Министерство образования Республики Беларусь
БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра «Инженерная математика»

ПРИКЛАДНАЯ МАТЕМАТИКА. ПРИМЕНЕНИЕ WOLFRAM MATHEMATICA ДЛЯ ШИФРОВАНИЯ ИНФОРМАЦИИ

Учебный материал для студентов специальностей
приборостроительного факультета
1-38 80 01 «Приборостроение»

Электронный учебный материал

Минск
БНТУ 2020

УДК 519.6

Авторы: Гундина М.А., Кондратьева Н.А.

Рецензент: Габец В.Л.

Белорусский национальный технический университет пр-т Независимости, 65, г. Минск, Республика Беларусь Тел.(017) 292-67-84
E-mail: hundzina@bntu.by
http://www.bntu.by/ru/struktura/facu1t/psf/im/
Регистрационный № БНТУ/

Учебный материал содержит основные подходы к шифрованию текстовой информации и основные подходы для реализации алгоритмов шифрования в системе Wolfram Mathematica.

Данный учебный материал может быть использован как дополнительный для организации самостоятельной работы магистрантов как заочного, так и дневного отделения специальностей, изучающих дисциплину «Прикладная математика», для более глубокого освоения компьютерных систем при решении прикладных задач.

ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

На сегодняшний день остается актуальной задача обеспечения секретности передаваемой информации. Рассмотрим примеры использования системы Wolfram Mathematica для шифрования текстовой информации.

Известно, что метод замены часто реализуется многими пользователями при работе на компьютере. Если не переключить на клавиатуре набор символов с латиницы на кириллицу, то вместо букв русского алфавита при вводе текста будут печататься буквы латинского алфавита [1].

Остановимся подробнее на известных шифрах однозначной записи.

1 Шифр Цезаря

Известен метод шифрования, который использовался Гаем Юлием Цезарем. Он получил название «шифр Цезаря». Алгоритм шифрования основан на замене каждой букву на букву, следующую в алфавите через 2 позиции [1]. Переводная таблица представлена в табл. 1.

Таблица 1. Переводная таблица Цезаря

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

P	Q	R	S	T	U	V	W	X	Y	Z
S	T	U	V	W	X	Y	Z	A	B	C

Русский вариант таблицы представлен в табл.2.

Таблица 2. Русский вариант шифрозамены

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К
Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н

Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь

Ъ	Ы	Ь	Э	Ю	Я
Э	Ю	Я	А	Б	В

В системе Mathematica есть встроенная функция StringReplace, позволяющая заменить одни символы на другие согласно установленному правилу.

Пример реализации шифрования в Wolfram Mathematica:

StringReplace["Квадрат гипотенузы равен сумме квадратов катетов",{"а"->"г","б"->"д","в"->"е","г"->"ё","д"->"ж","е"->"з","ё"->"и","ж"->"й","з"->"к","и"->"л","й"->"м","к"->"н","л"->"о","м"->"п","н"->"р","о"->"с","п"->"т","р"->"у","с"->"ф","т"->"х","у"->"ц","ф"->"ч","х"->"ш","ц"->"щ","ч"->"ъ","ш"->"ы","щ"->"ь","ъ"->"э","ы"->"ю","ь"->"я","э"->"а","ю"->"б","я"->"в"}]

Результат выполнения этой команды будет следующим:

Кегжугх ёлтсхзрцкю угезр фцппз негжугхсе нгхзхсе.

2 Тарабарская грамота

Тарабарская грамота – это шифр, широко использовавшийся в древнерусских рукописях. Он представляет собой шифр замены без ключа. Согласные в алфавите делят на две равные части, и первую пишут строкой в алфавитном порядке, а вторую под буквами первой в обратном порядке.

Русский вариант шифрозамен представлен в табл. 3.

Таблица 3. Таблица шифрозамен

Б	В	Г	Д	Ж	З	К	Л	М	Н
Щ	Ш	Ч	Ц	Х	Ф	Т	С	Р	П

В этом случае буквы, расположенные на одном столбце, переходят одна в другую. Гласные буквы остаются без изменения.

Пример реализации расшифровки в Wolfram Mathematica:

```
StringReplace["Квадрат гипотенузы равен сумме квадратов катетов",{"б"->"щ","в"->"ш","г"->"ч","д"->"ц","ж"->"х","з"->"ф","к"->"т","л"->"с","м"->"р","н"->"п","п"->"н","р"->"м","с"->"л","т"->"к","ф"->"з","х"->"ж","ц"->"д","ч"->"г","ш"->"в","щ"->"б"}].
```

Результатом выполнения этой команды будет следующий набор символов:

Кшацмак чинокепуфы машеп лурре тшацмакош такекош.

