фонд. Русенският университет „Ангел Кънчев” носи цялата отговорност за съдържанието на настоящия документ, и при никакви обстоятелства не може да се приеме като официална позиция на Европейския съюз или Министерството на образованието и науката."

Проект:№ BG051PO001-3.3.06-0008 „Подпомагане израстването на научните кадри в инженерните науки и информационните технологии”

ЛИТЕРАТУРА

[1] Йовчев Цв., История на криптографията, Софийски университет „Св. Климент Охридски", 2011.

[2] disrupted cipher, http://users.telenet.be/d.rijmenants/en/handciphers.htm.

[3] Grilles cipher, http://cryptiana.web.fc2.com/code/hamilton.htm.

[4] Rail Fence cipher, http://practicalcryptography.com/ciphers/rail-fence-cipher/.

[5] Types of transposition system, http://www.umich.edu/~umich/fm-34-40-2/ch11.pdf

За контакти:

Гл. ас. д-р Виктория Рашкова, Катедра "Информатика и информационни технологии", Русенски университет "Ангел Кънчев", тел.: 082-888 214, e-mail: vkr@ami.uni-ruse.bg