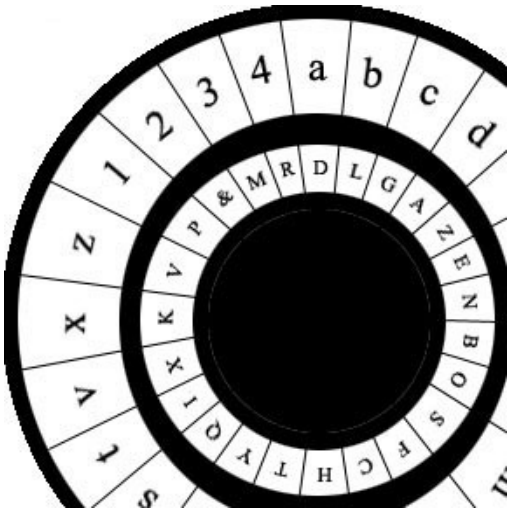
КРАТКА ИСТОРИЈА НА КРИПТОЛОГИЈАТА II

Весна Димитрова
Природно-математички факултет - Скопје
Александра Милева
Факултет за информатика - Штип

Во претходниот број на СИГМА зборувавме за почетоците на криптологијата и за криптографските системи до 15 век. Во 15 век интересот за откривање на нови криптографски системи бил многу голем. Популарноста на криптологијата не се задржала само во редовите на полициски и дипломатски институции, туку таа се проширила и многу повеќе. Нејзиниот развој станува толку важен што многу држави ангажирале цели тимови за правење на нови криптографски системи. Популарноста на криптологијата се зголемува во 16 и 17 век кога се отпечатени голем број криптографски книги. Меѓу познатите имиња од тој период се: *Leone Battista Alberti, Johannis Trithemius, Giovanni Battista Porta, Blaise de Vigenère* и.т.н.

Во западна Европа скоро сите владини институции користеле криптологијата во една или друга форма. Исто така и кодовите станале многу популарни. Првиот поголем напредок во криптографијата бил во Италија.

Leon Battista Alberti (1404-1472) е познат како "Татко на западната криптологија". Тој е еден од најраните криптоаналитичари на западот. Анализирајќи разни системи за шифрирање (замена на букви, транспозиција на букви во даден збор, и.т.н), тој открил нов начин на шифрирање познат како "повеќеалфабетска замена" (*polyalphabetic substitution*). Повеќеалфабетската замена е техника која што дозволува различни симболи од шифрираниот текст да претставуваат еден ист симбол од оригиналниот текст. Ова го отежнува дешифрирањето на пораките.



Слика1 Дискот на *Alberti*

Тој исто така го дизајнирал и познатиот шифрирачки диск (Слика 1). Дискот се состои од два концентрични круга ставени еден над друг на иста оска при што надворешниот е стационарен, а внатрешниот подвижен. Двата круга се поделени на 24 келии. Во надворешниот круг се напишани малите букви од латиницата (тоа се всушност буквите од англиската азбука без буквите j, u, w, и без h, k, y) и броевите од 1 до 4 кои се користат заедно со книга со кодови која содржи фрази и зборови. На секоја фраза или збор и одговара соодветен четирицифрен број од цифрите 1 до 4. Во внатрешниот круг се напишани по случаен редослед големите букви од латиницата (буквите од англиската азбука без буквите j, u, w) и симболот &. Надворешниот круг ги претставува буквите од оригиналниот, а внатрешниот од шифрираниот текст. На почетокот внатрешниот круг е стационарен и буквите од даден оригинален текст се шифрираат соодветно со буквите од внатрешниот круг. Потоа внатрешниот круг се ротира и се шифрираат следните букви од оригиналниот текст со сега новите букви од внатрешниот круг и т.н. Со ротација на дискот после одреден број на зборови од оригиналната порака се губи можноста за анализа со помош на фрекфенција на буквите. Оваа идеја со ротација на дискот неколку пати во текот на шифрирањето на пораката ја прави оваа техника нескршлива долго време.

Шифрирањето на пораки со помош на дискот е многу едностано. За правилно дешифрирање на пораките потребно е да се знае положбата на внатрешниот диск во текот на шифрирањето на пораката. Така, на пример зборот odi може да се шифрира со CAB, ако дискот е поставен како на сликата, но може да се шифрира и со SLE, ако се изротира десно за две места и т.н.

