STUDY " VIGENÈRE CIPHER" WITH MS EXCEL AND COMPUTATIONAL MATHEMATICS MAPLE

Krasimir Enev
Konstantin Preslavsky University of Shumen, College – Dobrich krne@abv.bg
Radostina Rafailova-Zheleva
Konstantin Preslavsky University of Shumen, College – Dobrich rodezia@abv.bg
Detelina Hristova
Konstantin Preslavsky University of Shumen, College – Dobrich detihris@abv.bg

Abstract: In our contribution, we place a major emphasis on studying the Vigener Vigener code. The study was conducted in an in-depth algorithm research to solve a specific example of cryptography in Maple Computational Mathematics.
Cryptography is a science of how to ensure the secrecy of the message, and cryptanalysis - a science to declare the message, how to extract open text without knowing the key. Cryptographers are involved in cryptography, and cryptanalysts are the cryptanalysts. Cryptography covers all practical aspects of secret messaging, including authentication, digital signatures, e-money, and more. Cryptology is composed of the two unauthorized related areas - cryptography and cryptanalysis.
Computational math systems Matlab, Maple, Mathematica, Mathcad and others, occupy a lasting place in scientific research when analyzing experimental data, etc. The Maple system, which is based on both symbolic and numerical calculations, occupies a special place among them. The article is an overview of the relationship "cryptology - mathematics" and has been developed with various mathematical methods and software examples of cryptology, demonstrating this relationship. MAPLE is successfully used as a natural replacement of programming systems due to the huge number of built-in functions and procedures.
Practical criteria for a modern cryptosystem: level of secrecy - determined by the required time and computational resources to compromise the cryptosystem; Functionality; Methods of operation - security behavior in different ways of applying, the type of input data, etc.; Performance and speed; Implement ability - what is the complexity of hardware or software implementation, the necessary resources.
The aim of the article is the realization of some mathematical methods in examples of cryptology.
The following objectives are the following:
- studying and analyzing Cesar's cipher;
- modeling of specific examples from Cesar's cryptology using specialized software
We use the ASCII alphabet to encrypt or decrypt a message with the Caesar shield we use 256 characters, this may be a problem when writing the encrypted or decrypted text, so I will remove the special characters by leaving only the big letters as I know they are Positions 65 to 90 inclusive and lower case letters 97 to 122 inclusive.
Although easy to understand and implement, the cipher resists attempts to break it over three centuries, and therefore earns the nickname of an unbreakable cipher. There are many attempts to encrypt, which are essentially Visegner's cipher. The first common method of breaking the cipher was proposed by Friedrich Kasiiski in 1863.
Keywords: cryptography, mathematical methods, computer mathematics, Vigenère cipher, Maple.

ИЗСЛЕДВАНЕ НА „ШИФЪРА НА ВЕЖЕНЕР” С MS EXCEL И КОМПЮТЪРНАТА МАТЕМАТИКА MAPLE

Красимир Енев
ШУ„Епископ Константин Преславски” България, Колеж-Добрич krne@abv.bg
Радостина Рафаилова-Желева
ШУ„Епископ Константин Преславски” България, Колеж-Добрич rodezia@abv.bg
Детелина Христова
ШУ„Епископ Константин Преславски” България, Колеж-Добрич detihris@abv.bg

Резюме: В нашия принос поставяме основен акцент върху изучаването на "Шифъра на Виженер". Проучването е проведено в задълбочено изследване на алгоритми за решаване на конкретен пример за криптография в изчислителната математика Maple.

Криптографията е наука за това как да се гарантира тайната на посланието и криптоанализата - наука, която да декларира посланието, как да извлича отворен текст без да знае ключа. Криптографистите участват в криптографията, а криптаналистите са криптаналистите. Криптографията обхваща всички практически аспекти на тайните съобщения, включително удостоверяване, цифрови подписи, електронни подписи и др. Криптологията се състои от двете неразрешени свързани области - криптография и криптанализ.
Компютърните математически системи Matlab, Maple, Mathematica, Mathcad и други, заемат трайно място в научните изследвания при анализирането на експериментални данни и т.н. Системата Maple, която се основава както на символни, така и на числени изчисления, заема специално място сред тях. Статията е преглед на връзката "криптология - математика" и е разработена с математически метод и софтуерни примери за криптология, демонстриращи тази връзка. MAPLE се използва успешно като естествена замяна на програмните системи поради огромния брой вградени функции и процедури.
Практически критерии за съвременна криптосистема: ниво на тайна - определено от необходимото време и изчислителни ресурси за компрометиране на криптосистемата; Функционалност; Методи на работа - поведението на сигурността при различните начини на прилагане, вида на входните данни и т.н .; Ефективност и скорост; Възможност за внедряване - каква е сложността на внедряването на хардуера или софтуера, необходимите ресурси.
Целта на статията е реализирането на някои математически методи в примери за криптология.
Нашите цели са следните:
- изучаване и анализ на шифъра на Виженер;
- моделиране на конкретни примери от криптологията на Виженер чрез използване на специализиран софтуер.
Използваме ASCII азбуката за криптиране или декриптиране на съобщение с шифъра на Виженер, като използваме 256 символа, това може да е проблем при писането на кодиран или декриптиран текст, така че ще премахна специалните знаци като оставя само големите букви, както знам има позиции от 65 до 90 включително и малки букви от 97 до 122 включително.
Макар и лесен за разбиране и реализация, шифърът устоява на опитите за разбиването му в продължение на три века и затова си спечелва прозвището **неразбиваем шифър**. Съществуват много опити за шифроване, които по същество са шифър на Виженер. Първият общ метод за разбиване на шифъра е предложен от Фридрих Касиски през 1863 г.
Ключови думи: криптография, математически методи, компютърна математика, Vigenère cipher, Maple.

