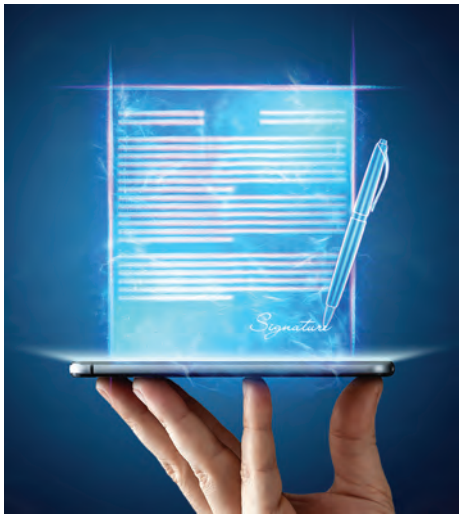
O matematici *digitalnog potpisa*

Zrinka Franušić, Zagreb

Digitalni potpis je elektronička zamjena za vlastoručni potpis koji u prvom redu mora osigurati vjerodostojnost. Osmišljen je s pomoću matematičkih modela koji se oslanjaju na neke teško rješive probleme. Budući da su digitalni potpisi vrste kriptografskih protokola, ovdje ćemo najprije opisati najpoznatije modele iz klasične kriptografije bez čijeg je poznavanja teško razumjeti suvremene kriptografske sheme.



Uvod

Brzi rast globalne digitalizacije i prijelaz na različite načine *online* poslovanja iznjedrili su veliku potrebu za uporabom **elektroničkog potpisa** koji se češće popularno naziva **digitalni potpis**. Njegova glavna uloga je zamjena tradicionalnog vlastoručnog potpisa, no samo ako se njime koristimo u skladu s odgovarajućim zakonima. Stoga ćemo najprije navesti službene zahtjeve koje mora zadovoljiti digitalni potpis, a zatim opisati neke jednostavnije matematičke modele, odnosno kriptosustave, koji omogućavaju da se ti zahtjevi ispune.

O pravnoj regulativi digitalnog potpisa

Najčešće se ističu tri vrste elektroničkog potpisa:

- SES – **jednostavni** elektronički potpis (engl. *simple electronic signature*),
- AdES – **napredni** elektronički potpis (engl. *advanced electronic signature*),
- QES – **kvalificirani** elektronički potpis (engl. *qualified electronic signature*).

SES nije obuhvaćen pravnom regulativom i njome se koristimo za potpisivanje dokumenata koji nemaju veliku vrijednost. Primjer SES-a je ubacivanje skeniranog potpisa u dokument u pdf formatu. Za razliku od toga, AdES i QES moraju ispunjavati odredbe regulirane zakonom. U Republici Hrvatskoj se od 8.8.2017. provodi Uredba (EU) br. 910/2014[1] Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama (...) iz 2014. godine. Prema navedenom dokumentu *elektronički potpis* označava *podatke u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podatcima u elektroničkom obliku i koje potpisnik koristi za potpisivanje*.

izv. prof. dr. sc. Zrinka Franušić, Sveučilište u Zagrebu Prirodoslovno-matematički fakultet, Matematički odsjek, fran@math.hr

[1] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32014R0910&qid=1499665194132

Nadalje, uredbom (Članak 26) su propisani i zahtjevi za napredne elektroničke potpise (AdES i QES). Napredan elektronički potpis mora ispunjavati sljedeće zahtjeve:

(a) na nedvojben način povezan je s potpisnikom

(b) omogućava identificiranje potpisnika

(c) izrađen je korištenjem podataka za izradu elektroničkog potpisa koje potpisnik može, uz visoku razinu pouzdanja, upotrijebiti pod svojom isključivom kontrolom

(d) povezan je s njime potpisanim podatcima tako da se može otkriti bilo koja naknadna izmjena podataka.

Ukratko, prethodni se zahtjevi mogu izreći kao tri ključna svojstva koja mora posjedovati digitalni potpis:

(1) **vjerodostojnost** (engl. *authenticity*)

(2) **netaknutost** (engl. *integrity*)

(3) **nepobitnost** (engl. *non-repudiation*).

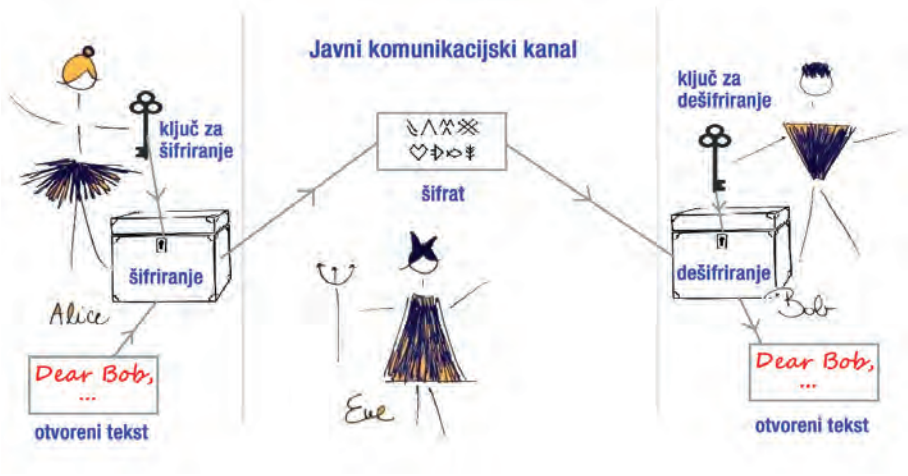
Razlika između digitalnih potpisa AdES i QES jest u tome što QES mora biti potvrđen od ovlaštene agencije za izdavanje digitalnih certifikata (kao što je npr. FINA u RH).

Matematički modeli koji mogu ispuniti navedene zahtjeve su tzv. **kriptosustavi s javnim ključem**. No da bismo ih bolje razumjeli, valja krenuti redom.

Kriptografija. Kriptosustavi s tajnim ključem

Kriptografija je znanstvena disciplina koja se bavi konstrukcijom i analizom protokola za maskiranje poruka tako da one budu razumljive samo onima kojima su namijenjene. Sama riječ **kriptografija** dolazi od grčkih riječi *kryptós* (skriven, tajan) i *grápho* (pisati) pa bismo ju mogli prevesti kao **tajnopis**. Siguran **kriptosustav** trebao bi omogućiti komunikaciju između **pošiljatelja** zvanog *Alice* i **primatelja** zvanog *Bob* preko **nesigurnog kanala** (npr. interneta) koji nadzire "treća strana", tzv. *Eve*. Poruka koju Alice želi poslati Bobu naziva se **otvoreni tekst**. Prije slanja Alice **šifrira** otvoreni tekst, odnosno transformira ga u **šifrat** iz kojeg nije moguće lako pročitati sadržaj poruke koristeći se **ključem za šifriranje**. Bob prima šifrat te s pomoću **ključa za dešifriranje** dobiva originalnu poruku.