Задача 1. Да се шифрира пораката “napad sega” со помош на дискот, ако се знае дека клучот е “dA dE” и дискот се ротира после секој збор.

Решение: Од клучот ја гледаме поставеноста на дискот. Тоа значи дека за шифрирање на зборот “napad” дискот е поставен како на сликата, за шифрирање на зборот “sega” тој е ротиран два пати во лево. Така, се добива шифираната порака

FDHDA XNOG.

Со помош на неговото откритие “Албертовиот шифрирачки диск”, се шифрирале и дешифрирале разни пораки цели 400 години. Тој бил разбиен дури во 19 век, но и тогаш новите криптографски системи во споредба со неговиот биле многу поедноставни.

Johannis Trithemius (1462-1516)*, Giovanni Battista Porta* (1523-1596) и *Blaise de Vigenère* (1535-1615) се следните тројца важни дизајнери на шифрувачи со повеќеалфабетска замена.

Johannis Trithemius е автор на “*Polygraphia*” првата печатена книга за криптографијата од 1518 година и првиот човек кој во историјата на крипологијата, дизајнирал табела која ја нарекол *“tabula recta*” и ја користел за повеќеалфабетско шифрирање. Во првата редица од

табелата се наоѓаат 24 букви од латиницата (без j и v), а во секоја наредна редица се истите, но поместени за една буква во лево во однос на претходната редица (Слика 2).

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	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a
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	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c
e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
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	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z

Слика 2 Табела на *Trithemius*

Шифрирањето со помош на оваа табела е многу едноставно. Така, првата буква од дадена оригинална порака е истата буква од првата редица, втората буква ја заменувал со буквата од втората редица, и.т.н. На пример, ако оригиналната порака е “attack”, шифрираната порака ќе биде “auxdgp”. Доколку оригиналната порака содржи повеќе од 24 букви, шифрирањето се врши во групи ог 24 елементи, значи 25-та буква повторно се заменува со буква од првата редица, 26-та со буква од втората редица и т.н.

Задача 2. Да се дешифрира пораката

ssggff bbao cmac

со помош на шифрирањето на *Trithemius*.

Решение. Користејќи ја табелата на *Trithemius* за секоја буква ја бараме нејзината оригинална буква во соодветната редица. Така, се добива се добива пораката

SREDBA UTRE RANO.

Giovanni Battista Porta во своето дело “*De Furtivis Literarum Notis*” (1563), за прв пат во криптологијата, воведува т.н. “*digraphic*” шифрувач, во кој две букви се претставуваат со еден симбол. Тој ги класифицира системите во три вида: промена на редоследот на буквите (транспозиција - *transposition*), замена на една буква со друга (*substitution*) и замена на буква со симбол (симбол може да е и буква од друга азбука, *symbol-substitution*).

Неговата табела содржи тринаесет клуча. Тоа се тринаесет мали букви, придружени со останатите тринаесет мали букви од азбуката кои за секој пар од големи букви се поместуваат едно место во десно (Слика 3).

	a	b	c	d	e	f	g	h	i	j	k	l	m
A B	n	o	p	q	r	s	t	u	v	w	x	y	z
C D	z	n	o	p	q	r	s	t	u	v	w	x	y
E F	y	z	n	o	p	q	r	s	t	u	v	w	x
G H	x	y	z	n	o	p	q	r	s	t	u	v	w
I J	w	x	y	z	n	o	p	q	r	s	t	u	v
K L	v	w	x	y	z	n	o	p	q	r	s	t	u
M N	u	v	w	x	y	z	n	o	p	q	r	s	t
O P	t	u	v	w	x	y	z	n	o	p	q	r	s
Q R	s	t	u	v	w	x	y	z	n	o	p	q	r
S T	r	s	t	u	v	w	x	y	z	n	o	p	q
U V	q	r	s	t	u	v	w	x	y	z	n	o	p
W X	p	q	r	s	t	u	v	w	x	y	z	n	o
Y Z	o	p	q	r	s	t	u	v	w	x	y	z	n

Слика 3 Табела на *Porta*

Системот на *Porta* е многу едноставен. Така, на пример ако сакаме да ја шифрираме буквата i со клуч D, тогаш гледаме во редицата каде се наоѓа клучот и ја бараме соодветната буква, во овој случај буквата u. Доколку буквата не се наоѓа во првиот ред, ја бараме во редот на клучот и ја заменуваме со буква од првиот ред што се наоѓа во истата колона. Така, буквата p со клуч C ја шифрираме со буквата d.

