МАТЕМАТИЧКА ГИМНАЗИЈА

МАТУРСКИ РАД

из предмета МАТЕМАТИКА

Савремена криптографија

Ученик
Јелена Тришовић, IV$_д$

Ментор
др Миодраг Живковић

Београд, јун 2014.

Садржај

1. Увод

Идеја овог рада је да представи развој криптографије од њених почетака до данашњих дана и да прикаже неке од познатих шифарских система, уз теоријски увод из теорије бројева и теорије коначних поља. Нагласак је на шифровању и дешифровању порука, без већег увида у криптоанализу и разлоге због којих су шифре безбедне, односно небезбедне. У кратким цртама, описује се неколико историјских ситуација у којима је криптографија одиграла врло значајну улогу.

Као теоријска основа за рад, коришћен је претежно материјал са сајта [3], а за историјске чињенице књиге [1] и [2].

2. Основни појмови

У овом поглављу дат је кратак преглед неопходних термина.

- **Отворени текст** је порука коју треба послати, нпр. $ZDRAVO$;
- **Шифрат** је шифрована порука, нпр. $VBZQWO$;
- **Шифровање** је трансформација отвореног текста у шифрат (ова трансформација мора бити таква да постоји њен инверз, како би било могуће од шифрата добити отворени текст);
- **Дешифровање** је инверзна трансформација шифрата у отворени текст;
- **Криптографија** је наука која се бави развојем сигурних начина за комуникацију. Она обухвата процес читања и писања скривених порука, тј. шифровање и дешифровање;
- **Кодирање** трансформише отворени текст у низ цифара или бита, јер је манипулисање бројевима, односно битима, једноставније него манипулисање текстом.
  На пример, велика слова енглеског алфабета можемо кодирати са $A \longrightarrow 0,\ B \longrightarrow 1,\ \ldots, Z \longrightarrow 25$, те се онда реч $ZDRAVO$ кодира са $25\ 3\ 17\ 0\ 21\ 14$. У пракси се углавном користи $ASCII$ код, који сваки симбол представља са 8 бита, на пример: $A \longrightarrow 01000001,\ B \longrightarrow 01000010, 1 \longrightarrow 00110001$ итд;
- **Декодирање** трансформише низ цифара или бита у полазни текст;

Кодирање и декодирање нису тајни процеси, већ само припрема за алгоритам шифровања који у највећем броју случајева барата цифрама или битима.

- **Проточна шифра** трансформише отворени текст у шифрат симбол по симбол или бит по бит, што је чешће случај;
- **Блоковска шифра** примењује се на симболе отвореног текста груписане у блокове. **Биграми** су парови, а **триграми** тројке слова. Неки алгоритми користе блокове бита, као на пример AES (Advanced Encryption Standard) који ради са блоковима од 128 бита (тј. 16 знакова);
- **Шифра премештања (транспозиције)** премешта (пермутује) слова, знакове или бите;
- **Шифра замене (супституције)** замењује слова (знакове, бите) другим, не мењајући им редослед;
- **Комбинована шифра** примењује наизменично премештања и замене;
- **Шифарски систем** се састоји од алгоритма шифровања и алгоритма дешифровања;
- **Кључ** је параметар којим се бира конкретна шифарска трансформација у оквиру изабраног шифарског система;
- **Симетрични систем** подразумева употребу истог тајног кључа за шифровање и дешифровање. Особе које размењују информације путем шифрованих порука (у даљем

тексту ове особе су Алиса и Боб, а особа која покушава да прочита њихову коресподенцију, Керол), морају се унапред договорити око избора кључа;

- **Асиметрични систем (систем са јавним кључем)** подразумева да Алиса и Боб објаве своје кључеве за шифровање, а да у највећој тајности чувају своје кључеве за дешифровање, који се не могу одредити на основу кључева за шифровање уз прихватљив напор;

- **Криптоанализа** је процес помоћу кога Керол покушава да трансформише шифрат у одговарајући отворени текст, не знајући кључ;

- **Декриптирање** је (макар и делимично) успешна криптоанализа;

Уобичајене претпоставке у вези са шифарским системима су следеће:

- Шифровање и дешифровање треба да буду једноставни за регуларне учеснике, Алису и Боба, док декриптирање треба да буде тежак проблем;
- Сигурност и практичност шифарског система су скоро увек противречни захтеви;
- Претпоставља се да Керол зна детаље примењеног шифарског система, а да не зна само кључ.

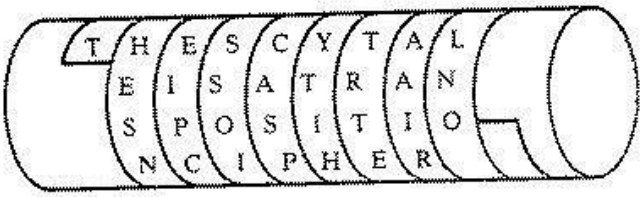
3. Историја – примери шифара од антике до данас

Према [1], први примери слања скривених порука сежу до Херодота, који их је забележио у конфликтима између Грчке и Персије. По Херодотовом мишљењу, уметност писања тајних, скривених порука спасла је Грке од напада персијског владара Ксеркса. Наиме, Ксеркс је започео изградњу Персеполиса, нове престонице свог царства и поклони су стизали одасвуд, осим из Атине и Спарте. Како би казнио овакво показивање пркоса, следећих пет година Ксеркс је мобилисао највећу армију у историји и био спреман да крене у изненадни напад. Међутим, овим припремама био је сведок Демаратус, Грк протеран из домовине, мада још увек лојалан Грчкој. Решио је да обавести своје сународнике на опасност, али је тешкоћа лежала у проналажењу начина да се таква порука достави без знања Персијанаца. Демаратус је састругао восак са дрвених таблица коришћених за писање, написао поруку и поново је прекрио воском, тако да су таблице деловале празно. Порука је несметано стигла до Грка, који су уклонили восак, прочитали упозорење и почели да се припремају за рат. Ксеркс је изгубио елемент изненађења и на крају, изгубио и сам рат.

Било је још доста оваквих прича везаних за слање скривених порука у том периоду. Вероватно једна од најпознатијих је о гласнику коме је обријана коса, порука му је записана на кожи главе, сачекано је да му коса поново израсте и тек је онда послат на пут.

Све ово су примери само скривања порука како би остале тајне, али не и њихове измене. Овај принцип, који се назива **стеганографија**, остао је у употреби и хиљадама година касније, често у комбинацији са криптографијом, чинећи само проналажење поруке тешким.

Паралелно са стеганографијом, развијала се и криптографија чији је циљ било скривање не саме поруке, већ њеног значења. Први забележени пример шифре јесте ***Спартанска шифра скитале*** *(400 година п.н.е.).* Ово је пример шифре транспозиције. Слова поруке исписују се на дугачкој папирној траци и наизглед сачињавају поруку која ништа не значи, али када се обмота око скитале, дрвеног штапа чији је дијаметар кључ за шифровање, и прочита с лева на десно, одозго на доле, добија се отворени текст поруке (слика 1 [5]).



Слика 1. Изглед шифроване поруке намотане око скитале

Прва забележена употреба шифре супституције у војне сврхе појављује се у ,,Галским ратовима“ Јулија Цезара и стога се назива ***Цезарова шифра***. *Ова шифра* свако слово замењује трећим словом удесно од њега (дуж абецеде). Ако је реч о енглеском алфабету, онда су замене $\mathrm{A} \longrightarrow D, \mathrm{B} \longrightarrow \mathrm{E}, \ldots, Z \longrightarrow \mathrm{C}$, па шифрат $CGUYR$ одговара поруци $ZDRAVO$. Уопште гледано, могућа је замена основног алфабета другим алфабетом са произвољним распоредом слова. Оваква шифра је једноставна за имплементацију и пружа релативно висок ниво сигурности, макар у првом миленијуму нове ере, када није постојао начин да се дешифрује. Цезарова шифра доминирала је све док Ал-Кинди, арапски научник из деветог века нове ере, није пронашао начин

да разбије ову моноалфабетску шифру супституције методом познатом као ***анализа учестаности***.

Све до двадесетог века није било значајнијег напретка у криптографији – примењиване су углавном разне варијације моноалфабетске шифре супституције које су отежавале њено дешифровање – један од примера је ***Вижнерова шифра*** из 16. века. Ова шифра користи Вижнеров квадрат како би се извршило шифровање методом супституције, али помоћу 26 алфабета од којих је сваки померен за по једно слово у односу на претходни. Помоћу кључа који Алиса и Боб размене пре почетка кореспонденције, утврђује се који алфабет се користи за шифровање ког слова тако што се кључ напише изнад отвореног текста неколико пута, и за шифровање сваког слова отвореног текста користи се алфабет из Вижнеровог квадрата који почиње словом кључа које се налази изнад њега. Овај поступак знатно компликује процес криптоанализе због великог броја алфабета који су у употреби, али је и овој шифри доскочено, мада тек средином 19. века. На слици 2 [8] је Вижнеров квадрат, са осенченим алфабетима који се користе у случају кључа WHITE. Примећујемо да истим словима у отвореном тексту не одговарају увек иста слова у шифрату (нпр. два узастопна слова T из отвореног текста ће у шифрату бити замењена са два различита слова). Ова особина Вижнерове шифре знатно отежава Ал-Киндијев метод анализе учестаности.

Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Слика 2. Вижнеров квадрат

Кључ: W H I T E W H I T E W H

Отворени текст: A T T A C K A T N O O N

Шифрат: W A B T G G H B G S K U

У 20. веку коначно поново долази до већих открића у криптографији. Једна од нових шифара је ***Плејферова шифра*** [3], примењивана у првим деценијама 20. века. То је једна од првих шифара која је обрађивала биграме, а истовремено је и шифра замене. На пример, за кључ PALMERSTON формира се следећа табела:

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

Да би се шифровао пар SF, посматра се правоугаоник коме су темена ова два слова; остала два темена правоугаоника су шифрат, OC. Редослед је одређен чињеницом да су S и O у истој врсти као F и C. Ако су два слова отвореног текста у истој врсти, онда се свако слово замењује словом са

његове десне стране. Тако SO постаје TN, а BG постаје CB. Ако су два слова отвореног текста у истој колони, онда се свако слово замењује словом испод себе. Тако IS постаје WC, а SJ постаје CW. Двострука слова раздвајају се словом X, па се тако отворени текст BALLOON трансформише у BA LX LO ON пре шифровања. Свако слово J у тексту замењује се словом I (тако се број различитих слова смањује на 25). Ову шифру усвојили су Британци и највероватније је користили у Бурском рату.

ADFGVX је шифра коју су користили Немци у Првом светском рату. Заснива се на примени следеће фиксне табеле:

	A	D	F	G	V	X
A	K	Z	W	R	1	F
D	9	B	6	C	L	5
F	Q	7	J	P	G	X
G	E	V	Y	3	A	N
V	8	O	D	H	0	2
X	U	4	I	S	T	M

Свако слово које треба шифровати се проналази у табели и замењује паром ознака (врста, колона). Тако, у фази замене, отворени текст PRODUCTCIPHERS постаје FG AG VD VF XA DG XV DG XF FG VG GA AG XG. Затим следи фаза премештања, која зависи од кључа без поновљених слова. Нека је кључ реч DEUTSCH. Слова кључа се нумеришу према редоследу у алфабету и резултат прве фазе пише се испод кључа у више врста на следећи начин:

D	E	U	T	S	C	H
2	3	7	6	5	1	4
F	G	A	G	V	D	V
F	X	A	D	G	X	V
D	G	X	F	F	G	V
G	G	A	A	G	X	G

Слова се затим исписују редом по колонама, при чему бројеви изнад колона треба да чине растући низ. У овом примеру, шифрат је DXGX FFDG GXGG VVVG VGFG GDFA AAXA (размаци се игноришу).

За време Другог светског рата, Шенон (Shannon) је показао да наизменично коришћење замена и премештања даје добре шифарске системе. Систем ADFGVX је лош, јер се користе само по једна замена и премештање, при чему је замена фиксна (не зависи од кључа). За време Другог светског рата коришћене су компликоване комбиноване шифре, као што су немачка ***ENIGMA*** и јапанска ***PURPLE***, а направљени су и рачунари (Colossus) за разбијање тих шифри. Још увек је тајна које шифре су користили Американци.

После 1970. године угрожавање безбедности рачунара постало је озбиљан проблем. Појавила се потреба за сигурнијим шифрама за комерцијалну употребу. Постало је могуће реализовати сложене алгоритме у једном чипу, што је омогућавало брзо шифровање, али су порасле и могућности криптоанализе.

Проблем је интензивно анализиран између 1968. и 1976. године. Године 1974. појавила се шифра LUCIFER (IBM), а 1975. DES (скраћеница од Data Encryption Standard). Оба ова система су комбиноване шифре. DES користи кључ од 56 бита. У њему се наизменично користе 16 замена и 15 премештања. Међутим, без обзира на то колико замена је извршено, безбедност шифре зависи од тајности кључа која се не може увек гарантовати. Уколико Керол на било који начин дође до кључа (који се у неком тренутку мора разменити), шифра је бескорисна. Зато је откриће система са јавним кључем довело до великог преокрета у криптографији.

4. Преглед неопходних појмова и тврђења

У овом поглављу, изнесени су основи теорије бројева и алгебре који се користе у савременим шифарским системима. У делу 4.1. дати су неки од основних појмова и теорема везаних за дељивост и конгруенције. Неке сложеније теореме дате су без доказа. У делу 4.2. овог поглавља, обрађене су основе коначних поља које се користе у шифарском систему AES. Коришћени су [3] и [4].

4.1. Дељивост, конгруенције и основне теореме

Дефиниција:Нека Z означава скуп целих бројева: $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$. За целе бројеве $a, b \in \mathbb{Z}$ кажемо да ***„ a дели b"*** (ознака је $a|b$) ако је $b = p * a$ за неко $p \in \mathbb{Z}$. Број a дели b ако и само ако је b умножак a.

Тако $3|12$ јер је $12 = 4 * 3$, $3|3$ јер је $3 = 1 * 3$, $3|-3$ јер је $-3 = (-1) * 3$, $3|0$ јер је $0 = 0 * 3$.

Особине оператора "|" :

1. Ако $a, b, c \in Z$ и $a|b$, онда $a|bc$;
2. Ако $a|b$ и $a|c$, онда $a|(b \pm c)$;
3. Ако $a|b$ и $a \nmid c$, онда а $a \nmid (b \pm c)$.

Дефиниција: ***Прости*** су они бројеви који су дељиви само са 1 и сами собом. Прости бројеви су $2, 3, 5, 7, 11, 13, \dots$

Основна теорема аритметике: Сваки број $n \in \mathbb{Z}$, $n > 1$, може се једнозначно представити у облику производа простих бројева на следећи начин:
$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$,
где су α_i позитивни цели бројеви, а p_i прости пројеви за $k \in Z$ и $i \in \{1, 2, \dots, k\}$. Овакво представљање броја n назива се ***канонска факторизација.***

Сви позитивни делиоци броја n су облика $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, где је $0 \le \beta_i \le \alpha_i$ за свако $i \in \{1, 2, \dots, k\}$, па n има $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$ различитих позитивних делилаца.

Последица основне теореме аритметике: Ако је p прост број и $p|ab$, онда $p|a$ или $p|b$.

Дефиниција: Нека су $a, b \in Z$ позитивни цели бројеви, од којих један може бити 0. ***Највећи заједнички делилац (НЗД)*** a и b (ознака $nzd(a, b)$) је највећи цео број d који дели и a и b. Приметимо да ако $d|a$ и $d|b$, онда $d|nzd(a, b)$.

Ако знамо факторизације бројева $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ и $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$ (неки од експонената могу бити 0), онда је $nzd(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_k^{\gamma_k}$, где је $\gamma_i = min\{\alpha_i, \beta_i\}$, за $k \in Z$ и $i \in \{1,2,\ldots,k\}$. За бројеве којима је највећи заједнички делилац једнак 1 кажемо да су ***узајмно прости***.

Дефиниција: Нека $a \bmod b$ означава остатак при дељењу a са b; ако је $a = qb + r$, $0 < r < b$, онда је $a \bmod b = r$.

На пример, $12 \bmod 5 = 2, 7 \bmod 5 = 2$.

Растављање великих бројева на просте чиниоце је тежак проблем. Уместо помоћу растављања на чиниоце, једноставан и ефикасан начин за израчунавање НЗД је примена Еуклидовог алгоритма. Користи се чињеница да је $nzd(a,b) = nzd(a \bmod b, b)$. Одредимо нпр. $nzd(329,119)$. Најпре делимо 329 са 119; добијамо количник 2 и остатак 91. У сваком наредном кораку, делилац и остатак постају наредни дељеник и делилац:

$$329 = 2 * 119 + 91$$

$$119 = 1 * 91 + 28$$

$$91 = 3 * 28 + 7$$

$$28 = 4 * 7 + 0$$

Последњи остатак различит од 0 је тражени НЗД. Овде је $nzd(329,119) = 7$. Низ дељења који чини Еуклидов алгоритам може се искористити да се $nzd(a,b)$ представи у облику целобројне линеарне комбинације $nzd(a,b) = na + mb$, за неке $n,m \in Z$. У сваком кораку се замењује члан низа остатака:

$7 = 91 - 3 * 28$ (заменити мањи)

$= 91 - 3(119 - 1 * 91)$ (упростити)

$= 4 * 91 - 3 * 119$ (заменити мањи)

$= 4(329 - 2 * 119) - 3 * 119$ (упростити)

Према томе, $7 = 4 * 329 - 11 * 119$, односно $n = 4$ и $m = -11$.

