O matematici digitalnog potpisa

Šarić, Rebeka

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Rebeka Šarić

O MATEMATICI DIGITALNOG POTPISA

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Zrinka Franušić

Zagreb, rujan, 2022.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Posebnu zahvalu upućujem svojoj mentorici na susretljivosti te uloženom vremenu i trudu prilikom pisanja ovog diplomskog rada. Zahvaljujem se svim prijateljima koji su mi uljepšali studentski život. Najveće hvala ide mojoj obitelji na breskompromisnoj podršci, ljubavi i razumijevanju tijekom studija i života. Posebno hvala ide i tebi na razumijevanju i strpljenju tijekom ovih studentskih godina, a i svih onih ranije.

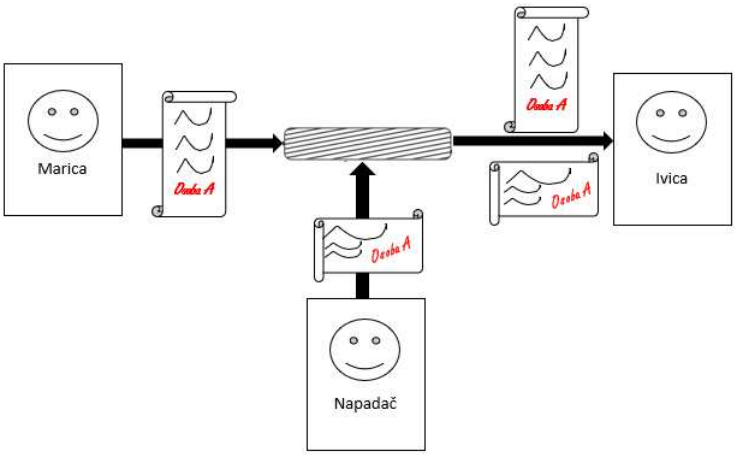
Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Sadržaj

Uvod

U današnje vrijeme primjena digitalnog potpisa sve više raste. Koristi se za potpisivanje električkih dokumenata kao što su elektronički ugovori, pisma, bankovne transakcije i slično. Digitalni potpis ima slična obilježja kao i vlastoručan potpis te je zamjena za isti u elektroničkom obliku. Glavno pitanje koje se postavlja sigurnost je korištenja digitalnog potpisa. Kada bi Marica (pošiljalac) ručno potpisala dokument, onda bi svi koji znaju njezin potpis mogli potvrditi da je uistinu ona potpisala taj dokument. Na sličan način funkcionira i digitalni potpis. Marica želi potpisati neki dokument d i koristi tajni ključ za generiranje potpisa m, a Ivica (primalac) koristeći odgovarajući javni ključ tada može potvrditi da je m uistinu potpis od d.

Kako bi digitalni ključ bio pravovaljan, treba zadovoljiti određene kriterije kao što su *nepobitnost*, *netaknutost* i *vjerodostojnost*. Ako Ivica zna da je samo Marica mogla poslati poruku koju je on upravo primio, digitalni potpis je vjerodostojan.



Kažemo da je digitalni potpis netaknut ako Ivica zna da poruka koju je poslala Marica nije promijenjena prilikom slanja. Ako Marica ne može zanijekati da je poslala poruku, digitalni potpis je nepobitan. U radu su izloženi zakoni Republike Hrvatske te Europske

unije povezani s digitalnim potpisom.

Digitalno potpisivanje omogućuju kriptosustavi javnog ključa ili asimetrični kriptosustavi. Oni su se pojavili 70-tih godina 20. stoljeća, a za šifriranje koriste funkcije koje se računaju lako, ali njihovi inverzi vrlo teško. Za takve funkcije kažemo da su jednosmjerne. Iz toga slijedi da samo funkcija za dešifriranje mora biti tajna, dok funkcija za šifriranje može biti javna. Pri samoj konstrukciji jednosmjernih funkcija koriste se neki teški matematički problemi, kao što je primjerice faktorizacija velikih prirodnih brojeva. U radu je dan kratki uvid u kriptografiju općenito te su opisani RSA i ElGamalov kriptosustav javnog ključa te pripadne sheme digitalnog potpisa uz primjere.

Poglavlje 1

Uvod u kriptografiju

Znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka tako da ih može pročitati samo onaj kojem su one namijenjene naziva se ***kriptografija***. *Kriptoanaliza* ili *dekriptiranje* je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa. Grana znanosti koja obuhvaća i kriptografiju i kriptoanalizu je *kriptologija*.