3 Магические квадраты в криптографии

Одной из областей применения магических квадратов является криптография. Полибий изобрел полибианский квадрат размером 5×5, заполненный алфавитом в случайном порядке. Для шифрования на квадрате находили букву текста и вставляли в шифровку нижнюю от нее в том же столбце. Если буква была в нижней строке, то брали верхнюю из того же столбца. Этот квадрат использовали для шифрования методом двойной перестановки. Число вариантов двойной перестановки весьма велико: для таблицы 3x3 их 36, для 4x4 их 576, а для 5x5 их уже 14400.

На известной гравюре Дюрера "Меланхолия" позади грустящего ангела изображен магический квадрат, заполненный цифрами. Подобные квадраты широко применялись для вписывания шифруемого текста по приведенной в них нумерации. Если потом выписать содержимое таблицы по строкам, то получалась шифровка перестановкой букв.

Считалось, что созданные с их помощью шифровки охраняет не только ключ, но и магическая сила. Рассмотрим способ шифрования текста, используя порядок, заданный магическим квадратом (рис. 1). На рис. 2 представлено зашифрованное определение магического квадрата.

144	2	3	141	140	6	7	137	136	10	11	133
13	131	130	16	17	127	126	20	21	123	122	24
25	119	118	28	29	115	114	32	33	111	110	36
108	38	39	105	104	42	43	101	100	46	47	97
96	50	51	93	92	54	55	89	88	58	59	85
61	83	82	64	65	79	78	68	69	75	74	72
73	71	70	76	77	67	66	80	81	63	62	84
60	86	87	57	56	90	91	53	52	94	95	49
48	98	99	45	44	102	103	41	40	106	107	37
109	35	34	112	113	31	30	116	117	27	26	120
121	23	22	124	125	19	18	128	129	15	14	132
12	134	135	9	8	138	139	5	4	142	143	1

Рисунок 1 – Магический квадрат 12-ого порядка

я	а	г	а	т	е	с	и	м	м	_	с
в	ч	_	р	а	ы	н	м	_	а	р	и
_	а	н	а	д	м	ы	и	о	и	л	ы
а	_	н	я	а	о	р	е	н	к	а	п
а	а	з	к	о	а	е	л	к	я	_	о
в	е	м	р	а	р	_	а	я	и	л	а
б	т	_	ц	а	н	т	а	з	д	а	р
к	м	_	с	т	е	т	в	ы	_	з	н
_	о	л	д	я	н	н	п	_	_	р	м
з	н	н	ч	н	ц	и	и	_	р	т	т
у	л	и	л	ь	о	т	м	и	д	а	и
к	л	а	и	к	_	о	ч	и	д	о	м

Рисунок 2 – Криптограмма

Магические квадраты большой размерности могут быть хорошей основой для надежной системы шифрования, потому что ручной перебор всех вариантов ключа для этого шифра немыслим.

Построим магический квадрат 32-ого порядка, используя метод Рауз-Болла, вызывав соответствующую пользовательскую функцию.

После этого, построим матрицу размерности 32×32, и наполним ее предложением, которое необходимо зашифровать.

Выберем для шифрования текст, который описывает гравюру Дюррера:

«Перед нами морской берег, безграничная даль воды и сумеречное небо, прорезанное радугой и зловещими лучами кометы. На переднем плане в окружении разбросанных в беспорядке столярных и строительных инструментов сидит, подперев рукой голову, погруженная в глубокую задумчивость крылатая женщина, в руке у нее раскрытый циркуль, к поясу привязаны связка ключей и кошель. Неподалеку на земле лежит деревянный шар, дальше виднеется большой каменный многогранник, из-за которого выглядывает правильный тигель. Позади женщины взобравшийся на жернов угрюмый мальчуган с трудом выводит что-то на дощечке. Справа в глубине возвышается каменное здание, может быть, недостроенное, так как к нему прислонена деревянная лестница, на стенах здания висят песочные часы, весы и колокол и начертан магический квадрат. В небе, в лучах кометы, распростерла крылья огромная летучая мышь, на крыльях мыши надпись меланхолия. Почему меланхолия изображена крылатой? Что за мальчик изображен позади? В чем значение магического квадрата? Для чего разбросаны вокруг инструменты?»

В итоге построен магический квадрат и матрица, содержащая некоторое сообщение.

Построим функцию кодирования исходного выражения.

```
f[S_,M2_]:=Module[{S1,M22,M1},S1=S; M22=M2;
M1=Table[“”,{i,1,Dimensions[S][[1]]},{j,1,Dimensions[S][[1]]}];
```

For[i=1,i≤Dimensions[S][[1]],For[j=1,j≤Dimensions[S][[1]],M1[[i,j]]=M2[[S[[i,j]]]];j++];i++];Return[M1]]

В матрицу *M1* будет сохраняется символ, который находится на месте с номером, который берется из магического квадрата.

Рисунок 3 – Текст, в котором переставлены буквы в соответствии с порядком заданном в магическом квадрате

Затем ставим в соответствие каждой букве цвет. Для этого задаем набор, используемых символов, обозначим его a1.