Релација mod: Поред тога што mod означава бинарну операцију (остатак при целобројном дељењу), mod је и ознака релације у Z: пишемо $a \equiv b \,(mod\, m)$ ако $m|b - a$.

Тако је $7 \equiv 2 \,(mod\, 5)$, јер $5|7 - 2$, $2 \equiv 7 \,(mod\, 5)$, јер $5|2 - 7$, итд. За $k \in \{0,1,2,3,4\}$, бројеви $k, k \pm 5, k \pm 10, \ldots$ су сви међусобно конгруентни по модулу 5.

Особине конгруенција:

1. **Рефлексивност:** $a \equiv a \pmod{m}$;
2. **Симетричност:** ако је $a \equiv b \pmod{m}$, онда је $b \equiv a \pmod{m}$;
3. **Транзитивност:** ако је $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, онда је $a \equiv c \pmod{m}$;

Последица особина 1, 2. и 3. је да је конгруентност по модулу m релација еквиваленције, па разбија све целе бројеве на m дисјунктних подскупова (класа еквиваленције за ову релацију). Сваки подскуп садржи тачно једног представника у интервалу $[0, m - 1]$. Скуп ових подскупова означава се са Z/mZ или Z_m. Видимо да Z/mZ има m елемената; бројеви $0,1, \ldots, m - 1$ су представници m елемената скупа Z/mZ. .

4. Ако је $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, онда је $a \pm c \equiv b \pm d \pmod{m}$ и $a * c \equiv b * d \pmod{m}$. Због тога се ове три операције могу вршити у Z/mZ, односно релација mod је сагласна са операцијама $+, -$ и $\times$.

Нека је $m = 5$. Тада је $Z/5Z$ = {0,1,2,3,4} (због једноставности, поистовећујемо елементе $Z/5Z$ са њиховим представницима — бројевима). У $Z/5Z$ је $2 * 3 \equiv 1$, јер је $2 * 3 = 6 \equiv 1 \pmod{5}$; Таблица сабирања у $Z/5Z$:

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

5. **Промена модула конгруенције:** Ако је $a \equiv b \pmod{m}$ и $d|m$, онда $a \equiv b \pmod{d}$. Тако из $12 \equiv 2 \pmod{10}$ следи $12 \equiv 2 \pmod{5}$.
6. **Инверз:** Неки елемент $x \in Z/mZ$ има мултипликативни инверз $\frac{1}{x} = x^{-1}$ у Z/mZ ако је $nzd(x,m) = 1$: пошто се $nzd(x,m) = 1$ изрази у облику целобројне линеарне комбинације $1 = ax + bm$, види се да је $ax \equiv 1 \pmod{m}$. Скуп елемената Z/mZ који имају инверзе означава се са Z/mZ^*.

На пример, $\frac{1}{2} \equiv 2^{-1} \equiv 3 \pmod{5}$, јер је $2 * 3 \equiv 1 \pmod{5}$.

У скупу $Z/9Z = \{0,1,\ldots,8\}$ могу да се користе операције $+, -, \times$, док у скупу $Z/9Z^* = \{1,2,4,5,7,8\}$ могу да се користе само операције $\times$ и $/$.

7. **Дељење у Z/mZ^***: Ако је $a \equiv b \pmod{m}, c \equiv d \pmod{m}$ и $nzd(c,m) = 1$ (из чега следи и $nzd(d,m) = 1$), онда је $ac^{-1} \equiv bd^{-1} \pmod{m}$, односно $a/c \equiv b/d \pmod{m}$. Према томе, дељење је дозвољено уколико је дељеник узајамно прост са модулом m, односно инвертибилан је;

8. **Решавање конгруенције:** Потребно је за дате a, b, m по x решити конгруенцију $ax \equiv b \pmod{m}$. Ако је $nzd(a,m) = 1$, онда су решења сви бројеви $x \equiv a^{-1}b \pmod{m}$. Ако је $nzd(a,m) = g$, онда конгруенција има решења ако $g \mid b$. Тада је конгруенција еквивалентна са $ax/g = b/g \pmod{m/g}$. Пошто је сада $nzd(a/g, m/g) = 1$, решења су $x \equiv (a/g)^{-1}(b/g) \pmod{m/g}$. Ако $g \nmid b$, онда конгруенција нема решења.

Теорема 1: Ако је $nzd(a,m) = 1$ и $ax \equiv ay \pmod{m}$, онда је $x \equiv y \pmod{m}$.

Доказ: Ако је $ax \equiv ay \pmod{m}$, онда је и $a(x-y) \equiv 0 \pmod{m}$, тј. $m \mid a(x-y)$ те због $nzd(a,m) = 1$ мора бити $m \mid (x-y) \Leftrightarrow x \equiv y \pmod{m}$, чиме је доказ завршен.

Кинеска теорема о остацима: Нека су $m_1, m_2, \ldots, m_r$ у паровима узајамно прости природни бројеви. Систем конгруенција $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}, \ldots, x \equiv a_r \pmod{m_r}$, има јединствено решење по модулу $m_1 m_2 m_3 \ldots m_r$. Другим речима, ако знамо остатке неког броја по модулу m и по модулу n, онда знамо остатак тог броја и по модулу mn.
Ево алгоритма за одређивање броја x: Потребан нам је израз који је конгруентан са a_1 по модулу m_1, односно са нула по осталим модулима $m_i, i \neq 1$. Ту особину има израз $a_1 m_2 m_3 \ldots m_r b_1$, где је $m_2 m_3 \ldots m_r b_1 \equiv 1 \pmod{m_1}$ и $b_1 \equiv (m_2 m_3 \ldots m_r)^{-1} \pmod{m_1}$. Исто тако, потребан нам је израз који је конгруентан са $a_2 \pmod{m_2}$, односно са 0 по модулу осталих m_i. Користимо израз $a_2 m_1 m_3 \ldots m_r b_2$, где је $m_1 m_3 \ldots m_r b_2 \equiv 1 \pmod{m_2}$, итд. Дакле,

$$x \equiv a_1 m_2 m_3 \ldots m_r b_1 + a_2 m_1 m_3 \ldots m_r b_2 + \cdots + a_r m_1 m_2 \ldots m_{r-1} b_r \pmod{m_1 m_2 m_3 \ldots m_r}.$$

Ојлерова функција φ: Нека $n \in Z_+$ и нека је $Z_n^* = \{a \mid 1 \leq a \leq n, nzd(a,n) = 1\}$. Овај скуп је група за множење (скуп је затворен у односу на множење, множење је асоцијативно, 1 је неутрални елемент, и сваки елемент има инверз), а назива се још и ***сведен систем остатака*** по модулу n. Ојлерова функција дефинише се као $\varphi(n) = |Z_n^*|$.

На пример, $Z_{12}^* = \{1, 5, 7, 11\}$, па је $\varphi(12) = 4$. Приметимо да, ако је p прост број, онда је $\varphi(p) = p - 1$, а ако је $r > 1$, а p је прост број, онда је $\varphi(p^r) = p^{r-1}(p-1)$.

За остале природне бројеве се вредност Ојлерове функције може израчунати коришћењем чињенице да ако је $nzd(m,n) = 1$, онда $\varphi(mn) = \varphi(m)\varphi(n)$ (на основу кинеске теореме о остацима, сваком пару (x,y) остатака по модулима m, n једнозначно одговара остатак z по модулу mn, такав да је $z \equiv x \pmod{m}$ и $z \equiv y \pmod{n}$; одатле следи да је $nzd(z, mn) = 1$ тачно ако и само ако је истовремено тачно $nzd(x,m) = 1$ и $nzd(y,n) = 1$).

Да би се израчунало $\varphi(n)$, потребно је n раставити на просте чиниоце, као у следећем примеру: $\varphi(720) = \varphi(2^4)\varphi(3^2)\varphi(5) = 2^3(2-1)3(3-1)(5-1) = 192$. Уопште, ако је $n = \prod_1^k p_i^{\alpha_i}$, онда је $\varphi(n) = \prod_1^k p_i^{\alpha_i - 1}(p_i - 1)$.

Мала Фермаова теорема: Ако је p прост број и $a \in \mathbb{Z}$, онда је $a^p \equiv a \ (mod p)$. Ако p не дели a, онда је $a^{p-1} \equiv 1 \ (mod p)$.
Општије, ако је $nzd(a,m) = 1$, онда је $a^{\varphi(m)} \equiv 1 \ (mod \ m)$ (ово тврђење се назива **Ојлерова теорема**).

Доказ: Приметимо да је

$$\{ax \ (mod \ m) | \ x \in \ Z_m^*\} = Z_m^*.$$

(ако x пролази све остатке из Z_m^* онда и $ax \ (mod \ m)$ пролази све остатке из Z_m^*, на основу теореме 1)
Због тога је

$$\prod_{x \in Z_m^*} x \equiv \prod_{x \in Z_m^*} ax \equiv a^{\varphi(m)} \prod_{x \in Z_m^*} x \quad (mod \ m)$$

Скраћивањем са бројем $\prod_{x \in Z_m^*} x$ узајамно простим са m, добија се $a^{\varphi(m)} \equiv 1 \ (mod \ m)$, чиме је доказ завршен.