1.1 Kriptografija kroz povijest

Kriptografija dolazi od riječi *kriptos* za skriven i *grafo* za pisati, grčkog je podrijetla i može se prevesti kao ***skriveno pisanje*** ili ***tajnopis***. Posebno je zanimljivo da početke šifriranja poruka možemo pronaći još u 5. stoljeću prije Krista kod starih Grka. Kroz povijest, od starih Grka pa sve do danas ljudi su željeli sigurno komunicirati, ali bili su svjesni da poruke putuju nesigurnim komunikacijskim kanalima. Iako su se načini prenošenja poruka promijenili, glavni problem ostao je isti – kako sigurno prenijeti poruku, tj. kako onemogućiti onom koji nadzire komunikacijski kanal da sazna sadržaj poruke koja se prenosi. Upravo je to zadaća kriptografije. Kroz povijest, ona je imala važnu diplomatsku i vojnu ulogu te je odlučivala o ishodima bitaka i sudbinama špijuna, a danas ona ima važnu ulogu u osiguravanju sigurnosti internetskih transakcija i komunikacija te se stoga u velikoj mjeri bavi podatcima u digitalnom obliku. Postupci kriptiranja i dekriptiranja matematičke su prirode, a provode se uz pomoć računala čime je suvremena kriptografija postala informatička disciplina koja se temelji na teoriji brojeva. Teorija brojeva je grana matematike koja se bavi proučavanjem svojstava cijelih brojeva kao što su rastav na proste faktore, djeljivost, rješivost jednadžbi u skupu cijelih brojeva, itd.

Najčešće korištene metode šifriranja poruka u prošlosti bile su *transpozicija* ili premještanje osnovnih elemenata teksta te *supstitucija* ili zamjena. Takve metode obilježile

su predznanstveno razdoblje klasične kriptografije. Kombinacija ovih metoda nalazi se i u suvremenim simetričnim kriptosustavima. Smatra se da znanstveno razdoblje kriptografije započinje objavom djela C. E. Shannona: *Komunakacijska teorija tajnih sustava*, 1949. godine. S druge strane, postoje i asimetrični kriptosutavi poznati i kao kriptosustavi s javnim ključem koji su se pojavili 1970-ih godina. Njihovom pojavom riješen je problem klasične kriptografije, tj. oni su omogućili sigurnu razmjenu ključeva jer za šifriranje primjenjuju funkcije koje se lako računaju, ali čiji se inverzi računaju vrlo teško pa samo funkcija za dešifriranje mora biti tajna dok funkcija za šifriranje može biti javna.

1.2 Osnovni pojmovi kriptografije

Glavni zadatak kriptografije je omogućiti *pošiljaocu* i *primaocu* komuniciranje preko nesigurnog komunikacijskog kanala tako da treća osoba ne može razumjeti njihove poruke. Komunikacijski kanali mogu biti telefonska linija ili računalna mreža, a treća osoba može nadzirati te komunikacijske kanale. Za poruku koju pošiljalac šalje primaocu koristi se naziv *otvoreni tekst*. Pomoću unaprijed dogovorenog ključa pošiljalac transformira otvoreni tekst. Postupak se naziva *šifriranje*, a dobiveni rezultat *šifrat* ili *kriptogram*. Potom pošiljalac šalje šifrat preko komunikacijskog kanala te primalac koji zna *ključ* kojim je šifrirana poruka može dešifrirati šifrat i odrediti otvoreni tekst, a protivnik može doznati šifrat, ali ne može odrediti otvoreni tekst. Shematski prikaz klasične kriptografije nalazi se na slici 1.1.

Slika 1.1: Shematski prikaz klasične kriptografije

Matematička funkcija koja se koristi za šifriranje i dešifriranje je *kriptografski algoritam* ili *šifra*. Riječ je o dvije funkcije pri čemu jedna služi za šifriranje (preslikava osnovne elemente otvorenog teksta u osnovne elemente šifrata), a druga za dešifriranje (preslikava osnovne elemente šifrata u osnovne elemente otvorenog teksta). Elementi otvorenog teksta mogu biti bitovi, slova te grupe bitova ili slova. Same funkcije se biraju u ovisnosti o ključu

iz određene familije funkcija. *Prostor ključeva* je skup svih mogućih vrijednosti ključeva, a *kriptosustav* se sastoji od kriptografskog algoritma i svih mogućih otvorenih tekstova, ključeva i šifrata.

Definicija 1.2.1. ***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 teskta;*
2) $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elemenata šifrata;*
3) $\mathcal{K}$ *je prostor ključeva, tj. konačan skup svih mogućih ključeva;*
4) Za svaki $K \in \mathcal{K}$ *postoji funkcija šifriranja* $e_K \in \mathcal{E}$ *i odgovarajuća funkcija dešifriranja* $d_K \in \mathcal{D}$*. Pritom su* $e_K : \mathcal{P} \to \mathcal{C}$ *i* $d_K : \mathcal{C} \to \mathcal{P}$ *funkcije sa svojstvom da je* $d_K(e_K(x)) = x$ *za svaki otvoreni tekst* $x \in \mathcal{P}$*.*

Iz definicije 1.2.1 slijedi da je funkcija šifriranja e_K injekcija za svaki $K \in \mathcal{K}$. Kada to ne bi bilo tako, poruka bi bila dvosmislena, odnosno za dva različita otvorena teksta x_1 i x_2 primalac ne bi mogao odrediti treba li y dešifrirati u x_1 ili x_2 jer bi vrijedilo $e_K(x_1) = e_K(x_2) = y$.