Във връзка с развитието на информационните технологии, актуални стават задачите за осигуряване на безопасността на документи, съхранявани в компютри и предавани по канали за връзка. За решаването на тези задачи, наред с други методи, ефективно се прилагат криптографски методи. Дълго време те основно са прилагани за нуждите на дипломацията, военното дело, специалните служби, и са били известни само на тесен кръг професионалисти - криптографи. Изобретяването на нови принципи на криптогра-фията, и появата на т.нар. криптографии с открит (публичен) ключ, дава мощен импулс за използване на криптографията за нуждите на гражданското общество, за нуждите на бизнеса, банковото дело, и позволило да се осигури безопасност при взаимодействие на широк кръг не обезателно доверяващи един на друг субекти.
Необходимо е да се различава теоретичната и приложната криптография. За задълбоченото изучаване на въпросите на теоретичната криптография е необходимо запознаване с голям кръг математически дисциплини: теория на вероятностите и статистика, висша алгебра, теория на числата, теория на графите, дикретна математика и др. Приложната криптография, което съответства на названието й, повече се занимава с въпроси на прилагане постиженията на теоретичната криптография за нуждите на конкретни практически области.
Най-известният криптограф на XVI век е *Блез Де Виженер,* френски посланик в Рим. Той се запознава там с трудове по криптография и през 1585 г. написва „*Трактат за шифрите*”, в който излага основата на криптографията. Той произнася следната мисъл, повторена по-късно от *Блез Паскал* и от *Норберт Винер*: „Всички неща в света са шифър. Цялата природа е просто шифър и секретно писмо”. *Виженер* в голяма степен развива идеята на *Кардано* за приложение на открит или шифрован текст в качеството на ключ. Той описва шифър, подобен на шифъра на *Тритемий*, но изменя системата за избор на конкретен шифър на замяна за всяка буква (фиг.2). Една от предложените техники е да се използват буквите на друг открит текст за избор на ключ за всяка буква на изходния текст. Описаният шифър, известен като *шифър на Виженер*, и,

при дължина на случайния ключ равна на дължината на откритият текст, е абсолютно надежден шифър, доказано по-късно математически (през XX век в работите на *Шенон*).

A	A	B	C	D	E	F	G	H	I	K	L	M
B	N	O	P	Q	R	S	T	U	X	Y	Z	W
C	A	B	C	D	E	F	G	H	I	K	L	M
D	O	P	Q	R	S	T	U	X	Y	Z	W	N
E	A	B	C	D	E	F	G	H	I	K	L	M
F	P	Q	R	S	T	U	X	Y	Z	W	N	O
G	A	B	C	D	E	F	G	H	I	K	L	M
H	Q	R	S	T	U	X	Y	Z	W	N	O	P
I	A	B	C	D	E	F	G	H	I	K	L	M
K	R	S	T	U	X	Y	Z	W	N	O	P	Q
L	A	B	C	D	E	F	G	H	I	K	L	M
M	S	T	U	X	Y	Z	W	N	O	P	Q	R
N	A	B	C	D	E	F	G	H	I	K	L	M
O	T	U	X	Y	Z	W	N	O	P	Q	R	S
P	A	B	C	D	E	F	G	H	I	K	L	M
Q	U	X	Y	Z	W	N	O	P	Q	R	S	T
R	A	B	C	D	E	F	G	H	I	K	L	M
S	X	Y	Z	W	N	O	P	Q	R	S	T	U
T	A	B	C	D	E	F	G	H	I	K	L	M
U	Y	Z	W	N	O	P	Q	R	S	T	U	X
X	A	B	C	D	E	F	G	H	I	K	L	M
Y	Z	W	N	O	P	Q	R	S	T	U	X	Y
Z	A	B	C	D	E	F	G	H	I	K	L	M
W	W	N	O	P	Q	R	S	T	U	X	y	Z

Фиг.1. Таблици на Порта

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W
A	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W
B	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A
C	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B
D	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C
E	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D
F	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E
G	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F
H	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G
I	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H
K	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I
L	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K
M	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L
N	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M
O	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N
P	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O
Q	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P
R	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q
S	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R
T	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S
U	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T
X	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U
Y	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X
Z	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y
W	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z

Фиг.2. Таблици на Виженер

Шифровка/дешифровка с шифъра на Виженер с Maple 15.