Последица: Ако је $nzd(c,m) = 1$ **и** $a \equiv b \ (mod \ \varphi(m))$, при чему су a **и** b ненегативни цели бројеви, онда је $c^a \equiv c^b \ (mod \ m)$.

Дефиниција: Најмањи од природних бројева t за који важи

$$a^t \equiv 1 (mod \ m)$$

назива се ***поретком броја a по модулу m.***

Дефиниција: Ако је поредак броја g по модулу m једнак $\varphi(m)$, број g се назива ***примитивним кореном по модулу m.***

Теорема 2: Поредак броја a по модулу m постоји ако и само ако су бројеви a и m узајамно прости.

Теорема 3: Ако је t поредак броја a по модулу m, тада је $a^s \equiv 1 (mod \ m)$, ако и само ако $t|s$.

Теорема 4: Ако је g примитивни корен по модулу m, тада бројеви $1, g, g^2, g^3, \ldots, g^{\varphi(m)-1}$ образују сведен систем остатака по модулу m .

Последица: Ако је p прост број и g примитивни корен по модулу p, тада бројеви $1, g, g^2, g^3, \ldots, g^{p-2}$ образују сведен систем остатака по модулу p.

Теорема 5: За сваки прост број p постоји примитивни корен по модулу p.

4.2. Коначна поља

Ако је p прост број, означимо са $Fp = Z/pZ$ поље са p елемената, $Fp = \{0,1,\ldots,p-1\}$ са операцијама $+, -, \times$. Приметимо да за елементе $a \neq 0$ важи $nzd(a,p) = 1$, па се може одредити a^{-1}. Због тога се може делити било којим ненултим елементом. Ово поље слично је пољима рационалних, реалних или комплексних бројева.

У скупу $F_p^* = \{1,\ldots,p-1\}$ се могу користити операције $\times$ и $/$. На основу последице теореме 4 и теореме 5, постоји број g који је примитивни корен по модулу p и важи да су $\{g, g^2, g^3, \ldots, g^{p-1}\}$ и $\{1,2,\ldots,p-1\}$ једнаки (иако су њихови елементи можда написани различитим редоследом).

На пример, у групи $F_5^*, g = 2: 2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1$. У овој групи и 3 је генератор: $3^1 = 3, 3^2 = 4, 3^3 = 2, 3^4 = 1$.

Дефиниција: Неки елемент $x \in F_p^*$ јесте ***генератор*** групе F_p^* ако и само ако је његов ***ред*** (број различитих елемената у скупу $\{x, x^2, x^3, \ldots\}$ једнак $p - 1$.

Теорема: Нека је g генератор групе F_p^*. Тада је g^k генератор ове групе ако и само ако је $nzd\{k, p-1) = 1$.

Доказ: Претпоставимо да је $nzd(k, p-1) = 1$. Нека је n ред елемента g^k, $1 \leq n \leq p-1$. Тада је $1 = (g^k)^n = g^{kn}$. Према томе, $p-1 | kn$. Пошто је $nzd(k, p-1) = 1$, биће $p-1 | n$, па дакле $p-1 = n$, због $n \leq p-1$.

Доказ у супротном смеру: ако је $nzd(k, p-1) = d > 1$, онда g^k није генератор, јер је $(g^k)^{(p-1)/d} = 1$.

Претпоставимо да је p велики прост број. Нека је изабран неки генератор g групе F_p^* и неки елемент $h \in F_p^*$. Тада је јако тешко одредити x такво да је $g^x = h$, иако знамо да оно постоји. Управо на овој чињеници се заснива један број савремених шифарских система.

Размотримо сада другачију врсту коначних поља. Нека је $F_2[x]$ скуп полинома са коефицијентима из $F_2 = Z/2Z = \{0,1\}$. Приметимо да је у овом пољу $-1 = 1$, па је одузимање исто што и сабирање. Полиноми из овог скупа су

$0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3, \ldots$

Постоје два полинома степена 0 (0 и 1), четири полинома степена мањег од 2, осам полинома степена мањег од 3, итд. Уопште, број полинома степена мањег од $n+1$ је 2^{n+1}. То су полиноми $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ где је $a_i \in \{0,1\}$, за $0 \leq i \leq n$. Полиноми се множе на уобичајени начин, при чему се са коефицијентима рачуна у F_2:

$$x^4 + x^3 + x^2$$

$$\underline{\qquad x^3 + x^2 + x \qquad}$$

$$(x^2 + x + 1)(x^2 + x) = x^4 \qquad\qquad + x$$

Дефиниција: Неки полином је ***несводљив*** над пољем ако се не може раставити у производ полинома (нижег степена) са коефицијентима из тог поља.

Над пољем F_2, полином $x^2 + x + 1$ није дељив ниједним полиномом првог степена, па је несводљив (то је једини несводљиви квадратни полином над тим пољем), док полином $x^2 + x + 1 = (x+1)^2$ није несводљив. Једини несводљиви кубни полиноми над F_2 су $x^3 + x + 1$ и $x^3 + x^2 + 1$. Уопште, несводљиви полиноми добијају се од списка свих полинома прецртавањем умножака несводљивих полинома, слично као што се прости бројеви добијају применом Ератостеновог сита.

Када се елементи Z сведу по модулу простог броја p (дакле нерастављивог броја), добијају се остаци $0, 1, \ldots, p-1$, тј. бројеви мањи од p. Тај скуп означавамо са Z/pZ или $Z/(p)$.

Посматрајмо сада полиноме $F_2[x]$ и њихове остатке по модулу несводљивог полинома $x^3 + x + 1$. Добијају се сви полиноми мањег степена и важи $x^3 + x + 1 \equiv 0$, тј. $x^3 \equiv x + 1 \ (mod\,(x^3 + x + 1))$ (ову конгруенцију по модулу $x^3 + x + 1$ писаћемо убудуће као једнакост). Дакле, на скупу $F_2[x]]/\,(x^3 + x + 1) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$ дефинисане су уобичајене операције $+, -, \times$, при чему је $x^3 = x + 1$.

Пример множења у $F_2[x]]/\,(x^3 + x + 1)$:

$$x^2 + x + 1$$

$$\underline{\qquad\qquad x + 1 \qquad\qquad}$$

$$x^2 + x + 1$$

$$\underline{\qquad x^3 + x^2 + x \qquad}$$

$$x^3 \qquad\qquad + 1$$

Пошто је $x^3 = x + 1$, биће $x^3 + 1 \equiv (x + 1) + 1 = x\,(mod\,(x^3 + x + 1))$. Према томе, $(x^2 + x + 1)(x + 1) = x$ у $F_2[x]/\,(x^3 + x + 1)$. Ово поље означава се са F_8 јер има 8 елемената. Приметимо да је $x^4 = x^3 * x = (x + 1)x = x^2 + x$ у F_8.

Уопште, ако је $p(x)$ несводљиви полином степена d, онда је скуп $F_2[x]/(p(x))$ поље, које се означава са F_{2^d} и то поље има 2^d елемената. Ово поље састоји се од свих полинома степена мањег од d. $F_{2^d}^*$ је скуп од не-нула елемената поља, са $\varphi(2^d — 1)$ генератора. На пример, у F_8 је полином x генератор F_8^*:

$g = x, x^2 = g^2, x^3 = g + 1, x^4 = x^3 * x = (g + 1)g = g^2 + g, x^5 = x^3 * x^2 = g^2 + g + 1, x^6 = x^4 * x^2 = (x^2 + x)x^2 = x^4 + x^3 = g^2 + 1, x^7 = x^6 * x = (x^2 + 1)x = x^3 + x = 1$
. Сви генератори у овом пољу су g^a, где је $nzd(a, 2^3 — 1) = 1$.

Елементи поља лако се могу представити у рачунару - на пример, полином $1 * x^1 + 0 * x + 1$ представља се тројком 101, те се стога често користе поља типа F_{2^d}.

Инвертовање елемената: Покажимо како се елементи инвертују на примеру елемента $x^4 + x^3 + 1$ над пољем $F_2[x]/(x^6 + x + 1)$. Потребно је применити Еуклидов алгоритам на полиноме $x^6 + x + 1$ и $x^4 + x^3 + 1$. Прво дељење даје $x^6 + x + 1 = (x^4 + x^3 + 1)q + r$, где је r полином степена мањег од 4.