Napominjemo da ako pošiljatelj želi poslati poruku s više elemenata otvorenog teksta

$$x = (x_1, x_2, x_3, \ldots, x_n) \in \mathcal{P}^n,$$

za neki $n \in \mathbb{N}$, pripadni šifrat je oblika

$$y = (e_K(x_1), e_K(x_2), e_K(x_3), \ldots, e_K(x_n)) \in \mathcal{C}^n$$

uz $K \in \mathcal{K}$.

1.3 Klasifikacija kriptosustava

Kriptosustave možemo razvrstati prema:

- tipu operacija koje se koriste pri šifriranju
- načinu na koji se obrađuje otvoreni tekst
- tajnosti i javnosti ključeva.

Tip operacija koje se koriste pri šifriranju
S obzirom na tip operacija koje se koriste pri šifriranju razlikujemo *supstitucijske šifre* i *transpozicijske šifre*. Kada se svaki element otvorenog teksta zamjenjuje s nekim drugim elementom govorimo o supstitucijskoj šifri, a kada se elementi otvorenog teksta premještaju (permutiraju), onda govorimo o transpozicijskoj šifri. Primjerice, ako riječ ATLAS šifriramo u LTASA, načinili smo transpoziciju, a ako je šifriramo u CVNCU, onda smo

načinili supstituciju. Napomenimo da postoje kriptosustavi koji kombiniraju ove dvije metode.

Način na koji se obrađuje otvoreni tekst
S obzirom na načina na koji se obrađuje otvoreni tekst postoji podjela na *blokovne šifre*, gdje se obrađuje jedan po jedan blok elemenata otvorenog teksta koristeći jedan te isti ključ, te *protočne šifre* koje obrađuju elemente otvorenog teksta jedan po jedan koristeći pritom paralelno generirani niz ključeva.

Tajnost i javnost ključeva
S obzirom na tajnost i javnost ključeva razlikujemo *simetrične kriptosustave* i *kriptosustave s javnim ključem*. Razlika je da se kod simetričnih ili konvencionalnih kriptosustava, ključ za dešifriranje može izračunati poznajući ključ za šifriranje i obratno, to jest oni su najčešće identični pa sigurnost takvih kriptosustava leži upravo u tajnosti ključeva odakle slijedi i naziv *kriptosustavi s tajnim ključem*. Dok se kod kriptosustava s javnim ključem ili asimetričnih kriptosustava ključ za dešifriranje ne može izračunati iz ključa za šifriranje. Tako ovdje sigurnost leži u tome da je ključ za šifriranje javni ključ te bilo tko može šifrirati poruku pomoću njega, ali samo osoba koja ima odgovarajući ključ za dešifriranje, privatni ili tajni ključ, može dešifrirati tu poruku.

1.4 Jednostavni simetrični kriptosustavi

1.4.1 Cezarova šifra

Opisat ćemo način šifriranja koji potječe od rimskog vojskovođe Julija Cezara, a koji se sastoji u tome da se svako slovo otvorenog teksta, tj. poruke, zamijeni slovom koje se nalazi n mjesta dalje u abecedi. Dakle, riječ je o supstitucijskoj šifri. Sam Cezar je u komunikaciji sa svojim prijateljima koristio šifru u kojoj su se slova otvorenog teksta zamjenjivala slovima koja su se nalazila tri mjesta dalje od njih u abecedi, a postoje indikacije da je prvi rimski car August, Cezarov nećak, pomicao slova za samo jedno mjesto u abecedi, odnosno koristio je najjednostavniju verziju ove šifre uz $n = 1$. U primjerima ćemo se koristiti engleskom abecedom i pretpostavit ćemo da se ona ciklički nastavlja (nakon Z ponovno dolazi A).

Tako bi se primjerice otvoreni tekst

JULIJANSKI KALENDAR UVEO JE GAJ JULIJE CEZAR

pomakom za tri mjesta udesno šifrirao u

MXOLMDVNL NDOHQGDU XYHR MH JDM MXOLMH FHCDU.

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

Slika 1.2: Prikaz Cezarove šifre uz $n = 3$

Matematički model Cezarove šifre

Kako bismo Cezarovu šifru definirali u smislu ranije uvedene definicije 1.2.1, uvodimo korespodenciju između slova abecede (A-Z) i cijelih brojeva (0-25) tako da svakom slovu abecede jednoznačno pridružimo njegov redni broj krenuvši od 0. Oznaku $\mathbb{Z}_{26}$ koristimo za skup $\{0, 1, 2, 3, \ldots, 25\}$, a tom skupu su jednaki prostor otvorenog teksta, prostor šifrata i prostor ključeva, tj.

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

Šifriranje i dešifriranje može se opisati funkcijama:

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

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

pri čemu je $0 \leqslant n \leqslant 25$ ključ ove šifre.