Шифърът на *Виженер* прилича на шифъра на *Цезар*, основната разлика е в ключа който е дума или фраза .

```
> restart;
```

Включваме пакета „StringTools” , който ще ни е необходим за работа с ASCII азбуката.

```
with(StringTools):
```

Започваме със съобщение , което искаме да криптираме / декриптираме

```
message1:=”My name is Grigor”
```

"My name is Grigor"

Създаваме **алгоритам за ключ** ,в който да ограничим специалните символи в ASCII азбуката, подобен на този който бе използван за криптиране и декриптиране с шифъра на *Цезар* без специални символи, като тук ще с използва ключ от дума или фраза.

```
vigenere := proc(letter, count, key, klength)
 local temp,L1;
 temp := letter:
L1 := 1 + ((count -1) mod klength);
 if (letter > 64) and (letter < 91) then
 temp := 65 + ((temp - 65 + key[L1]) mod 26): fi:
 if (letter > 96) and (letter < 123) then
 temp := 97 + ((temp - 97 + key[L1]) mod 26): fi:
 temp:
 end:
```

L1- е коя буква от ключа е използвана, като трябва да се премести по цялата дължината на ключа.

Следващата процедура е за криптиране на съобщението отново ще ограничим специалните символи в ASCII азбуката.

```
EncodeProc := proc(message, key, klength)
local temp1, messageLength,  position, counter:
```

Конвертираме съобщението в числени стойности:

```
temp1 := convert(convert(message, bytes),array):
messageLength:= linalg[vectdim](temp1):
counter := 0:
```
Процедура за ограничаване на специалните знаци:
```
for position from 1 to messageLength do
 if (temp1[position] > 64) and (temp1[position] < 91)
 then counter := (counter mod klength) + 1:
temp1[position] := 65 + ((temp1[position] - 65 + key[counter]) mod 26): fi:
 if (temp1[position] > 96) and (temp1[position] < 123)
 then counter := (counter mod klength) + 1:
temp1[position] := 97 + ((temp1[position] - 97 + key[counter]) mod 26): fi: od:
```
Конвертираме обратно в ASCII код
```
convert(convert(temp1,list), bytes):
end:
```
Създаваме процедури за криптираща и декриптираща ключа, който използваме с малки букви:
wordtoekey := x -> map(a -> a-97, convert(x,bytes)):- криптираща
wordtodkey := x -> map(a -> 123-a,convert(x,bytes)):- декриптираща
Създаваме процедура , с която въвеждаме ключа, в дадения случай ключа = grigor
Enterkey := wordtoekey("grigor"); [6, 17, 8, 6, 14, 17]
Следващата процедура показва дължината на ключа.
keylength := nops(Enterkey); 6
Процедура за криптиране на съобщението:
ciphertext1 := encodevigenere(message1, Enterkey, keylength);
"Sp vgav oj Oxwxui"
Визуализира криптираното съобщение:
ciphertext1; "Sp vgav oj Oxwxui"
Въвеждаме ключа за декриптиране:
decryptkey := wordtodkey("grigor"); [20, 9, 18, 20, 12, 9]
Декриптираме съобщението:
encodevigenere(ciphertext1, decryptkey, keylength);
"My name is Grigor"

ЗАКЛЮЧЕНИЕ

В нашата разработка е поставен основен акцент върху изследване на „***Шифъра на Виженер*** ”. Подготовката премина в по-задълбочено изучаване на алгоритми за решаване на конкретни примери от криптографията с компютърната математика Maple.По-нататъшен интерес представлява анализът на нови математически методи в криптологията и на специализиран софтуер за решаване на съвременни проблеми на криптографията.

ЛИТЕРАТУРА

[1] **Вернер**, М. Основы кодирования, Техносфера, 2004.
[2] **Нонинска,** И. Криптографски методи на защита на информацията, София, 2007.

ИЗПОЛЗВАНИ ИЗТОЧНИЦИ

[3] https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
[4] https://www.maplesoft.com/support/help/Maple/view.aspx?path=worksheet/documenting/startupcode