$((x^6 + x + 1) - r)/\,(x^4 + x^3 + 1) = x^2 + x + 1$

$x^6 + x^5 + x^2$

$x^5 + x^2 + x + 1$

$x^5 + x^4 + x$

$x^4 + x^2 + 1$

$x^4 + x^3 + 1$

$x^3 + x^2 = r$

Дакле, $x^6 + x + 1 = (x^4 + x^3 + 1)(x^2 + x + 1) + (x^3 + x^2)$. На сличан начин добија се $x^4 + x^3 + 1 = (x^3 + x^2)x + 1$. Према томе,

$1 = (x^4 + x^3 + 1) + (x^3 + x^2)x$

$= (x^4 + x^3 + 1) + x(x^6 + x + 1 + (x^4 + x^3 + 1)(x^2 + x + 1))$

$= (x^4 + x^3 + 1) + x(x^6 + x + 1) + (x^4 + x^3 + 1)(x^3 + x^2 + x)$

$= (x^4 + x^3 + 1)(x^3 + x^2 + x + 1)\ (mod\,(x^6 + x + 1))$

Дакле, у пољу $F_2[x]/(x^6 + x + 1) = F_{64}$, $(x^4 + x^3 + 1)^{-1} = x^3 + x^2 + x + 1$.

У описаном пољу F_8 са полиномима из $Z[x]$ ради се по два модула: коефицијенти се рачунају по модулу два, а полиноми по модулу $x^3 + x + 1$. Приметимо да ако је $d > 1$ онда $F_{2^d} \neq Z/2^dZ$ (у F_8 је $1 + 1 = 0$, а у $Z/8Z$ је $1 + 1 = 2$).

5. Савремени шифарски системи

Већина открића у криптографији и криптоанализи дешавала се под будним оком агенција за безбедност различитих држава (углавном САД и Велике Британије). Та открића нису била одмах објављивана јавности, већ су држана у тајности како би се остварила предност над читањем туђих преписки. Стога, за настанак неких шифара постоје две приче: она која је прва изашла у јавност, захваљујући људима који су, радећи ван владиних агенција дошли до открића и она, друга, која доказује да се до истог открића дошло много година раније, независно, али да оно није могло бити објављено. Тако је било и са једним од највећих открића у криптографији – системом са јавним кључем. У овом поглављу, коришћене су историјске чињенице из [1], док је за примере шифарских система коришћен сајт [3].

5.1. Системи са јавним кључем

У симетричном шифарском систему, ако знамо алгоритам шифровања и кључ за шифровање, онда лако можемо да одредимо алгоритам дешифровања, односно кључ за дешифровање. Ово важи, на пример, за Цезарову шифру, за проточне шифре, DES и AES .

Основна идеја шифарског система са јавним кључем јесте да свако зна шифарску трансформацију (алгоритам шифровања), али се не зна довољно једноставан алгоритам за одређивање кључа за дешифровање, полазећи од кључа за шифровање.

Витфилд Дифи (Whitfield Diffie) био је амерички криптограф који није радио за Владу, већ је самостално развијао своје идеје. Био је сведок настанка ARPANET-а, претече данашњег интернета

и предвидео је дигиталну револуцију и чињеницу да ће људи широм света једног дана користити новонасталу мрежу. Постало му је јасно да ће заштита порука послатих преко те мреже бити све тежа. Тајна размена кључа електронским путем била би готово неизводљива, те би самим тим и приватност људи широм света била озбиљно угрожена. Проналажење начина да се овај проблем превазиђе постало је његова опсесија. Јако тешко, успео је да пронађе људе сличне себи – Мартина Хелмана (Martin Hellman) и Ралфа Меркла (Ralph Merkle), такође криптографе. До тада, размена кључа деловала је неизбежно, иако је проузроковала много проблема. Њихова идеја било је проналажење такозване, једносмерне функције (one-way function) којом би било могуће шифровање поруке. Идеја такве функције је следећа: нека су X, Y скупови, и нека је $f: X \longrightarrow Y$ једносмерна функција. За дато $x \in X$ лако је израчунати $f(x)$ (те је шифровање лако и брзо), али је за дато $y \in Y$ тешко одредити x такво да је $y = f(x)$ (те је дешифровање тешко и споро). Постоји и појам привидно једносмерне функција (trapdoor one-way function), инвертибилне једносмерне функције f , за коју је одређивање вредности f^{-1} лако, за оне који умеју да је нађу (те је дешифровање лако и брзо). Велики број оваквих функција пронађен је у модуларној аритметици, тј. рачуну са конгруенцијама. После великог броја неуспеха, 1976. године су коначно успели да докажу да је проблем јавне размене кључа решив и објавили су свој проналазак, познат као Дифи-Хелман-Мерклов начин размене кључа (Diffie- Hellman- Merkle key exchange). Овај систем је био функционалан, мада не и довољно практичан.
Идући њиховим стопама, научници са универзитета МИТ, Роналд Рајвест, Ади Шамир и Леонард Едлман (Ronald Rivest, Adi Shamir и Leonard Adleman), су осмислили нови, практичнији алгоритам са јавним кључем, 1977. године, који је по њима назван RSA.

Међутим, у [9] се наводи да се, годинама касније, испоставило да је систем јавног кључа осмислио Џејмс Елис (James Ellis), запослени у оквиру британске Владе, још 1969. године, а да је шифру познату као RSA, осмислио Клифорд Кокс (Clifford Cocks), студент са Кембрица, 1973. године и да је ово откриће његов ментор пријавио Владиној агенцији за комуникације, због чега је оно остало тајна.

Најважније примене криптографије са јавним кључем јесу:

1. Размена кључа за симетрични шифарски систем који је бржи него код система са јавним кључем, те самим тим и чешће коришћен;

2. Дигитални потпис који служи као потврда аутентичности дигиталног документа.

У наставку, биће изложена два значајна савремена алгоритма шифровања: један са јавним кључем (RSA) и један са симетричним кључем (AES).

5.1.1. RSA

Боб најпре бира два проста броја са око 150 декадних цифара. Затим израчунава бројеве $n = pq \approx 10^{300}$ и $\varphi(n) = (p-1)(q-1)$. Затим, он одређује неки број e, такав да је $nzd(e, \varphi(n)) = 1$ и израчунава $d \equiv e^{-1} (mod\, \varphi(n))$. Приметимо да је $ed \equiv 1 (mod\, \varphi(n))$ и $1 < e, d < \varphi(n)$. Боб објављује пар бројева (n, e) као свој јавни кључ, а чува у тајности d, p и q. Цео овај поступак Боб обавља једном годишње.

Алиса жели да пошаље Бобу поруку M (то може да буде кључ за AES кодиран бројем $0 \leq M < n$). Ако је порука већа од n, онда Алиса разбија поруку на блокове који се могу представити бројевима мањим од n. Затим она проналази Бобов јавни кључ (n,e) (нпр. на његовом сајту), израчунава $C \equiv M^e (mod\, n)$ (то је привидно једносмерна функција), при чему је $0 \leq C < n$, и потом шаље број C Бобу.

Боб израчунава $C^d (mod\, n)$ и добија M, тј. отворени текст због следећег: $C^d \equiv (M^e)^d \equiv M^{ed} \equiv M\ (mod\, n)$ (ово важи због тога што, ако је $nzd(m,n) = 1$ и $a \equiv 1\ (mod\, \varphi(n))$, онда је $m^a \equiv m\ (mod\, n)$, а важиће, у датом случају, чак и ако $nzd(M,n) \neq 1$). Пресретнуту поруку C, Керол по свему судећи не може да искористи ако не зна Бобов параметар d.

Пример: Боб бира $p = 17, q = 41$. Он затим израчунава $n = pq = 17 * 41 = 697$ и $\varphi(n) = (17 - 1)(41 - 1) = 640$. Он бира $e = 33$, што је узајамно просто са 640 и затим израчунава $d \equiv 33^{-1}\ (mod\, 640) = 97$. Боб на свој сајт ставља пар $n = 697, e = 33$.
Алиса жели да користи афину шифру $C = aP + b\ (mod\, 26)$ (шифру у којој се свако слово са редним бројем P у коришћеној азбуци замењује словом са редним бројем C) са кључем $C = 7P + 25\ (mod\, 26)$ да би Бобу могла да пошаље дугачку поруку. Она кодира кључ бројем $7 * 26 + 25 = 207$, па израчунава шифрат $207^e\ (mod\, n) \equiv 207^{33} \equiv 156\ (mod\, 697)$ и шаље Бобу број 156. Полазећи од броја 156, Керол је тешко да израчуна 207.
Боб добија поруку 156, па израчунава $156^d\ (mod\, n)$: $156^{97} \equiv 207 (mod\, 697)$. Затим он декодира поруку (то није део алгоритма RSA) $207 = 7 * 26 + 25$ и може да декодира дугачку поруку коју му Алиса пошаље.

Сваки корисник има свој пар бројева: Алиса има пар (n_A, e_A), Боб пар (n_B, e_B), итд. на свом сајту, или у именику на неком познатом сајту. Пар (n_A, e_A) је Алисин јавни кључ, а d_A је њен тајни кључ.