Prije nego što uvedemo precizniju terminologiju koja nam je potrebna za konstrukciju kriptosustava dajemo primjer jednog od najjednostavnijih modela šifriranja tzv. **Cezarovu šifru** kojom se koristio rimski car Gaj Julije Cezar (1. stoljeće pr. Kr.) za svoju privatnu korespondenciju.



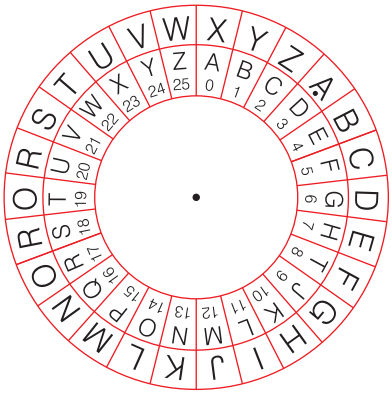
Slika 1. Shema klasičnog kriptosustava

Primjer 1. Cezarova šifra

Ova se šifra realizira zamjenom svakog slova abecede slovom koje je 3 mjesta unaprijed, tj. abeceda se pomiče ciklički udesno kao što je prikazano u sljedećoj tablici:

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
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

Prema tome poruka – otvoreni tekst ALEA IACTA EST šifrira se kao DOHD LDFWD HVW. Jasno da se dešifriranje provodi pomicanjem svakog slova šifrata za 3 mjesta ulijevo.



Slika 2. Cezarov disk za šifriranje

Napominjemo da se razmaci između riječi te interpunkcijski znakovi ne šifriraju što znači da otvoreni tekst iz prethodnog primjera zapisujemo kao ALEAIACTAEST, a pripadni šifrat kao DOHDLDFWDHVW.

Definicija 1. ***Kriptosustav*** *je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju vrijedi:*

1) $\mathcal{P}$ *je konačan skup svih mogućih osnovnih elemenata otvorenog teksta*
2) $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elemenata šifrata*
3) $\mathcal{K}$ *je konačan skup svih mogućih ključeva*
4) $\mathcal{E}$ *je skup svih funkcija šifriranja, a* $\mathcal{D}$ *skup svih funkcija dešifriranja takvih da za svaki ključ* $K \in \mathcal{K}$ *postoji funkcija šifriranja* $e_K : P \to \mathcal{C}$ *u* $\mathcal{E}$ *i odgovarajuća funkcija dešifriranja* $d_K : \mathcal{C} \to \mathcal{P}$ *iz* $\mathcal{D}$ *za koje vrijedi da je*

$$d_K(e_K(x)) = x,$$

za svaki otvoreni tekst $x \in \mathcal{P}$.

Skup $\mathcal{P}$ ponekad se naziva **prostor otvorenih tekstova** (od engl. *plaintext*), $\mathcal{C}$ – **prostor šifrata** (od engl. *ciphertext*), a $\mathcal{K}$ – **prostor ključeva**. U klasičnim šiframa najčešće su prostori $\mathcal{P}$ i $\mathcal{C}$ jednaki skupu slova engleske abecede ili skupu njihovih numeričkih ekvivalenata:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

U primjerima ćemo slova hrvatske abecede Č, Ć, Đ, Dž, Lj, Nj, Š, Ž, zamijeniti redom slovima C, C, DJ, DZ, LJ, NJ, S, Z.

Koristeći se navedenom terminologijom i oznakama poopćenje Cezarove šifre koje se dobiva pomicanjem svakog slova abecede za n mjesta udesno možemo opisati sljedećim matematičkim modelom:

CEZAROVA ŠIFRA

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0, 1, 2, \ldots, 25\} = \mathbb{Z}_{26}.$$

Za svaki ključ $n \in \mathcal{K}$ funkcije šifriranja i dešifriranja su

$$e_n : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad e_n(x) = (x + n) \mod 26,$$

$$d_n : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad d_n(y) = (y - n) \mod 26.$$

(Operacija "mod 26" daje ostatak pri dijeljenju nekog cijelog broja brojem 26.)

Vrlo važno pitanje koje se veže za svaki kriptosustav jest pitanje njegove sigurnosti. Stoga nas zanima koliko je lako ili koliko je teško pronaći otvoreni tekst iz šifrata, ali bez poznavanja ključa. Takav postupak naziva se **dekriptiranje** ili popularno – **razbijanje** šifrata (ili kriptosustava), a disciplina koja se time bavi zove se **kriptoanaliza**. Bez ulaženja preduboko u tu problematiku, budući da kriptoanaliza uglavnom uključuje "ozbiljniju" matematiku, često ćemo kratko komentirati i razinu sigurnosti opisanog kriptosustava.

Cezarova šifra je vrlo slaba, odnosno nesigurna jer je njezin prostor ključeva vrlo mali – ima ih točno 25 (ako izuzmemo $n = 0$ za koji je funkcija šifriranja jednaka identiteti). Zato ju se vrlo lako može *razbiti* primjenom tzv. *grube sile*, tj. ispitujući redom svaki od mogućih ključeva, $n = 1, \ldots, 25$, sve dok ne dobijemo smisleni tekst.

Primjer 2. Afina šifra

Poopćenje Cezarove šifre koje za funkciju šifriranja upotrebljava *afinu* funkciju

$$x \mapsto ax + b \mod 26,$$

za neke $a, b \in \mathbb{Z}_{26}$, naziva se **afina šifra**. Uređeni par (a, b) predstavlja *ključ* ove šifre. No ona će biti valjana samo ako je funkcija šifriranja bijekcija na $\mathbb{Z}_{26}$. Na primjer, za $(a, b) = (2, 1)$ vrijedi da je $2 \cdot 1 + 1 = 3$, ali i $2 \cdot 14 + 1 \mod 26 = 3$, što znači da bi se dva otvorena teksta $x_1 = 1$ i $x_2 = 14$ šifrirala istim šifratom $y_1 = y_2 = 3$. Uočimo da će uvjet bijektivnosti biti ispunjen ako i samo ako su parametar a i broj 26 relativno prosti. Zaista, ako je $\operatorname{nzd}(a, 26) = 1$, tada kongruencija[2]

$$ax + b \equiv y \pmod{26}$$

ima jedinstveno rješenje.

Na primjer, poruku *ZAGREB* s pomoću afine šifre s ključem $(3, 4)$ šifriramo na sljedeći način:

otvoreni tekst	Z	A	G	R	E	B
x	25	0	6	17	4	1
$y = 3x + 4 \mod 26$	1	4	22	3	16	7
šifrat	B	E	W	D	Q	H

Matematički model afine šifre dan je izrazima:

AFINA ŠIFRA

$$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26},$$

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \operatorname{nzd}(a, 26) = 1\}.$$

Za $K = (a, b) \in \mathcal{K}$ funkcije šifriranja i dešifriranja dane su s

$$e_K(x) = (ax + b) \mod 26,$$

$$d_k(x) = a^{-1}(y - b) \mod 26,$$

pri čemu a^{-1} označava multiplikativni inverz broja a u prstenu $\mathbb{Z}_{26}$.