Funkcija a mod 26, za neki cijeli broj a, označava ostatak pri dijeljenju broja a s 26 (koji je jedinstven prema Teoremu o dijeljenju s ostatkom). Na skupu $\mathbb{Z}_{26}$ definirane su operacije zbrajanja, oduzimanja i množenja modulo 26 na način da se rezultat dobiven odgovarajućom operacijom, ako nije iz skupa {0,1,2,3,...,25}, zamijeni s njegovim ostatkom pri dijeljenju s 26. Skup $\mathbb{Z}_{26}$ uz operacije zbrajanja i množenja modulo 26 čini komutativni prsten s jedinicom.

Osnovni elementi otvorenog teksta u Cezarovoj šifri su slova, odnosno njihovi numerički ekvivalenti, a ključ n određuje za koliko mjesta udesno pomičemo slova pri šifriranju.

Dekriptiranje šifrata dobivenog Cezarovom šifrom

Neke od metoda dekriptiranja su primjena *„grube sile"* i *frekvencijska analiza slova*. Ako ispitujemo sve moguće ključeve redom dok ne dobijemo neki smisleni tekst koristimo se metodom „grube sile". S obzirom da je broj ključeva mali (ima ih upravo onliko koliko i slova - 26), to i nije toliko teško. Primjerice ako šifrat glasi „HJEFW", upotrebom „grube sile" dekriptiranje je prikazano na slici 1.3 te se može vidjeti da se relativno brzo može doći do otvorenog teksta.

H J E F W za $n = 0$,
G I D E V za $n = 1$,
F H C D U za $n = 2$,
E G B C T za $n = 3$,
D F A B S za $n = 4$,
C E Z A R za $n = 5$.

Slika 1.3: Prikaz dekriptiranja šifrata „HJEFW" upotrebom metode „grube sile"

Dekriptiranje frekvencijskom analizom slova temelji se na činjenici da se u svakom jeziku neka slova pojavljuju češće od drugih. Otkrivanjem najfrekventnijeg slova u šifratu i poistovjećivanjem njega s najfrekeventnijim slovom nekog jezika možemo doći do otvorenog teksta. Stoga je za korištenje ove metode korisno znati na kojem je jeziku pisan tekst jer su najfrekventnija slova recimo enegleskog jezika redom E, T, A, O, I, a hrvatskog jezika A, I, O, E, N. Primjerice, ako šifrat glasi

GIDEVSZE WEPEXE,

tražimo najfrekventnije slovo u tom šifratu. To je slovo E koje se u šifratu pojavljuje 5 puta. Uz pretpostavku da je otvoreni tekst pisan na hrvatskom jeziku i da se radi o slovu A, dobivamo otvoreni tekst

CEZAROVA SALATA.

1.5 Naprave za šifriranje

Spomenut ćemo i neke naprave koje su bile kroz povijest korištene za šifriranje.

Skital

Kao što je već navedeno, neki elementi kriptografije bili su prisutni još kod starih Grka. Spartanci, u 5. stoljeću prije Krista, koriste prvu kriptografsku napravu za šifriranje **skital** ili **scitala** prikazanu na slici 1.4[1]. Naziv dolazi od grčke riječi za palicu. Skital je bio drveni štap oko kojeg se omotala vrpca od pergamenta. Na namotanoj vrpci, pošiljalac je napisao otvoreni tekst uzduž štapa, a kada se ona odmotala, izgledalo je kao da se na njoj nalazi besmislen niz slova. Poruku je mogao pročitati samo onaj koji je imao štap jednake debljine. Ujedno, ovo je i primjer transpozicijske šifre.

[1] Slika 1.4 preuzeta s https://security.foi.hr/wiki/index.php/Linearna_kriptoanaliza.html

Slika 1.4: Skital

Jeffersonov kotač za šifriranje nosi naziv po svojem izumitelju Thomasu Jeffersonu. Kotač je prikazan na slici 1.5[2] te se sastoji od drvenog cilindra s rupom u sredini kroz koju je povučena željezna os. Cilindar je presječen na 26 manjih cilindara jednakih širina koji se mogu okretati oko zajedničke osi neovisno jedan od drugoga. 26 jednakih kvadratića nalazi se na vanjskom dijelu svakog diska te se na proizvoljan način popunjavaju s 26 slova engleske abecede i to različito od diska do diska. Pošiljalac i primalac imaju dva identična kotača. Kako bi se šifrirao otvoreni tekst, pošiljalac podijeli tekst na blokove od po 26 slova, a blok se šifrira tako da se rotiranjem diskova u jednom od 26 redaka dobije otvoreni tekst. Tada za šifrat biramo bilo koji od preostalih 25 redaka. Primalac dešifrira šifrat tako da rotiranjem diskova u jednom retku dobije šifrat i onda među preostalih 25 redaka potraži onaj koji sadrži neki smisleni tekst i taj redak predstavlja otvoreni tekst.