Када Алиса шаље поруку M Бобу, она израчунава $M^{e_B}\ (mod\, n_B)$. Боб за дешифровање, односно израчунавање M, користи свој кључ d_B.

Зашто је тешко одредити d на основу e и n? Као што је речено, $d \equiv e^{-1}\ (mod\, \varphi(n))$, али иако је одређивање инверза ефикасно, одређивање $\varphi(n)$ је тешко ако знамо само n, јер је потребно раставити n на чиниоце, а за овај посао се не знају алгоритми довољно мале сложености.

5.2. Системи са симетричним кључем, AES

Влада САД је око 1970. године покренула процес развоја алгоритма за шифровање који би се могао реализовати на чипу, који би могао бити широко коришћен и који би био сигуран. Тако је 1975. године прихваћен алгоритам DES (Data Encryption Standard) фирме IBM. DES је симетрични шифарски систем са кључем дужине 56 бита који отворени текст дужине 64 бита трансформише у шифрат дужине 64 бита. Кључ дужине 56 бита је већ око 1995. године омогућавао разбијање ове шифре, без обзира на њен квалитет. Због тога се данас користи тзв. троструки DES, систем који

подразумева примену алгоритма DES три пута (са два различита кључа — први, други, први, тј. укупно 112 бита кључа) за шифровање 64-битних отворених текстова. Међутим, DES није био пројектован са намером да се користи његова трострука верзија - сигурно је да постоји ефикаснији алгоритам по нивоу сигурности еквивалентан троструком DES. Због тога је 1997. године расписан конкурс за нови алгоритам. Нови стандард (AES, Advanced Encryption Standard) је 2001. године постао алгоритам Рајндол (Rijndael) са блоком величине 128 бита и кључем дужине 128, 192 или 256 бита.

5.2.1. Упрошћени AES

Упознаћемо се најпре са поједностављеном верзијом алгоритма AES (у даљем тексту SAES) коју је конструисао Е. Шафер са своја два бивша студента 2002. године и објавио га у часопису Cryptologia 2003. године [10].

Алгоритми проширивања кључа и шифровања у SAES користе табелу S (S-box), чија структура се описује коришћењем коначног поља од 16 елемената. Нека је $F_{16} = F_2[x]/(x^4 + x + 1)$. Реч **нибл** означава четворку бита, нпр. 1011. Ниблу $b_0b_1b_2b_3$ може се придружити елемент $b_0x^3 + b_1x^2 + b_2x + b_3$ поља F_{16}.

5.2.2.Табела S

Функција S је бијективно пресликавање ниблова у ниблове, $S: \{0,1\}^4 \longrightarrow \{0,1\}^4$. Ова функција је композиција два пресликавања. Прво од њих је инверзија нибла у F_{16}. На пример, инверз полинома $x + 1$ је полином $x^3 + x^2 + x$, па прва компонента пресликавања S пресликава 0011 у 1110. Нибл 0000 је изузетак — није инвертибилан, па се пресликава у себе самог. Ниблу $N = b_0b_1b_2b_3$ (резултату инверзије) придружује се елемент $N(y) = b_0y^3 + b_1y^2 + b_2y + b_3$ прстена $F_2[y]/(y^4 + 1)$ ($y^4 + 1 = (y + 1)^4$, па није несводљив полином). Нека је $a(y) = y^3 + y^2 + 1$ и $b(y) = y^3 + 1$ у $F_2[y]/(y^4 + 1)$. Множење у овом прстену је слично као у F_{16}, изузев што се ради по модулу $(y^4 + 1)$, те је $y^4 = 1, y^5 = y$ и $y^6 = y^2$. Друга компонента пресликавања S је трансформација нибла $N(y)$ у нибл $a(y)N(y) + b(y)$. Тако се нибл $1110 = y^3 + y^2 + y$ пресликава у:

$$(y^3 + y^2 + 1)(y^3 + y^2 + y) + (y^3 + 1) =$$

$$= (y^6 + y^5 + y^4) + (y^5 + y^4 + y^3) + (y^3 + y^2 + y) + (y^3 + 1) =$$

$$= y^2 + y + 1 + y + 1 + y^3 + y^3 + y^2 + y + y^3 + 1 = y^3 + y + 1 = 1011$$

Према томе, $S(0011) = 1011$.

Приметимо да, пошто $F_2[y]/(y^4 + 1)$ није поље, нису сви његови елементи инвертибилни. Међутим, полином $a(y)$ јесте инвертибилан. У литератури се друга компонента пресликавања S обично зове афино матрично пресликавање.

Пресликавање S може се приказати следећом табелом:

nib	S(nib)	nib	S(nib)
0000	10001	1000	0110
0001	0100	1001	0010
0010	1010	1010	0000
0011	1011	1011	0011
0100	1101	1100	1100
0101	0001	1101	1110
0110	1000	1110	1111
0111	0101	1111	0111

5.2.3.Проширивање кључа

Алгоритам SAES има 16-битни кључ $k_0k_1\ldots k_{15}$. Од њега треба формирати низ од 48 бита, тј. три поткључа од по 16 бита, од којих су првих 16 једнаки оригиналном кључу, процесом ***проширивања кључа***.

Нека је $RC[i] = x^{i+2} \in F_{16}$. Тако је нпр. $RC[1] = x^3 = 1000$ и $RC[2] = x^4 = x + 1 = 0011$. Ако су N_0 и N_1 ниблови, нека је N_0N_1 њихова конкатенација и нека је $RCON[i] = RC[i]0000$ (то је бајт, низ од 8 бита). Тако је $RCON[1] = 10000000$ и $RCON[2] = 00110000$.
Нека су функције $RotNib$ и $SubNib$ дефинисане изразима $RotNib(N_0N_1) = N_1N_0$, односно $SubNib(N_0N_1) = S(N_0)S(N_1)$. Ове две функције пресликавају бајтове у бајтове, а њихова имена одговарају природи трансформација које се њима постижу (ротација, односно супституција ниблова применом S).

Дефинишимо сада низ бајтова W. Бити бајтова $W[0]$, односно $W[1]$, су првих, односно других осам бита кључа. Остали чланови низа $W[i], 2 \leq i \leq 5$, дефинишу се рекурентном релацијом (операција $\oplus$ представља сабирање по модулу 2, бит по бит):

$$W[i] = \begin{cases} W[i-2] \oplus RCON\left(\frac{i}{2}\right) \oplus SubNib\big(RotNib(W[i-1])\big), & i \equiv 0 \ (mod 2) \\ W[i-2] \oplus W[i-1], & i \equiv 1 \ (mod\ 2) \end{cases}$$

Нека су бити садржани у члановима низа W означени са $k_0k_1\ldots k_{47}$. За $0 \leq i \leq 2$, нека је $K_i = W[2i]W[2i + 1]$. Према томе, $K_0 = k_0k_1\ldots k_{15}$, $K_1 = k_{16}k_{17}\ldots k_{31}$ и $K_2 = k_{32}k_{33}\ldots k_{47}$. За $i \geq 1$, K_i је поткључ који се користи на крају i-те рунде; K_0 се користи пре прве рунде.

5.2.4.Пример проширивања кључа

Нека је кључ $0101\ 1001\ 0111\ 1010$. Према томе, $W[0] = 0101\ 1001$ и $W[1] = 0111\ 1010$. Због $i = 2$, примењује се $RotNib(W[1]) = 1010\ 0111$, па $SubNib(1010\ 0111) = 0000\ 0101$. Добијени резултат се сабира са $W[0] \oplus RCON(1)$, и добија се $W[2]$, као у следећој таблици:

	0000	*0101*
	0101	*1001*
⊕	*1000*	*0000*
	1101	*1100*

Дакле, $W[2] = 1101\ 1100$.

Сада је $i = 3$, па је $W[3] = W[1] \oplus W[2] = 0111\ 1010 \oplus 1101\ 1100 = 1010\ 0110$.
За $i = 4$, примењује се $RotNib(W[3]) = 0110\ 1010$, па $SubNib(0110\ 1010) = 1000\ 0000$.
Добијени резултат се сабира са $W[2] \oplus RCON(2)$, и добија се $W[4]$. Како је
$1000\ 0000 \oplus 1101\ 1100 \oplus 0011\ 0000 = 0110\ 1100$, имамо $W[4] = 0110\ 1100$.
На крају, $i = 5$, па је $W[5] = W[3] \oplus W[4] = 1010\ 0110 \oplus 0110\ 1100 = 1100\ 1010$.

5.2.5.Упрошћени алгоритам AES

Алгоритам SAES трансформише 16-битне отворене текстове у 16-битне шифрате, користећи проширени кључ $k_0k_1 \ldots k_{47}$. Алгоритам шифровања је композиција осам функција које се редом примењују на отворени текст:

$$A_{K_2} \circ SR \circ NS \circ A_{K_1} \circ MC \circ SR \circ NS \circ A_{K_0}$$

(функција A_{K_0} примењује се прва). Свака од ових функција примењује се на стање, где је стање четворка ниблова, приказана на слици 3. Почетно стање састоји се од отвореног текста, а завршно стање је шифрат.