Napominjemo da skup $\mathbb{Z}_{26}$ s obzirom na zbrajanje i množenje modulo 26 ima algebarsku strukturu komutativnog prstena s jedinicom. Svi dopustivi parametri a afine šifre i njihovi multiplikativni inverzi navedeni su u sljedećoj tablici:

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

[2] O kongruencijama je bilo riječi u prošlom broju MiŠ-a (MiŠ 114, str. 174).

Uspoređujući Cezarovu i afinu šifru, lako možemo ustanoviti da je afina šifra nešto sigurnija jer je prostor ključeva nešto veći (njih $12 \cdot 26 = 312$). No sve **supstitucijske** šifre koje svako slovo abecede mijenjaju nekim drugim slovom mogu se lako razbiti s pomoću **frekvencijske analize slova**. Poznato je da se u svakom jeziku neka slova pojavljuju češće, a ti su podatci vrlo dobro poznati. Tako su u hrvatskome jeziku najfrekventnija slova A, I, O, E, N, a u engleskome E, T, A, O, I.

Razbijanje šifrata primjenom frekvencijske analize slova može se izbjeći tako da se svako slovo abecede može šifrirati na više načina. U sljedećem primjeru opisujemo vrlo popularnu Vigenerèovu šifru koja se upotrebljavala čak do kraja 19. stoljeća i smatrala **neprobojnom**. Osmislio ju je Talijan Giovan Battista Bellaso sredinom 16. stoljeća, a popularizirao francuski diplomat Blaise de Vigenerè po kojem i nosi ime. Ideja je da se ključ sastoji od više slova, odnosno tzv. **ključne riječi** što će rezultirati time da se svako slovo može šifrirati na više načina.

Primjer 3. Vigenerèova šifra

Pretpostavimo da je ključna riječ *MRAV*. Budući da ključna riječ odgovara numeričkim ekvivalentima $12, 17, 0, 21$, šifrat dobivamo tako da prvo slovo otvorenog teksta zamijenimo slovom koje je 12 mjesta udesno, drugo sa slovom koje je 17 mjesta udesno, treće ostavimo isto, a četvrto pomičemo za 21 mjesto te ponavljamo postupak. To zapravo znači da svako četvrto slovo šifriramo Cezarovom šifrom s istim ključem. Na primjeru otvorenog teksta *NAGRADA* šifriranog ključnom riječi *MRAV* dobivamo:

	13	0	6	17	0	3	0
$+_{26}$	12	17	0	21	12	17	0
	25	17	6	12	12	20	0

	N	A	G	R	A	D	A
$+_{26}$	M	R	A	V	M	R	A
	Z	R	G	M	M	U	A

Već i na primjeru šifriranja ovako kratke riječi opažamo da se slovo *A* šifriralo na tri, od četiri moguća načina, tj. u *R, M i A*.

U praksi se za šifriranje upotrebljavao **Vigenerèov kvadrat**:

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

Šifrirano slovo nalazi se u presjeku retka sa slovom ključne riječi i stupca s odgovarajućim slovom otvorenog teksta. Za dešifriranje se koristimo sličnim postupkom, u retku sa slovom ključne riječi pronađe se slovo šifrata, a slovo stupca kojem pripada je slovo otvorenog teksta. U gornjoj tablici je šifrat označen crvenom, a otvoreni tekst plavom bojom.

Matematički model Vigenerèove šifre glasi:

VIGENERÈOVA ŠIFRA

$$\mathcal{P} = \mathcal{K} = \mathcal{C} = (\mathbb{Z}_{26})^m,\ m \in \mathbb{N}.$$

Za ključ $K = (k_1, \ldots, k_m) \in (\mathbb{Z}_{26})^n$ funkcije šifriranja i dešifriranja dane su s

$$e_K(x) = (x_1 + k_1, \ldots, x_m + k_m) \mod 26,$$

$$d_K(y) = (y_1 - k_1, \ldots, y_m - k_m) \mod 26,$$

gdje su $x = (x_1, \ldots, x_m), y = (y_1, \ldots, y_m) \in (\mathbb{Z}_{26})^m$.

Vigenerèova šifra je primjer **blokovne šifre** jer se svaki blok od m elemenata šifrira istim ključem (duljine m). Postoji i inačica ove šifre koja se svrstava u **protočne** šifre. Ona upotrebljava ključ samo na prvom bloku otvorenog teksta, a preostali dio šifrira se uzastopno s pomoću prethodnih dijelova poruke, tj. rabi se tzv. **autoključ**.

Sigurnost klasične Vigenerèove šifre leži upravo u duljini ključa. Krajem 19. stoljeća Friedrich Kasiski je pronašao metodu s pomoću koje se može ustanoviti duljina ključa (**Kasiskijev test**), a početkom 20. stoljeća William Friedman pronalazi još jednu metodu koja upotrebljava tzv. indeks koincidencije, zbog čega se šifra prestaje upotrebljavati.

Svim kriptosustavima (Cezarova, afina i Vigenerèova šifra) koje smo do sada opisali zajedničko je da se svaki element otvorenog teksta zamjenjuje nekim drugim elementom i stoga se oni svrstavaju u tzv. **supstitucijske šifre**. Umjesto toga, ako neka šifra permutira elemente otvorenog teksta, tada se ona naziva **transpozicijska šifra**. Na primjer, ako poruku SIFRA zapišemo kao FASIR, reći ćemo da smo načinili transpoziciju. Općenito, matematički model transpozicijske šifre možemo zapisati:

TRANSPOZICIJSKA ŠIFRA

$$\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m,\ m \in \mathbb{N}$$

$$\mathcal{K} = \{p : \{1, 2, \ldots, m\} \to \{1, 2, \ldots, m\} \ :\ p \text{ je permutacija}\}.$$

Za $p \in \mathcal{K}$ definiramo funkcije šifriranja i dešifriranja kao

$$e_p(x_1, \ldots, x_m) = (x_{p(1)}, \ldots, x_{p(m)}),$$

$$d_p(y_1, \ldots, y_m) = (y_{p^{-1}(1)}, \ldots, y_{p^{-1}(m)}).$$

Ovaj kriptosustav ima "bogat" prostor ključeva jer je broj permutacija, tj. bijekcija m-članog skupa jednak $m!$. No postavlja se pitanje kako praktično i konkretno realizirati ovaj kriptosustav. U praksi se najčešće koristimo **stupčanom transpozicijom** koju opisujemo u sljedećem primjeru.