Slika 1.5: Jeffersonov kotač za šifriranje

[2]Slika 1.5 preuzeta s https://www.theatlantic.com/science/archive/2017/03/h3ll0-mr-pr3s1d3nt/521193/

Enigma

Enigma je elektromehanička naprava koju je izumio Artur Scherbius 1918. godine. Njezina masovna upotreba započela je neposredno prije i za vrijeme Drugog svjetskog rata te je razbijanje njezine šifre imalo važnu ulogu za slijed i ishod rata. Sama enigma se sastojala od tipkovnice s 26 tipki poput pisaćeg stroja, zaslona s 26 žaruljica za prikaz šifriranog izlaza, tri mehanička rotora (šifrarnika) i električne prespojene ploče. Radilo se o elektromehaničkoj napravi koja je u standardnoj verziji pružala 150 738 274 937 250 mogućih kombinacija čime je napad ispitivanjem svih mogućih kombinacija bio nemoguć. Problem je bila razmjena ključeva pa bi svaki mjesec operateri enigme dobili novu knjigu s ključevima u kojoj bi se odredilo koji se ključ koristi koji dan. Također, svaki rotor je imao ugraviranu abecedu na vanjskom omotaču te bi operater rotirao rotor tako dugo dok se na vrhu ne bi pojavila slova specificirana u dnevnom ključu. Na slici 1.6[3] prikazana je enigma.

Slika 1.6: Enigma

[3] Slika 1.6 preuzeta s https://www.theatlantic.com/science/archive/2017/03/h3ll0-mr-pr3s1d3nt/521193/

Poglavlje 2

Kriptografija javnog ključa

2.1 Ideja kriptosustava s javnim ključem

Za sigurnost simetričnih kriptosustava nužna je tajnost ključa. Upravo iz toga slijedi i glavni problem takvih sustava - kako sigurno razmijeniti ključ. Pošiljalac i primatelj tajno izabiru ključ K, koji generira funkcije za šifriranje e_K i dešifriranje d_K, a pritom su te funkcije ili iste ili se d_K lako dobije iz e_K. No, pošiljalac i primalac moraju biti u mogućnosti sigurno razmijeniti tajni ključ preko sigurnog komunikacijskog kanala ili se osobno susresti prije samog šifriranja. Sredinom 70-ih godina 20. stoljeća Diffie[1] i Hellman[2] ponudili su jedno moguće rješenje problema razmjene ključeva koje se temeljilo na činjenici da je u nekim grupama potenciranje puno jednostavnije od logaritmiranja. Također, oni se smatraju začetnicima kriptografije javnog ključa. Ideja javnog ključa je konstruiranje kriptosustava kod kojih bi iz poznavanja funkcije za šifriranje e_K u nekom razumnom vremenu bilo praktički nemoguće izračunati funkciju dešifriranja d_K iz čega slijedi da funkcija za šifriranje e_K može biti javna. Dakle, osnovna ideja jest korištenje *jednosmjernih funkcija*. To su funkcije f koje se računaju lako, ali čiji se inverzi f^{-1} računaju teško. Ako se f^{-1} može lako izračunati ako nam je poznati još neki dodatni podatak, onda se f naziva *osobna jednosmjerna funkcija*. Konstrukcija takvih jednosmjernih funkcija temelji se na teškim matematičkim problemima, tj. problemima koje je teško riješiti za neke konkretne ulazne podatke. Primjeri takvih problema su: faktorizacija velikih složenih brojeva, problem diskretnog logaritma (za zadane a, b i p naći x takav da vrijedi $a^x \equiv b \pmod{p}$), eliptički diskretni logaritam.

[1] Whitfield Diffie, rođen 5. lipnja 1944., američki kriptograf. Zajedno s Hellmanom je osvojio najprestižniju nagradu u području računalnih znanosti - Turingovu nagradu za 2015. godinu.

[2] Martin Edward Hellman, rođen 2. listopada 1945., američki kriptograf. Primljen je u Nacionalnu kuću slavnih izumitelja 2011. godine.

Definicija 2.1.1. ***Kriptosustav s javnim ključem*** *sastoji se od dviju familija* $\{e_K\}$ *i* $\{d_K\}$ *funkcija za šifriranje i dešifriranje sa svojstvima:*
1. za svaki K je d_K *inverz od* e_K*;*
2. za svaki K je e_K *javan, ali je* d_K *poznat samo osobi K;*
3. za svaki K je e_K *osobna jednosmjerna funkcija.*

U definiciji 2.1.1 K prolazi skupom svih mogućih korisnika, e_K se naziva *javnim ključem*, a d_K *tajnim* ili *osobnim ključem.*

Ako pošiljalac A želi poslati poruku x primaocu B, onda B prvo pošalje A svoj javni ključ e_B, a potom A šifrira svoju poruku pomoću e_B te šalje primaocu šifrat $y = e_B(x)$. Preostaje da B dešifrira šifrat koristeći tajni ključ d_B čime dolazi do x, tj.

$$d_B(y) = d_B(e_B(x)) = x.$$

Kada bi se radilo o grupi korisnika koja bi željela komunicirati na ovakav način, onda svi korisnici stave svoje javne ključeve u neku javnu, svima dostupnu datoteku te onda B ne mora slati svoj javni ključ osobi A, već A jednostavno pročita e_B iz datoteke. Shematski prikaz kriptografije javnog ključa nalazi se na slici 2.1.