Задаем набор, используемых цветовв цветовой модели RGB (a2).

Ставим в соответствие каждой букве цвет:

Cod=Table[a1[[i]]→a2[[i]],{i,33}].

Теперь на основе построенной матрицы цветов строим изображение.

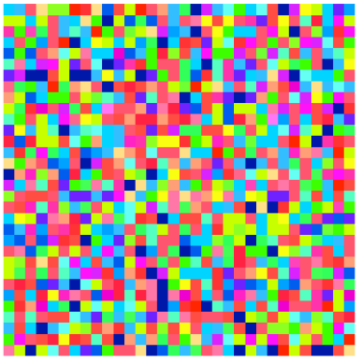

Рисунок 4 – Полученная криптограмма для текста

Аналогично построим функцию декодирования по следующей схеме: картинке ставим в соответствие массив цветов, каждому цвету ставим в соответствие букву. Затем останется в полученном наборе символов поменять их местами в порядке, заданном магическим квадратом.

4 Постолбцовая транспозиция

К классу «перестановка» относится шифр «маршрутная транспозиция» и его вариант «постолбцовая транспозиция». В данный прямоугольник вписывается сообщение по строкам. Шифрованный текст найдем, если будем выписывать буквы в порядке следования столбцов.

Рассмотрим реализацию этой транспозиции в Wolfram Mathematica.

Вводим сообщение:

t="Квадрат гипотенузы равен сумме квадратов катетов"

z=Table[0,{i,1,StringLength[t]}]

Разбиваем сообщение на строки:

For[i=1,i<=StringLength[t],i++,z[[i]]=StringTake[t,{i}]]

z2=Partition[z,3]//Transpose//Flatten

Результат представлен в следующем виде:

{К,д,т,и,т,у, ,в, ,м, ,а,а,в,а,т,в,р, ,п,е,з,р,е,с,м,к,д,т,
,т,о,а,а,г,о,н,ы,а,н,у,е,в,р,о,к,е,в}

Объединяем элементы этого списка:

StringJoin[z2]

Результат выглядит следующим образом:

Кдтиту в м ааватвр пезресмкдт тоаагоныануеврокев.

Замечание. Второй параметр Partition не обязательно равен 3.

Задания для самостоятельной работы

1. Расшифровать криптограмму Цезаря
2. Перевести текст с тарабарской грамоты
3. Расшифровать постолбцовый вариант маршрутной транспозиции

Вариант 1

1. ефвнгв жлччзузрщлуцзпгв чцрнщлв рзтузуюерг
2. пе нсюй ш тосоцед, нмичоцикля шоцы паникьля
3. ксеевоетн жедтоопис йртьбсв о, уыенл гдт

Вариант 2

1. рлъхс рз езърс тсж оцрсм
2. ноц сехагий тарепь и шоца пе кегек
3. Оелекчо окдклицоо ап к ароню

Вариант 3

1. ефз, ъхс тскргзхфв, лпззх ълфос, лдс рзескпсйрс рл тсрвхя рлъзёс, рл тскргхя дзк рзёс
2. щеф кмуца пе шысошивь и мыщту иф нмуца
3. Зосн вьлымтийоцсо е есм лекзсзсея

Вариант 4

1. ефз лфнцффхег хвёсхзбх н пцкюнз; ефз ргцнл н пгхзпгхлнз
2. щыс щы сел, лосошьи нмисекяк.
3. Заеууе ёаоаи с гтдв в емвнпа,асрнтт

Вариант 5

1. ср фхго тсахсп, жов пгхзпгхлнг ц рзёс рз шегхгос чгрхгклл
2. тко пе лахас цемеша, кору пе сехакь ш кепи
3. Ваау со оо г-е сгднлу нвту

Вариант 6

1. тсах жсойзр елжзхя хс, ъзёс рз елжвх жуцёлз
2. цшахцы ш чоц секо пе щышаек
3. Вю рюгу тлу вр м с нпв о р ататудонуиееуядвокд, оюойет

Вариант 7

1. пзшгрлнг зфхя угм пгхзпгхлъзфнлш ргцн
2. секор пе нминалевь, фирой пе нмипелевь
3. Нпеои нео ртаи лкм, в

Вариант 8

1. е пгхзпгхлнз рзх флпесосе жов рзвфрюш пюфозм
2. тко шелпой пе нмосехик, шель чоц щуцек лык
3. Нпеои нео ртаи лкм, в

Литература

1. Введение в криптографию / Под. ред. В.В. Ященко. – СПб.: Питер, 2001. – 288 с.
2. Габидулин, Э.М. Защита информации: учебное пособие / Э.М. Габидулин, А.С. Кшевецкий, А.И. Колыбельников. – М.: МФТИ, 2011. – 225 с.

СОДЕРЖАНИЕ