Primjer 4. Stupčana transpozicija

Pretpostavimo da je $m = 8$ te da smo za ključ šifre odabrali permutaciju

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 5 & 4 & 1 & 6 & 2 & 7 \end{pmatrix}.$$

Poruka koju želimo šifrirati glasi

INFORMACIJE SU VRLO DRAGOCJENA ROBA.

U tablicu s osam stupaca upisujemo otvoreni tekst po redcima:

8	3	5	4	1	6	2	7
I	N	F	O	R	M	A	C
I	J	E	S	U	V	R	L
O	D	R	A	G	O	C	J
E	N	A	R	O	B	A	X

Budući da otvoreni tekst ima 31 slovo, što nije višekratnik od 8, nadopunili smo ga slovom X koje ne mijenja smisao poruke. Šifrat dobijemo tako što iščitamo tekst po stupcima označenim od 1 do 8 redom:

RUGOARCANJDNOSARFERAMVOBCLJXIIOE.

Za dešifriranje podijelimo šifrat u skupine po 4 slova:

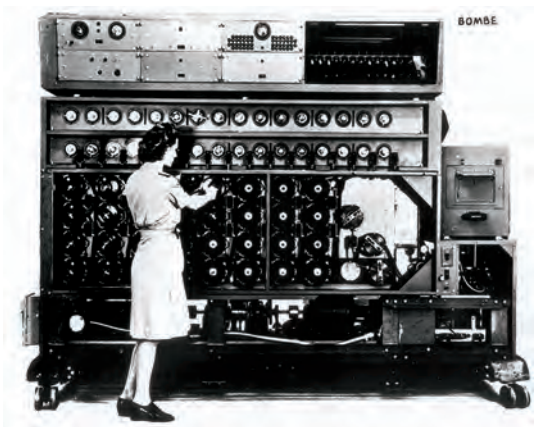
1	2	3	4	5	6	7	8
RUGO	ARCA	NJDN	OSAR	FERA	MVOB	CLJX	IIOE

i zapišemo ih po stupcima u redoslijedu koji je zadan ključem: 8 3 5 4 1 6 2 7.

Za razbijanje šifrata dobivenog stupčanom transpozicijom najprije treba odrediti duljinu ključa (m) koja je neki djelitelj duljine šifrata (n). Odabire se onaj m za koji u pripadnoj tablici dimenzije $(n : m) \times m$, i ispunjenoj po stupcima danim šifratom, dobivamo povoljan omjer samoglasnika i suglasnika (što je u hrvatskom jeziku otprilike $2 : 3$). Nakon toga je potrebno posložiti stupce tako da se u redcima pojavi smisleni tekst. U tu svrhu korisno je poznavati koji su najčešći bigrami u jeziku. Uočimo da frekvencijska analiza slova za transpozicijske šifre nema smisla jer su frekvencije slova u

šifratu iste kao frekvencije slova u otvorenom tekstu.

Šifre koje smo do sada opisali dio su **klasičnih kriptosustava**. Vidjeli smo da njihova sigurnost leži u tajnosti ključa, a iz poznavanja ključa za šifriranje lako možemo odrediti ključ ili postupak za dešifriranje. Takvi se sustavi općenito nazivaju **kriptosustavi s tajnim ključem** ili **simetrični kriptosustavi**. Da bi takvi sustavi bili što sigurniji, trebaju imati što veći prostor ključeva. Nadalje, šifriranje treba biti složenije, zadano algoritmom koji primjenom više iteracija kombinira i supstituciju i transpoziciju. Prije pojave računala takvo su što omogućile **naprave za šifriranje** od kojih je daleko najpoznatija ENIGMA kojom se koristila njemačka vojska tijekom Drugog svjetskog rata. Patentirao ju je Arthur Scherbius 1918. godine. Naprava je izgledala poput pisaćeg stroja na kojem bi pošiljatelj utipkao poruku. Svako slovo poruke bi se mehanički šifriralo, uz pomoć tri rotora i prespojne ploče, nakon čega bi se upalila odgovarajuća žaruljica ispod šifriranog slova. Šifrat se prenosio radiovezom, a primatelj, koji je posjedovao isti uređaj, utipkao bi šifrat i dobio otvoreni tekst. Svaki dan rotori Enigme bi se postavljali u početni položaj zadan kodnom knjižicom, a nakon toga šifrirao se novi dnevni ključ, odnosno nove postavke rotora. Broj mogućih ključeva Enigme je ogroman i iznosi oko $2.6 \cdot 10^{18}$ što sprječava napad grubom silom. Ipak, skupina poljskih matematičara predvođena Marianom Rejewskim te skupina britanskih kriptoanalitičara na čelu s Alanom Turingom razvili su metodu te konstruirali napravu tzv. Bombu kojom su uspješno razbijali šifrate kodirane Enigmom.



Slika 3. Enigma i Bomba

Simetrični kriptosustavi koji se baziraju na nizu supstitucija i transpozicija upotrebljavaju se i danas. Dva najpoznatija, koji su prihvaćeni i kao standardi su DES (Data Encryption Standard) i AES (Advanced Encryption Standard). DES se koristio od 1976., a 1998. je razbijen grubom silom, računalom nazvanim DES Cracker. Od 2001. godine u uporabi je AES čiji je algoritam konstruiran u konačnom polju reda 2^8.

Kriptosustavi s javnim ključem

Kao što smo već istaknuli, sigurnost svakog simetričnog kriptosustava leži u tajnosti ključa, a preporučljivo je i često mijenjanje ključa. No to znači da pošiljatelj i primatelj moraju nekako razmijeniti ključeve, što se u praksi odvija preko nesigurnog komunikacijskog kanala. Godine 1976. američki kriptografi Whitfield Diffie i Martin Hellman predstavili su **protokol za razmjenu ključeva** koji se može realizirati u konačnoj cikličkoj grupi.