Задача 3. Да се шифрира пораката “kod” со клучот “TRI” со помош на системот на *Porta.*

Решение. Првата буква од пораката, буквата k треба да се шифрира со клуч T. Во табелата на *Porta* ја бараме редицата каде се наоѓа клучот T и k ја шифрираме со o

	a	b	c	d	e	f	g	h	i	j	k	l	m
S T	r	s	t	u	v	w	x	y	z	n	o	p	q

За буквата o во редицата со клуч R одговара буквата j

	a	b	c	d	e	f	g	h	i	j	k	l	m
Q R	s	t	u	v	w	x	y	z	n	o	p	q	r

а за буквата d во редицата со клуч I одговара буквата z

	a	b	c	d	e	f	g	h	i	j	k	l	m
I J	w	x	y	z	n	o	p	q	r	s	t	u	v

Така, зборот “kod” со дадениот клуч според табелата ќе се шифрира со зборот “ojz”.

Задача 4. Да се шифрира пораката “isprati go pismoto” со клучот “david” со помош на системот на *Porta.*

Решение. Бидејќи пораката е со 16 букви, клучот со 5, ја делиме пораката на групи од по 5 елементи и секоја група ја шифрираме со дадениот клуч. Така, добиваме:

оригинален текст:	ispra | tigop | ismot | o
клуч:	david | david | david | d

шифриран текст: ufmiz | hvwfd| ufpfh | c

Следната техника за шифрирање ја открива Vigenère, дипломат на дворот на францускиот крал *Henrik* III. *И*дејата на оваа техника е користење на различна азбука за замена на секоја буква по ред од оригиналниот текст, со што многу се отежнува анализата на фрекфенција на букви. Примери за шифрирање и дешифрирање со оваа техника беа дадени во еден од претходните броеви на СИГМА во статијата "Што е криптогрфија?". Овој систем познат како "autokey" денес е искористен како основа во познатите *DES CBC* и *CFC* модови за кои ќе зборуваме во некој од следните броеви.

Откритијата на овие тројца дизајнери на шифрувачи со повеќеалфабетска замена биле актуелни цели 200 години. Првиот систематски метод за разбивање на овие шифрувачи е дизајниран од *Charles Babbage* (1791-1871) во 1854. Методот бил фокусиран на должината на клучот или клучниот збор. Ако клучот имал n букви, тогаш секој n-ти симбол во шифрираниот текст бил шифриран со истиот клуч. Така, ако шифрираниот текст се подели на n подтекстови, тогаш тој ќе биде многу лесно разбиен со помош на анализа на фреквенција на букви.

Задачи за вежбање

1. Да се шифрира пораката "test so alberti", со помош на дискот *на Alberti ,* ако клучот е "aZ aM aT".
2. Да се најде оригиналната порака на пораката "BAFS LSGEQXO", која е шифрирана со помош на дискот *на Alberti ,* ако клучот е "aR aL".
3. Да се најде оригиналната порака на пораката "PPTDOFAHNZEXEYTDR", која е шифрирана со помош на шифрирањето на *Trithemius.*
4. Да се напише табелата на *Trithemius* за англиската азбука (со сите 26 букви) и да се шифрира пораката "otkrij go kodot".
5. Дефинирај го дешифрирањето кај системот на *Porta*, а потоа да се најде оригиналната порака на пораката "VHZEMRKGWJKR", ако се знае дека е шифрирана со клуч "ENIGMA".

Литература

1. David Kahn, *The Codebreakers: History of Secret Communication,* MacMillan Publishing Co., London 1967
2. William Servos, *The Alberti cipher*, http://starbase.trincoll.edu/~crypto/historical/alberti.html
3. Fred Cohen, *A Short History of Cryptography*, http://all.net/books/ip/Chap2-1.html
4. Thomas Leary, *Cryptology in the 16th and 17th Centuries,* http://home.att.net/~tleary/cryptolo.htm
5. Artur Ekert, *Cracking codes*, http://plus.maths.org/issue34/features/ekert/index.html