$b_0b_1b_2b_3$	$b_8b_9b_{10}b_{11}$
$b_4b_5b_6b_7$	$b_{12}b_{13}b_{14}b_{15}$

Слика 3

Дефиниције примењених функција:

- **Функција A_{K_i}:** Скраћеница A_K потиче од $add\ key$. Функција A_{K_i} је сабирање стања са K_i по модулу два, бит по бит, тако да се индекси бита стања и бита кључа слажу по модулу 16.
- **Функција NS**: Скраћеница NS потиче од $nibble\ substitution$. Функција NS замењује сваки нибл N_i из стања ниблом $S(N_i)$, не мењајући редослед ниблова. Према томе, имамо следеће трансформације стања:

N_0	N_2
N_1	N_3

у стање:

$S(N_0)$	$S(N_2)$
$S(N_1)$	$S(N_3)$

- **Функција SR**: Скраћеница SR потиче од $shiftrow$. Функција SR врши следећу промену:

N_0	N_2
N_1	N_3

у стање:

N_0	N_2
N_3	N_1

- **Функција MC:** Скраћеница MC потиче од $mix\,column$. Колона $[N_i,N_j]^T$ у стању одговара елементу N_iz+N_j прстена $F_{16}[z]/\,(z^2+1)$. Тако колони $[N_i,N_j]^T$, где је $N_i=1010$ и $N_j=1001$, одговара елемент $(x^3+x)z+(x^3+1)$. Овде, као и раније, $F_{16}[z]$ означава полиноме по z са коефицијентима из F_{16}. Према томе $F_{16}[z]/\,(z^2+1)$ подразумева да се полиноми посматрају по модулу (z^2+1); због тога је $z^2=1$. Према томе, скуп представника састоји се од 16^2 полинома по z степена мањег од 2. Функција MC множи сваку колону полиномом $c(z)=x^2z+1$. У овом примеру:

$$\big((x^3+x)z+(x^3+1)\big)(x^2z+1)=(x^5+x^3)z^2+(x^3+x+x^5+x^2)z+(x^3+1)=$$

$$=(x^5+x^3+x^2+x)z+(x^5+x^3+x^3+1)=$$

$$=(x^2+x+x^3+x^2+x)z+(x^2+x+1)=$$

$$=(x^3)z+(x^2+x+1),$$

што одговара колони (N_k,N_l), где је $N_k=1000$, а $N_l=0111$. Приметимо да полином $z^2+1=(z+1)^2$ није несводљив над F_{16}, па $F_{16}[z]/\,(z^2+1)$ није поље, што значи да нису сви његови елементи инвертибилни; међутим, полином $c(z)$ јесте инвертибилан. Другим речима, функција MC трансформише колону

$b_0b_1b_2b_3$
$b_4b_5b_6b_7$

у колону

$b_0\oplus b_6$	$b_1\oplus b_4\oplus b_7$	$b_2\oplus b_4\oplus b_5$	$b_3\oplus b_5$
$b_2\oplus b_4$	$b_0\oplus b_3\oplus b_5$	$b_0\oplus b_1\oplus b_6$	$b_1\oplus b_7$

Композиција функција $A_{K_i}\circ MC\circ SR\circ NS$ је i-та рунда алгоритма шифровања. Према томе, упрошћени алгоритам има две рунде. Поред тога, примењује се допунска трансформација A_K пре прве рунде, а последња рунда нема трансформацију MC; ова чињеница биће објашњена у следећем одељку.

5.2.6.Дешифровање

Приметимо да за произвољне функције (за које су дефинисани композиција и инверзне функције) важи $(fog)^{-1}=g^{-1}\circ f^{-1}$. Поред тога, ако је композиција функције са самом собом идентично пресликавање, онда је функција сама себи инверзна и тада се каже да је она ***инволуција***. Све функције A_{K_i} су инволуције. Иако је и SR инволуција код SAES , због чињенице да она није инволуција и код AES, израз SR^{-1}неће бити упрошћаван. Дешифровање је према томе дефинисано композицијом

$$A_{K_0} \circ NS^{-1} \circ SR^{-1} \circ MC^{-1} \circ A_{K_1} \circ NS^{-1} \circ SR^{-1} \circ A_{K_2}$$

Да би се извршило пресликавање NS^{-1}, нибл се множи са $a(y)^{-1} = y^2 + y + 1$, па се резултату додаје $a(y)^{-1}b(y) = y^3 + y^2$ у прстену $F_2[y]]/ (y^4 + 1)$. После тога, нибл се инвертује у F_{16}. Уместо свега тога, може се користити унапред израчуната табела функције S^{-1}.

Пошто је MC множење са $c(z) = x^2z + 1$, функција MC^{-1} је множење са инверзом од $c(z)$, тј. $(c(z))^{-1} = xz + (x^3 + 1)$ у $F_{16}[z]/ (z^2 + 1)$.

Дешифровање се може обавити на горе описани начин. Сада ћемо видети разлог зашто у последњој рунди нема функције MC . Приметимо најпре да је $NS^{-1} \circ SR^{-1} = SR^{-1} \circ NS^{-1}$. Нека St означава неко стање. Тада је
$MC^{-1}(A_{K_i}(St)) = MC^{-1}(K_i \oplus St) = (c(z))^{-1}(K_i \oplus St) = (c(z))^{-1}(K_i) \oplus c(z)^{-1}(St) = A_{(c(z))^{-1}(K_i)}(MC^{-1}(St))$.
Према томе, $MC^{-1}(A_{K_i}(St)) = A_{(c(z))^{-1}(K_i)}(MC^{-1}(St))$.

Нека су $b_0b_1 \ldots b_7$ и $b_8b_9 \ldots b_{15}$ два бајта од којих се састоји K_i. Први бајт, $b_0b_1b_2b_3\ b_4b_5b_6b_7$ можемо сматрати елементом $F_{16}[z]/ (z^2 + 1)$. Њега множимо са $(c(z))^{-1}$, па га поново претварамо у бајт. Исто се ради и са $b_8b_9 \ldots b_{15}$. Према томе, $(c(z))^{-1}(K_i)$ има 16 бита. Израз $A_{(c(z))^{-1}(K_i)}$ означава сабирање по модулу два $(c(z))^{-1}$ са текућим стањем. Приметимо да се приликом извршавања MC^{-1}, стање множи са $(c(z))^{-1}$. Да би се извршило $A_{(c(z))^{-1}(K_i)}$, најпре се K_i множи са $(c(z))^{-1}$, а онда се резултат сабира по модулу два са текућим стањем.

Дешифровање се може вршити такође применом композиције

$$A_{K_0} \circ SR^{-1} \circ NS^{-1} \circ A_{(c(z))^{-1}(K_1)} \circ MC^{-1} \circ SR^{-1} \circ NS^{-1} \circ A_{K_2}$$

Другим речима, функције се у току дешифровања појављују истим редом као и при шифровању, изузев што се поткључеви примењују обрнутим редоследом. За оригинални AES ово може да олакша имплементацију, а било би немогуће да се MC појављује у последњој рунди.

5.2.7.Пример шифровања

Нека је кључ исти као у претходном примеру, 0101 1001 0111 1010. Према томе, $W[0] = 0101\ 1001, W[1] = 0111\ 1010, W[2] = 1101\ 1100, W[3] = 1010\ 0110,$ $W[4] = 0110\ 1100$ и $W[5] = 1100\ 1010$. Нека је отворени текст "Ed", кодиран $ASCII$ кодом, 01000101 01100100. Тада је почетно стање (водећи рачуна да ниблови иду редом у горњи леви, затим доњи леви, па горњи десни, па доњи десни угао) дато у следећој табели:

0100	0110
0101	0100

Најпре примењујемо A_{K_0} за $K_0 = W[0]W[1]$:

	0100		0110
⊕	0101	⊕	0111
	0101		0100
⊕	1001	⊕	1010

тј.

0001	0001
1100	1110

Применом NS добија се:

0100	0100
1100	1111

А затим применом SR:

0100	0100
1111	1100

Применивши MC, добијамо:

1101	0001
1100	1111

Затим се примењује A_{K_2}, при чему је $K_1 = W[2]W[3]$:

	1101		0001
⊕	1101	⊕	1010
	1100		1111
⊕	1100	⊕	0110

тј.

0000	1011
0000	1001

Применом NS добија се:

1001	0011
1001	0010

А затим применом SR:

1001	0011
0010	1001

Затим се примењује A_{K_2}, при чему је $K_2 = W[4]W[5]$:

	1001		0011
⊕	0110	⊕	1100
	0010		1001
⊕	1100	⊕	1010

тј.

1111	1111
1110	0011

Према томе, шифрат је $11111110\ 11110011$.