Pretpostavimo da je $(G, \cdot)$ ciklička grupa[3] reda n, tj. $|G| = n$ te neka je g generator grupe G, što označavamo $G = (g)$. Tada za svaki element $x \in G$

[3] Grupa je ciklička ako ju možemo generirati s pomoću jednog elementa (npr. svaki element jednak je nekoj potenciji generatora grupe). Svaka ciklička grupa je i Abelova grupa, što znači da je operacija *množenja* komutativna, asocijativna, postoji neutralni element množenja – tzv. jedinica, i svaki element ima svoj inverz u G.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$2^k \mod 19$	1	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10

Tablica 1. Ciklička grupa $\mathbb{Z}_{19}^*$

postoji jedinstven broj $k \in \{0, 1, \ldots, n-2\}$ takav da je

$$x = g^k.$$

Eksponent k naziva se **diskretni logaritam** od x. Primjer takve grupe je

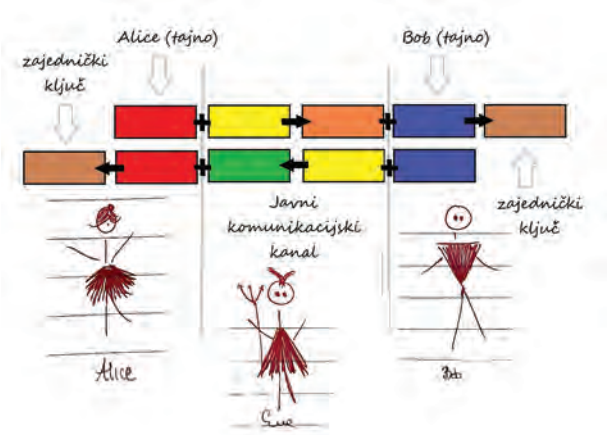
$$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\},$$

uz operaciju množenja modulo p, pri čemu je p prosti broj. Generator ove grupe je primitivni korijen[4] modulo p (obično rabimo najmanji). Na primjer, za $p = 19$ najmanji primitivni korijen je $g = 2$. U tablici 1 je svaki element iz $\mathbb{Z}_{19}^*$ prikazan kao potencija primitivnog korijena – generatora.

Primjer 5. Diffie-Hellmanov protokol za razmjenu ključeva

Pretpostavimo da Alice i Bob žele dogovoriti zajednički ključ u grupi $\mathbb{Z}_{19}^*$. Protokol se sastoji od nekoliko koraka:

(1) Alice i Bob odabiru slučajne brojeve iz skupa $\{0, 1, \ldots, 17\}$. Pretpostavimo da je Alice odabrala $a = 10$, a Bob $b = 13$.



Slika 4. Shema D-H protokola za razmjenu ključeva

(2) Alice šalje Bobu element $x = 2^{10} \mod 19 = 17$, a Bob Alice šalje $y = 2^{13} \mod 19 = 3$.

(3) Alice računa $y^a = 3^{10} \mod 19 = 16$, a Bob $x^b = 17^{13} \mod 19 = 16$.

Nakon ovog protokola Alice i Bob posjeduju isti tajni ključ $K = 16$. Na slici 4 je ovaj protokol shematski prikazan s pomoću miješanja boja.

Zapišimo matematički model ovog protokola.

DIFFIE-HELLMANOV PROTOKOL ZA RAZMJENU KLJUČEVA

Neka je $G = (g)$ ciklička grupa reda n.

(1) Alice odabire broj $a \in \{0, 1, \ldots, n-1\}$, a Bob odabire broj $b \in \{0, 1, \ldots, n-1\}$.

(2) Alice šalje Bobu element $x = g^a$, a Bob Alice šalje $y = g^b$.

(3) Alice računa element y^a, a Bob element x^b, odnosno posjeduju zajednički tajni ključ

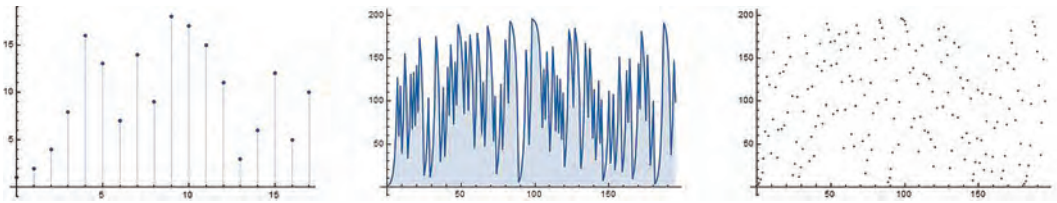
$$K = y^a = (g^b)^a = g^{ab} = (g^a)^b = x^b.$$

Recimo nešto o tome zašto nije lako otkriti tajni ključ dobiven ovim protokolom. Budući da javnim kanalom "putuju" elementi g^a i g^b, naš problem se sastoji u tome da iz poznavanja navedenih elemenata pokušamo otkriti $K = g^{ab}$. To je jedino moguće ako uspijemo naći a (ili b). Konkretno na primjeru 5, trebali bismo iz poznavanja $x = 17$ i $y = 3$, odrediti $K = 16$. To znači da je potrebno odrediti $a \in \{0, 1, \ldots, 17\}$ za koji je

$$2^a \equiv 17 \pmod{19},$$

odnosno treba riješiti **problem diskretnog logaritma**. Kao što možemo zapaziti iz tablice 1, ponašanje potencija 2^k, $k = 0, 1, \ldots, 17$, jest vrlo nepravilno. Štoviše, nalikuje generatoru slučajnih

[4] g je primitivni korijen modulo p ako je g^{p-1} najmanja potencija za koju je $g^{p-1} \equiv 1 \pmod{p}$.



(A) $p = 19$ (B) $p = 197$ (C) $p = 197$

Slika 5. Graf funkcije $k \mapsto 2^k \mod p$

brojeva, što se najbolje vidi na slici 5. Zbog toga se eksponent a može odrediti uzastopnim računanjem potencija, no ta je metoda potpuno neučinkovita ako je p dovoljno velik prosti broj. Postoje algoritmi koji su efikasniji (npr. Shanksov algoritam i Pollardov ρ algoritam), no niti oni nisu dovoljno brzi za velike p. Stoga se problem diskretnog logaritma smatra *teškim* problemom. Napominjemo da se modularno potenciranje može izvršiti vrlo učinkovito s pomoću metode koja se naziva **kvadriraj i množi** ili **binarne ljestve**.

Problem razmjene ključeva je, osim opisanog protokola, doveo do ideje **asimetričnog kriptosustava**, odnosno **kriptosustava s javnim ključem** u kojem bi iz poznavanja funkcije šifriranja, bilo nemoguće odrediti funkciju dešifriranja. U praksi se pod pojmom nemoguće uglavnom misli na nemogućnost dekriptiranja u realnom vremenu. Stoga bi funkcija šifriranja (e_K) bila **javna**, a funkcija dešifriranja (d_K) **tajna**. U tu svrhu trebale bi poslužiti tzv. **jednosmjerne** funkcije, tj. funkcije (ili operacije) koje se u "jednom smjeru" računaju lako, a u drugom teško (tj. teško im je odrediti inverz). Kao primjer takve funkcije može poslužiti potenciranje i računanje diskretnog logaritma u konačnoj grupi o kojima smo već govorili. Nadalje, jednostavan model pruža nam i problem faktorizacije velikih brojeva – pomnožiti dva broja je lako, a faktorizirati puno teže. Na taj način razmišljali su Ron Rivest, Adi Shamir i Len Adleman i 1977. godine predstavljajući svoj kriptosustav s javnim ključem tzv. **RSA kriptosustav**.