Slika 2.1: Shematski prikaz kriptografije javnog ključa

2.2 RSA

RSA kriptosustav je najpoznatiji kriptosustav s javnim ključem. Izumili su ga 1977. godine Ronald **R**ivest[3], Adi **S**hamir[4] i Len **A**dleman[5] po kojima je dobio i naziv. Sigurnost mu se temelji na teškoći faktorizacije velikih prirodnih brojeva koja se koristi u dobivanju dodatnog podatka, a u šifriranju i dešifriranju se koristi modularno potenciranje. Odnosno, on se temelji na pretpostavci da nije teško pomnožiti dva velika prosta broja, ali da je jako teško rastaviti veliki složeni broj na njegove proste faktore. Slijedi definicija RSA kriptosustava.

Definicija 2.2.1. ***RSA kriptosustav.*** *Neka je $n = pq$, pri čemu su p i q prosti brojevi. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, te*

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

Za $K \in \mathcal{K}$ definiramo

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

Vrijednosti n i e su javne, a vrijednosti p, q i d su tajne.

U definiciji 2.2.1 (n, e) predstavlja javni ključ koji treba znati svatko tko vam šalje poruku, a (p, q, d) tajni (osobni) ključ koji trebate znati samo vi. Osim toga, u definiciji 2.2.1 se pojavljuje i Eulerova funkcija. To je funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ pri čemu se s $\varphi(n)$ označava broj prirodnih brojeva u nizu $1, 2, \ldots, n$ koji su relativno prosti s n. U našem slučaju, uz činjenicu da su p i q prosti brojevi te da je $n = pq$, vrijedi:

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

Poruka razbijena na blokove koji odgovaraju brojevima manjim od n se šifrira kao

$$e_K(x) = x^e \mod n,$$

a dobiveni šifrat se dešifrira kao

$$d_K(y) = y^d \mod n.$$

[3]Ronald Linn Rivest, rođen 6. svibnja 1947. godine, američki kriptograf i profesor na sveučilištu MIT u Sjedinjenim Američkim Državama. Stekao je prvostupničku diplomu iz matematike na sveučilištu Yale.

[4]Adi Shamir, rođen 6. srpnja 1952., izraelski kriptograf i računalni znanstvenik. Dobio je 2017. godine Japansku nagradu u području elektronike, informacija i komunikacija za njegov doprinos informacijskoj sigurnosti kroz pionirsko istraživanje kriptografije.

[5]Leonard Max Adleman, rođen 31. prosinca 1945., američki kriptograf i teoretski računalni znanstveni. Zajedno s Rivestom i Shamirom osvaja 2002. godine Turingovu nagradu za doprinos kriptografiji.

Funkcija šifriranja e_K je „jednosmjerna funkcija", tj. uz poznavanje samo javnog ključa (n, e) iz $e_K = x^e \mod n$ ne možemo naći tajni ključ d, odnosno inverznu funkciju $d_K(y) = y^d \mod n$. Kako bismo to mogli odrediti potreban nam je dodatan podatak, tj. faktorizacija od n. Onaj koji zna ili može otkriti faktorizaciju od javno poznatog broja $n = pq$, tj. faktore p i q može izračunati $\varphi(n) = (p-1)(q-1)$ i saznati tajni eksponent d rješavajući pomoću proširenog Euklidovog algoritma linearnu kongruenciju

$$de \equiv 1 \pmod{\varphi(n)}.$$

Odabir parametara u RSA kriptosustavu

1. Tajno se odaberu dva velika prosta broja p i q slične veličine s preko 150 znamenaka i tako da q ima nekoliko znamenaka više od p. Odabir se provodi tako da prvo generiramo slučajan prirodan broj m s traženim brojem znamenaka pomoću nekog generatora slučajnih brojeva, a onda tražimo prvi prosti broj veći ili jednak m korištenjem nekog testa za testiranje prostosti.

2. Izračuna se $n = pq$ i $\varphi(n) = (p-1)(q-1) = n + 1 - p - q$.

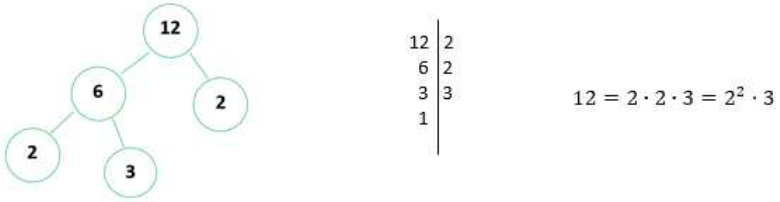
3. Slučajno se odabire broj e tako da vrijedi $e < \varphi(n)$ i $\text{nzd}(\varphi(n), e) = 1$, pri čemu je nzd oznaka za najvećeg zajedničkog djelitelja.