5.2.8.Комплетан AES

Због једноставности, посматраћемо верзију AES са 128-битним кључем и 10 рунди. Као је већ речено, AES обрађује 128-битне блокове. Биће описане разлике у односу на упрошћену верзију, у главним цртама:

- Свако стање састоји се од матрице бајтова димензије $4x4$;
- Коначно поље у коме се рачуна је $F_{2^8}[x]]/\ (x^8 + x^4 + x^3 + x + 1)$;

- Бајту $b_0b_1b_2b_3\,b_4b_5b_6b_7$ одговара елемент $b_0x^7 + \cdots + b_7 \in F_{2^8}$;
- Табела S најпре инвертује бајт у F_{2^8}, па га онда множи са $a(y) = y^4 + y^3 + y^2 + y + 1$ и резултату додаје $b(y) = y^6 + y^5 + y + 1$ у у прстену $F_2[y]]/ (y^8 + 1)$;
- Функција $ByteSub$ у AES је уопштење функције $SubNib$ — она сваки бајт B замењује његовом сликом $S(B)$;
- Функција $ShiftRow$ циклички помера врсте улево за $0,1,2$ и 3 места;
- Функција $MixColumn$ множи колону полиномом $c(z) = (x + 1)z^3 + z^2 + z + x$ у $F_{2^8}[z]/(z^4 + 1)$.Ова функција појављује се у свим рундама, сем у последњој;
- Функција $AddRoundKey$ је у ствари уопштење A_{K_i}. Допунска функција $AddRoundKey$ са поткључем за рунду 0 примењује се на почетку шифровања;
- Проширивање кључа ради са низом W чији чланови имају по четири бајта. Кључ попуњава $W[0], \ldots, W[3]$ и рачуна се на мало сложенији начин, коришћењем наредне две функције;
- Функција $RotByte$ циклички ротира групу од четири бајта за један бајт улево;
- Функција $ByteSub$ примењује функцију (табелу) S на сваки бајт.

Један од најједноставнијих, мада не и најчешћих начина коришћења блоковских шифри је ECB (Electronic Code Book). Ако је p_i i-ти блок отвореног текста, c_i одговарајући блок шифрата, а $E_k(t)$ означава примену блоковске шифре на t, онда је $c_i = E_k(p_i)$, док се дешифровање врши на основу израза $p_i = E_k{}^{-1}(c_i)$, за $i = 0,1, \ldots$ ECB јесте најједноставнији начин употребе, али има један озбиљан недостатак: за исти кључ, два иста отворена текста дају исте шифрате.
У случају да број бита није умножак 128, онда се на крају поруке додају знаци (који обично почињу са 1, јер обични ASCII знаци почињу нулом) тако да и последњи блок има дужину 128 бита.

6. Утицај криптографије на ток историје

Криптографија је кроз векове служила углавном у војне сврхе, за сакривање будућих акција од противника, али је чувала и тајне завереника, љубавника, криминалаца и уопште, свакога ко је

знао како да је користи. Међутим, врло често, била је једина слаба тачка оних који су је користили, и што су они били сигурнији у безбедност својих шифара, то су били рањивији.

У највећим сукобима човечанства, Првом и Другом светском рату, са развојем прислушкивања и пресретања непријатељских порука, криптографија и криптоанализа су ступиле на сцену као неопходно оружје.

Пресекавши немачке прекоокеанске комуникационе каблове пре почетка Првог светског рата, Велика Британија је приморала Немачку да за комуникацију користи радио и каблове контролисане од стране њених непријатеља. Тада Немачка није имала избора, осим да шифрује своје поруке, на шта су Британци били потпуно неприпремљени. Међутим, захваљујући вредном раду криптоаналитичара у, такозваној, *Соби 40*, као и захваљујући шифарским књигама допремљеним са потонулих немачких бродова, Британци су већи део порука успевали да прочитају и, што је најважније, да држе корак са променама алгоритама за шифровање. Процењује се да је, од октобра 1914. до фебруара 1919. године, пресретнуто и дешифровано више од 15 000 немачких порука. Вероватно је један од кључних тренутака било пресретање Цимерманновог (Zimmermann – немачки секретар спољних послова за време Првог светског рата) телеграма упућеног немачком амбасадору у Мексику, којим се Мексико позива да уђе у рат, како би се евентуална реакција САД на објављивање неограниченог подморничког рата држала под контролом. САД су водиле антиратну политику и остале неутралне упркос овој објави. Тада су Британци, осигуравши најпре да улога њихових криптоаналитичара у добијању телеграма буде сакривена, разоткрили намере Немаца и њихову антиамеричку политику председнику САД, Вудро Вилсону. Ово се сматра једним од фактора који је допринео уласку САД у рат, а самим тим и победи Савезника [2].

У Другом светском рату, Немачка је, поучена претходним искуством, развила нову шифру под називом *Енигма* (*Enigma).* Енигма је заправо била машина, налик на писаћу, на којој се, помоћу низа ротора, шифровало слово по слово [7]. Овог пута, Немци су били сигурни да им је шифра безбедна, што је у почетку и била. Прве напоре за дешифровање Енигме уложили су Пољаци, а касније су посао преузели Британци у Блечли парку (Bletchley Park), новооснованој бази посвећеној искључиво разбијању немачких шифара. Знатну помоћ у дешифровању обезбедили су сами Немци – слабим поштовањем процедура и ретким променама кључа који су слабили ову, иначе врло јаку, шифру. У циљу разбијања Енигме, настајали су механичко-електрични рачунари попут *Бомби*, који су извршавали проверу свих могућих комбинација грубом силом. Временом, напори уложени у Блечли парку су се исплатили и Британци су могли да читају велики број немачких порука, мада су ту своју способност морали да чувају у тајности како је не би изгубили. Сматра се да је овакав увид у немачке намере знатно скратио овај рат и свакако био велика предност за Савезнике.

Упркос својој улози у ратовима, криптографија се користи и у многим другим сферама свакодневног живота – на пример у банкарству, при трансакцијама, ради спречавања електронских пљачки. Такође, она нам обезбеђује да сачувамо за себе податке које не желимо да делимо са целим светом.

Са настанком шифара попут RSA и AES, за које се тврди да, уколико се примењују на правилан начин, немогуће дешифровати у реалном времену, приватност људи је заштићена, а Дифијев циљ испуњен. Међутим, те шифре су омогућиле и неометану комуникацију криминалаца. Стога је покренуто питање да ли јавности треба да буду доступне тако јаке шифре и како ограничити њихово коришћење. Чак се и трговина програмима за шифровање у САД сматра трговином

оружјем. Одавно је познато да сва интернет коресподенција пролази кроз филтере кључних речи, тј. да су Дифијева предвиђања о озбиљном нарушавању приватности била тачна. NSA (National Security Agency) – америчка Национална агенција за безбедност, према [6], активно гради центре за овакву контролу електронске поште, нарочито након преиспитивања њеног постојања од стране америчке јавности услед немогућности да спречи терористичке нападе који су се одиграли у претходних петнаестак година. О томе на каквим се тамо шифрама и алгоритмима за дешифровање сада ради, вероватно нећемо скоро сазнати.

7. Закључак

У овом раду, описана је кратка историја криптографије, са освртом на неке од најзначајнијих начина шифровања, попут Цезарове, Вижнерове и Плејферове шифре. Ипак, основна идеја била је

представљање савремених шифарских система, као што су RSA и AES, и наглашавање улоге коју математика игра у једној практичној науци као што је криптографија.

Постоји још много примера шифара и занимљивих историјских прича везаних за ову област које нису обрађене у овом раду, али и цела једна област, која је настала упоредо са криптографијом и највећим делом била одговорна за њен развој – криптоанализа. Историји ове науке, као и њеним достигнућима треба посветити барем подједнако пажње као и криптографији, ради бољег разумевања онога што је у овом раду већ речено, али и због тога што је, после непробојних шифара као што су RSA и AES, сада ред на криптоанализу да начини следећи корак.

8. Литература

[1] S. Singh, *The Code Book*, Fourth Estate, London, 1999;

[2] D. Kahn, *The Codebreakers*, The Macmillan Company, New York, 1973;

[3] http://poincare.matf.bg.ac.rs/~ezivkovm/nastava/kripto.htm;

[4] В. Мићић, З. Каделбург, Д. Ђукић, *Увод у теорију бројева*, Друштво математичара Србије, Београд, 2013;

[5] http://williamstallings.com/Extras/Security-Notes/lectures/classical.html;

[6] http://www.wired.com/2012/03/ff_nsadatacenter/all/;

[7] http://en.wikipedia.org/wiki/Enigma_machine

[8] http://pippick.com/reviews/worldfaceoff/worldtimer_faceoff.htm#item1.

[9] http://wayback.archive.org/web/20100519084635/http://www.gchq.gov.uk/history/pke.html

[10] Mohammad Musa, Edward Schaefer, and Stephen Wedig, *A simplified AES algorithm and its linear and differential cryptanalyses*, Cryptologia 27 (April 2003), 148–177.