U konstrukciji RSA kriptosustava rabi se **Eulerova funkcija** $\varphi : \mathbb{N} \to \mathbb{N}$, gdje je $\varphi(n)$ jednak broju elemenata skupa $\{1, \ldots, n\}$ koji su relativno prosti s n. Lako se može ustanoviti da je $\varphi(p) = p - 1$ za svaki prosti broj p. Nadalje, Eulerova funkcija je multiplikativna funkcija, što znači da je

$$\varphi(mn) = \varphi(m)\varphi(n),$$

za sve relativno proste brojeve $m, n \in \mathbb{N}$. Važna će nam biti i tvrdnja **Eulerova teorema**: Za relativno proste brojeve $a, n \in \mathbb{N}$ je

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

odnosno $a^{\varphi(n)}$ pri dijeljenju brojem n daje ostatak 1.

RSA KRIPTOSUSTAV

Neka je $n = pq$, gdje su p i q različiti prosti brojevi.

$$\mathcal{P} = \mathcal{C} = \mathbb{Z}_n,$$

$$\mathcal{K} = \{(n, p, q, d, e) : de \equiv 1 \pmod{\varphi(n)}, 1 < d, e < \varphi(n)\},$$

pri čemu je (n, e) *javni* ključ, a (p, q, d) *tajni* ključ.

Za $K \in \mathcal{K}$ funkcije šifriranja i dešifriranja su

$$e_K(x) = x^e \mod n,\ d_K(y) = y^d \mod n, \quad x, y \in \mathcal{P}.$$

Uočimo da je

$$d_K(e_K(x)) = x.$$

Zaista, ako je $\operatorname{nzd}(x, n) = 1$, tada je zbog Eulerova teorema

$$d_K(e_K(x)) = (x^e)^d = x^{ed} = x^{k\varphi(n)+1} = x^{k\varphi(n)} \cdot x \equiv x \pmod{n},$$

a budući da su $d_K(e_K(x))$, $x \in \mathbb{Z}_n$, slijedi jednakost. (I u ostalim slučajevima, tj. za $\text{nzd}\,(x,n) \in \{p,q,n\}$ može se pokazati da vrijedi jednakost.)

Primjer 6. RSA kriptosustav

Neka je

$$p = 7,\ q = 13,\ n = pq = 91.$$

Zbog multiplikativnosti funkcije φ vrijedi

$$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = 72.$$

Sada odabiremo dio javnog ključa – eksponent e takav da je $\text{nzd}\,(e, \varphi(n)) = 1$. Uzmimo na primjer $e = 5$. Za tajni dio ključa treba pronaći $d \in \mathbb{N}$ takav da je $de \equiv 1 \pmod{\varphi(n)}$, odnosno treba riješiti kongruenciju

$$5d \equiv 1 \pmod{72}.$$

Dobivamo da je $d = 29$. (Linearne kongruencije efikasno se rješavaju Euklidovim algoritmom.) Dakle, parametri ovog kriptosustava su:

javni ključ	tajni ključ
$(n,e) = (91,5)$	$(p,q,d) = (7,13,29)$

Tablica 2.

Ako je dan otvoreni tekst $x = 23$, tada s pomoću javnog ključa dobivamo šifrat

$$y = 23^5 \mod 91 = 4,$$

a dešifriramo s pomoću tajnog ključa

$$x = 4^{29} \mod 91 = 23.$$

Sigurnost ovog kriptosustava leži u težini faktorizacije broja n posebice jer su u praksi brojevi p i q ogromni – imaju barem stotinu znamenaka. Bez poznavanja faktorizacije broja n ne možemo odrediti vrijednost Eulerove funkcije $\varphi(n) = (p-1)(q-1)$, a ta nam je vrijednost potrebna da bismo odredili tajni eksponent d iz kongruencije $ed \equiv 1 \pmod{\varphi(n)}$. Iz tog se razloga faktorizacija $n = pq$ naziva *trapdoor* što bi se moglo prevesti kao "skriveni ulaz". Jednosmjerne funkcije čiji se inverz može lako izračunati uz dodatni podatak nazivaju se **osobne jednosmjerne funkcije**. Dakle, funkcija šifriranja u RSA kriptosustavu je osobna jednosmjerna funkcija čiji je *trapdoor* barem jedan od faktora broja n.

Sama veličina prostih brojeva p i q ponekad ne mora biti garancija sigurnosti. Ako su p i q približno jednaki, faktorizacija broja n može se brzo naći jer su faktori približno jednaki $\sqrt{n}$. Nije preporučljivo da brojevi $p-1$ i $q-1$ budu *glatki*, tj. da imaju puno malih prostih djelitelja. Izbor tajnog eksponenta e koji mora biti relativno prost s brojem $\varphi(n) = (p-1)(q-1)$ također je važan. Da bi se šifriranje odvijalo što brže, bilo bi dobro da eksponent bude što manji. Tako se dugo rabio eksponent $e = 3$, no ako je ista poruka šifrirana 3 puta istim eksponentom i trima različitim modulima (n_1, n_2, n_3), šifrat se lako može dekriptirati uz pomoć Kineskog teorema o ostatcima. Zato se preporuča korištenje većeg eksponenta, ali koji u binarnom zapisu ima puno više nula nego jedinica jer se potenciranje izvršava s pomoću brzog, već spomenutog, algoritma *kvadriraj i množi* (koji "množi" samo u slučaju jedinice u binarnom zapisu broja e). Valja napomenuti kako je šifriranje s pomoću asimetričnog kriptosustava puno sporije nego s pomoću simetričnog, zato se u praksi koriste tzv. **hibridni kriptosustavi** koji su kombinacija tih dvaju sustava.

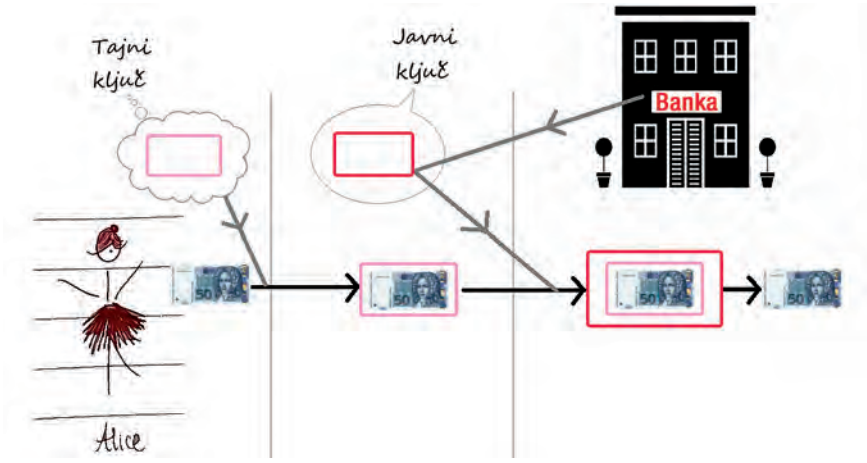
Modeli digitalnog potpisa

Digitalni potpis može se konkretno realizirati s pomoću kriptosustava s javnim ključem. Predstavit ćemo tri modela. Prvi, najjednostavniji model je zapravo čista primjena nekog kriptosustava s javnim ključem.