4. Pomoću proširenog Euklidovog algoritma se tajno izračuna d tako da je $de \equiv 1 \pmod{\varphi(n)}$.

5. Postavljanje ključa za šifriranje (n, e) u javni direktorij.

U prvom koraku možemo očekivati da ćemo morati testirati približno $\ln m$ brojeva dok ne nađemo prvi prosti broj zbog teorema o distribuciji prostih brojeva. Također, treba paziti da $n = pq$ bude otporan na metode faktorizacije koje su vrlo efikasne za brojeve specijalnog oblika. Dakle, kada se kaže da sigurnost RSA kriptosustava počiva na teškoći faktorizacije velikog prirodnog broja n treba voditi računa da postoje veliki prirodni brojevi koje možemo vrlo lako faktorizirati. Primjerice, mogli smo uzeti veliki broj $n = 10^{300}$, ali on se može lako faktorizirati kao $10^{300} = 2^{300} \cdot 5^{300}$ te je zato potrebno pažljivo odabrati dva prosta broja p i q tako da se n, koji je njihov produkt, teško faktorizira. Također, n se može puno lakše faktorizirati ako su p i q jako blizu jedan drugoga ili ako $p-1$ i $q-1$ imaju samo male proste faktore. No, tu se javlja pitanje kako tajno naći veliki prosti broj jer se može činiti da će to biti gotovo podjednako teško kao i faktoriziranje velikog prirodnog broja slične veličine. Stoga je važna činjenica iz teorije brojeva da se testiranje prostosti velikih brojeva može provesti puno efikasniji od poznatog školskog načina (dijeleći redom s 2,3,...), a da za faktorizaciju nemamo algoritam koji bi bio puno brži od školskog (pomoću

grananja, pomoću crte) koji je prikazan na slici 2.2. Istaknimo samo da najveći broj za koji je dokazano da je prost ima 22 338 618 znamenaka, a najveći broj n za koji je javno objavljena uspješna faktorizacija i koji zadovoljava sve savjete za izbor modula u RSA kriptosustavu ima 232 decimalne znamenke.



Slika 2.2: Prikaz rastavljanja broja 12 na proste faktore

U trećem koraku uvjet $\text{nzd}(\varphi(n), e) = 1$ znači da biramo broj e koji je relativno prost s brojem $(p-1)(q-1)$. Također, primijetimo da je e uvijek neparan jer je $p-1$ paran. Najčešće se broj e bira slučajnim odabirom, a onda se provjerava zadovoljava li on zadani uvjet. Iako se broj e može odabrati slučajno, ima ga smisla odabrati da bude što manji kako bi modularno potenciranje, tj. šifriranje $x^e \mod n$ bilo što brže. Kako veličina broja e i broj jedinica u binarnom zapisu od e utječu na broj operacija u šifriranju, izbor vrlo malog eksponenta e može predstavljati opasnost za sigurnost.

U četvrtom koraku se pomoću proširenog Euklidovog algoritma, odnosno rješavajući kongruenciju $de \equiv 1 \pmod{\varphi(n)}$ računa broj d. Uz uvjet $\text{nzd}(\varphi(n), e) = \text{nzd}((p-1)(q-1), e) = 1$, slijedi da takav d postoji i da je on jedistven u skupu $\{1, ..., (p-1)(q-1)-1\}$.

Što se tiče napada na RSA kriptosustav, jedan od klasičnih je traženje faktorizacije broja n. Ako napadač uspješno faktorizira n, onda on može pronaći $\varphi(n)$ i d. Također, ako napadač otkrije tajni eksponent d, onda treba promijeniti n, a ne samo eksponent e. Napomenimo i da svi do sada poznati napadi na RSA samo ukazuju na što treba paziti i što treba izbjegavati kod izbora parametara i korištenja RSA kriptosustava pa se pravilno korišten RSA kriptosustav može smatrati sigurnim.

Prije primjera, pokazat ćemo da vrijedi $(x^e)^d \equiv x \pmod{n}$.

Teorem 2.2.2. *Neka je (n, e) javni RSA ključ, a (p, q, d) pripadni tajni RSA ključ. Tada je*

$$(x^e)^d \equiv x \pmod{n}$$

za svaki broj x takav da je $0 \leq x < n$.

Dokaz.
S obzirom da vrijedi $ed \equiv 1 \mod (p-1)(q-1)$, slijedi da postoji prirodan broj l tako da je

$$ed = 1 + l(p-1)(q-1).$$

Tada je

$$(x^e)^d = x^{ed} = x^{1+l(p-1)(q-1)} = x(x^{(p-1)(q-1)})^l.$$

Odakle slijedi

$$(x^e)^d = x(x^{p-1})^{(q-1)l} \equiv x \pmod{p}.$$

Ako p ne dijeli x, onda iz Malog Fermatovog teorema slijedi tvrdnja. Pri čemu Mali Fermatov teorem govori da ako p ne dijeli a, onda je $a^{p-1} \equiv 1 \pmod{p}$, tj. da za svaki cijeli broj a vrijedi $a^p \equiv a \pmod{p}$, pri čemu je p prost broj.