Primjer 7. Digitalni potpis – model 1

Pretpostavimo da se banka za provjeru transakcija koristi RSA kriptosustavom. Recimo da je Alice klijentica banke kojoj je za transakciju dodijeljen ključ s parametrima iz primjera 6:

$$K = (n,p,q,d,e) = (91,7,13,29,5).$$



Slika 6. Digitalni potpis – model 1

Alice želi obaviti transakciju u banci u vrijednosti 50 kuna pa s pomoću svog tajnog ključa $(7, 13, 5)$ šifrira $x = 50$ i banci šalje poruku

$$y = 50^5 \mod 91 = 85.$$

Banka ju dešifrira s pomoću njenog javnog ključa $(91, 29)$ i dobiva iznos transakcije

$$x = 85^{29} \mod 91 = 50.$$

Model 1 ne predstavlja siguran digitalni potpis i može lako postati meta napada. Uočimo da banka ne može biti sigurna da je zahtjev za transakciju upravo poslala Alice. Može se dogoditi da Eve pošalje "slučajnu" poruku banci, npr. $y = 19$ i ona nakon otključavanja s Alisinim ključem prelazi u smislenu poruku $x = 80$. Ovaj se napad naziva **egzistencijalni falsifikat** (engl. *existential forgery*). Nadalje, šifriranje u RSA je multiplikativna operacija, pa ako Alice istim ključem šifrira dvije poruke i dobije šifrate npr. $y_1 = 4$ i $y_2 = 9$, tada je i $y_1 y_2 = 36$ (ili općenito $y_1 y_2 \mod n$) element iz prostora šifrata jer je

$$y_1 y_2 \equiv x_1^e x_2^e = (x_1 x_2)^e \pmod{n}.$$

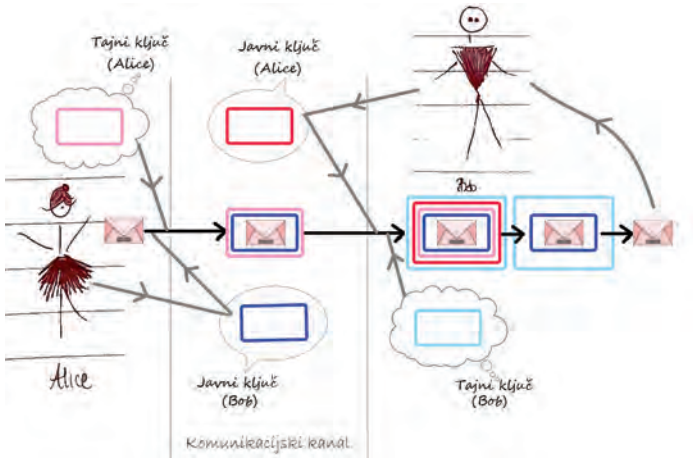
Model 2 bazira se na ideji da se poruka "omota" javnim ključem primatelja i tajnim ključem pošiljatelja. Konkretno, pretpostavimo da Alice posjeduje javni ključ j_A i tajni ključ t_A te analogno da Bob posjeduje j_B i t_B. Ako Alice šalje Bobu poruku x, ona će je najprije šifrirati Bobovim javnim ključem j_B, a zatim svojim tajnim t_A te komunikacijskim kanalom poslati šifrat:

$$y = t_A(j_B(x)) = t_A \circ j_B(x).$$

Kako bi dešifrirao poruku, Bob najprije primjenjuje javni Alisin ključ j_A, a zatim svoj tajni ključ t_B:

$$t_B(j_A(y)) = t_B(j_A(t_A(j_B(x)))) = t_B(\underbrace{j_A \circ t_A}_{=id}(j_B(x)))$$

$$= \underbrace{t_B \circ j_B}_{=id}(x) = x.$$



Slika 7. Digitalni potpis – model 2

Ako Bob dobije smislenu poruku, onda je siguran da ju je poslala Alice. Ovaj model može se realizirati kriptosustavima javnog ključa za koje su prostori otvorenog teksta i šifrata jednaki ($\mathcal{P} = \mathcal{C}$).

Primjer 8. Digitalni potpis – model 2

Neka su parametri za RSA kriptosustav dani s izrazom

$$(n, p, q) = (91, 7, 13).$$

Stoga je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{91}$. Tajni eksponent (ključ) korisnika K označit ćemo s e_K, a javni s d_K, a odgovarajuće funkcije – javnu i tajnu s $t_K, j_K : \mathbb{Z}_n \to \mathbb{Z}_n$,

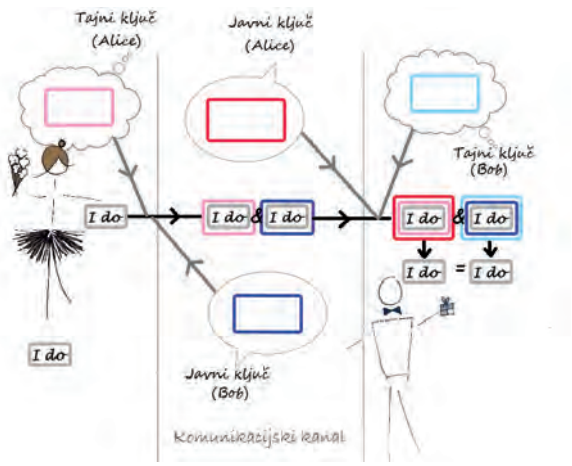
$$t_K(x) = x^{e_K} \mod n,\ j_K(x) = x^{d_K} \mod n,\ x \in \mathbb{Z}_n.$$

Daljnji postupak je raspisan u tablici 3.

Problem koji može nastupiti u modelu jest da primatelj ne može biti sasvim siguran kako tijekom slanja poruke nije došlo do neke promjene u sadržaju poslane poruke. Zbog toga je potrebno dodati **algoritam za verifikaciju** koji predstavljamo u modelu 3.

Primjer 9. Digitalni potpis – model 3

Koristeći se istim parametrima za RSA kriptosustav iz primjera 8, Alice javnim kanalom šalje dvije kriptirane poruke: jednu koristeći svoj tajni ključ, a drugu koristeći Bobov javni ključ. Po primitku istih Bob ih može dešifrirati s pomoću svog tajnog ključa i javnog Alisinog ključa od (tablica 4).



Slika 8. Digitalni potpis – model 3

	Alice	javni kanal	Bob
modul		$n = 91$	
eksponent	$e_A = 5$	$d_A = 29,\ d_B = 31$	$e_B = 7$
poruka	$\boxed{x = 50}$		
šifriranje	$(50^{31})^5 \mod 91 = 71$		
šifrat		$y = 71$	
dešifriranje			$(71^{29})^7 \mod 91 = 50$
poruka			$\boxed{x = 50}$

Tablica 3.

	Alice	javni kanal	Bob
modul		$n = 91$	
eksponent	$e_A = 5$	$d_A = 29,\ d_B = 31$	$e_B = 7$
poruka	$\boxed{x = 50}$		
šifriranje	$50^5 \mod 91 = 85$ $50^{31} \mod 91 = 15$		
šifrat		$(y_1, y_2) = (85, 15)$	
dešifriranje/ verifikacija			$85^{29} \mod 91 = 50$ $15^7 \mod 91 = 50$
poruka			$\boxed{x = 50}$

Tablica 4.

Model 3 ispunjava zahtjeve digitalnog potpisa koje smo istaknuli na samom početku: vjerodostojnost, netaknutost i nepobitnost. Naime, Bob zna da je samo Alice mogla poslati poruku (jer se "otključava" njenim tajnim ključem), nadalje zna da se poruka nije promijenila tijekom slanja (jer je verificirana njegovim tajnim ključem) i konačno Alice ne može zanijekati slanje poruke (jer ju je potpisala svojim tajnim ključem). Općenito, kriptosustav digitalnog potpisa definira se na sljedeći način.

Definicija 2. ***Kriptosustav digitalnog potpisa*** *je uređena petorka* $(\mathcal{S}, \mathcal{D}, \mathcal{K}, \mathcal{F}, \mathcal{V})$ *za koju vrijedi:*

1) $\mathcal{S}$ *je konačan skup svih mogućih elemenata potpisa*
2) $\mathcal{D}$ *je konačan skup svih mogućih elemenata digitalnog potpisa*
3) $\mathcal{K}$ *je konačan skup svih mogućih ključeva*
4) $\mathcal{F}$ *je skup svih funkcija potpisivanja, a* $\mathcal{V}$ *skup svih funkcija verifikacije takvih da za svaki ključ* $K \in \mathcal{K}$ *postoji funkcija potpisivanja* $\operatorname{sig}_K : \mathcal{S} \to \mathcal{D}$ *u* $\mathcal{F}$ *i odgovarajuća funkcija verifikacije* $\operatorname{ver}_K : \mathcal{S} \times \mathcal{D} \to \{0,1\}$ *iz* $\mathcal{V}$ *za koje je*

$$\operatorname{ver}_K(x,y) = \begin{cases} 1, & \text{ako } y = \operatorname{sig}_K(x) \\ 0, & \text{ako } y \neq \operatorname{sig}_K(x) \end{cases}.$$

Ako je $\operatorname{ver}_K(x,y) = 1$*, potpis je valjan, a u suprotnom, ako je* $\operatorname{ver}_K(x,y) = 1$ $\operatorname{ver}_K(x,y) = 0$*, potpis se smatra* ***krivotvorinom***.

U stvarnim modelima digitalnog potpisa osim asimetričnog kriptiranja pojavljuju se i *kriptografske hash funkcije*, odnosno *funkcije sažimanja* koje također doprinose očuvanju integriteta poruke i provjeri autentičnosti. Ukratko, *hash* funkcije općenito nisu bijektive (jer pojednostavljeno rečeno preslikavaju veći skup na manji) i ubrajaju se u jednosmjerne funkcije (– iz poznavanja vrijednosti funkcije teško je odrediti prasliku). Iako je moguće da se *hash* fukcija podudara na različitim vrijednostima, to je vrlo malo vjerojatno i u praksi se ne događa. Dobra *hash* funkcija još ima svojstvo da male razlike na ulaznim podatcima dovode do velikih razlika u izlaznim podatcima. Konkretno, ako Alice potpisuje neki službeni dokument, ona svojim tajnim (osobnim) ključem potpisuje njegov *sažetak*, tj. njegovu *hash* vrijednost. Nakon toga Bob uspoređuje *hash* vrijednost dokumenta s porukom koja je dekriptirana javnim Alisinim ključem. Ako se oni podudaraju, Bob zaključuje da je sadržaj poruke (dokumenta) nepromijenjen te da ga je potpisala Alice.

Primjer 10. *Hash* **funkcija**

Pretpostavimo da Alice želi potpisati poruku $x = 150$, a njezin ključ zadan je RSA kriptostavom modula $n = 91$. Jednostavna jednosmjerna funkcija je kvadriranje, pa ćemo, s obzirom da kodomena mora biti $\mathbb{Z}_{19}$, *hash* funkciju zadati izrazom

$$x \mapsto x^2 \mod n.$$

Stoga će Alice potpisati *hash* vrijednost poruke $150^2 \mod 91 = 23$.

Moderna kriptografija, u kojoj važnu ulogu ima i digitalni potpis, omogućava komunikacijsku i računalnu sigurnost. Ovdje smo pokazali da se mnoge kriptografske ideje temelje na različitim matematičkim konceptima, posebice onima iz teorije brojeva. No važnu ulogu imaju još neke grane matematike kao što su računska teorija složenosti i vjerojatnost. Štoviše, moderna kriptografija je interdisciplinarna znanost koja, osim matematičara, uključuje IT stručnjake, elektrotehničare i fizičare. Ona se vrlo dinamično razvija jer mora držati korak s tehnološkim razvojem. U budućnosti, ako ili kad zažive kvantna računala, morat će se implementirati sasvim drukčiji modeli kriptosustava. Postkvantna kriptografija već se snažno razvija, ali to je tema za neki drugi rad.

LITERATURA

1/ M. Barun, A. Dujella, Z. Franušić (2008.): Kriptografija u školi, *Poučak*, 33, str. 40–52.

2/ H. Čavrak: Enigma, *Hrvatski matematički elektronski časopis math.e*, broj 3, `http://e.math.hr/old/enigma/index.html`

3/ A. Dujella (2019.): *Teorija brojeva*, Školska knjiga, Zagreb.

4/ A. Dujella, M. Maretić (2007.): *Kriptografija*, Element, Zagreb, 2007.

5/ B. Ibrahimpašić, E. Liđan (2010.): Digitalni potpis, *Osječki matematički list*, Vol. 10 No. 2, str. 139–148.

6/ D. R. Stinson (2006.): *Cryptography: Theory and Practice*, Third Edition – Solutions Manual; Chapman & Hall/CRC, Sveučilište Waterloo, Ontario.

Izvori slika:

Slika 2: `http://inventwithpython.com/cipherwheel/`

Slika 3: `https://en.wikipedia.org/wiki/Enigma_machine` `https://www.britannica.com/topic/Bombe`

Likove u shemama kriptosustava nacrtala je Lucija Franušić.