U suprotnom, ako p dijeli x, onda je tvrdnja trivijalna jer su obje strane kongruencije jednake 0 mod p, tj.

$$(x^e)^d = x(x^{p-1})^{(q-1)l} \equiv 0 \equiv x \pmod{p}.$$

Analogno, vrijedi

$$(x^e)^d \equiv x \pmod{q}.$$

Kako su p i q različiti prosti brojevi, dobivamo

$$(x^e)^d \equiv x \pmod{n}.$$

Tvrdnja slijedi iz činjenice $0 \leq x < n$.

□

Dakle, ako je šifrat y dobiven koristeći formulu $y = e_K(x) = x^e \pmod{n}$, onda iz teorema 2.2.2 slijedi da se otvoreni tekst x može rekonstruirati koristeći

$$x = d_K(y) = y^d \mod n.$$

Iz toga slijedi da je RSA sustav stvarno kriptosustav jer za svaku funkciju šifriranja postoji funkcija dešifriranja.

Šifriranje i dešifriranje u RSA kriptosustavu na primjeru

Primjer 2.2.3. *Marica i Ivica žele komunicirati koristeći RSA kriptosustav. Ivica se odluči uzeti parametre $p = 3$ i $q = 17$. Prikažimo kako se određuju n, e i d.*

Nakon što je Ivica odabrao p i q računa

$$n = pq = 51,$$

$$\varphi(n) = (p-1)(q-1) = 32.$$

Zatim odabere $e = 5$ te provjerava je li e relativno prost s $\varphi(n)$.
Potom pomoću proširenog Euklidovog algoritma računa d takav da vrijedi

$$de \equiv 1 \pmod{\varphi(n)}$$

i dobiva

$$32 = 5 \cdot 6 + 2$$

$$5 = 2 \cdot 2 + 1,$$

tj. dobiva

$$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (32 - 5 \cdot 6) = 5 \cdot (1 + 2 \cdot 6) - 2 \cdot 32 = 5 \cdot 13 - 2 \cdot 32$$

iz čega slijedi da je $d = 13$.
Vrijednosti p, q, d zadržava za sebe, a n i e upisuje u javni direktorij ili šalje Marici. Odnosno, javni ključ je

$$(n, e) = (51, 5),$$

dok je tajni ključ

$$(p, q, d) = (3, 17, 13).$$

Primjer 2.2.4. *Ivica šalje Marici poruku FIZIKA. Marica je odabrala parametre $p = 5$ i $q = 43$.*

Nakon što je Marica odabrala parametre p i q računa

$$n = pq = 215,$$

$$\varphi(n) = (p-1)(q-1) = 168.$$

Zatim odabere $e = 11$ te provjerava je li e relativno prost s $\varphi(n)$.
Potom pomoću Euklidovog algoritma rješava linearnu diofantsku jednadžbu

$$de - t\varphi(n) = 1,$$

tj.

$$11x - 168y = 1$$

i dobiva $(x, y) = (168z + 107, 11z + 7), z \in \mathbb{Z}$ iz čega slijedi $d = 107$.
Vrijednosti p, q, d zadržava za sebe, a n i e upisuje u javni direktorij ili šalje Ivici.
Odnosno, javni ključ je

$$(n, e) = (215, 11),$$

dok je tajni ključ

$$(p, q, d) = (5, 43, 107).$$

Prvo ćemo riješiti primjer koristeći numerički ekvivalent iz $\mathbb{Z}_{26}$ karakterističan za klasičnu kriptografiju. Dakle, koristeći englesku abecedu i uzimajući da je $A = 01, B = 02, \ldots, Y = 25, Z = 26$, a razmak 0, numerički ekvivalent poruke FIZIKA koju Ivica želi poslati je

$$x = 060926091101.$$

Kako je $x > n, x$ razbija u dvoznamenkaste blokove, počevši s lijeve strane. Kada bi zadnjem bloku nedostajalo znamenki, on bi se nadopunio praznim mjestom kojem je pridružena vrijednost 0.
Sada je

$$x = (x_1, x_2, x_3, x_4, x_5, x_6) = (06, 09, 26, 09, 11, 01).$$

Poznavajući javne $n = 215$ i $e = 11$ i koristeći $y = e_K(x) \equiv x^e \pmod{n}$, Ivica računa:

$$y_1 = 6^{11} \mod 215 = 36 \mod 215,$$

$$y_2 = 9^{11} \mod 215 = 169 \mod 215,$$

$$y_3 = 26^{11} \mod 215 = 191 \mod 215,$$

$$y_4 = 9^{11} \mod 215 = 169 \mod 215,$$

$$y_5 = 11^{11} \mod 215 = 21 \mod 215,$$

$$y_6 = 1^{11} \mod 215 = 1 \mod 215.$$

Dobiveni šifrat je

$$y = (y_1, y_2, y_3, y_4, y_5, y_6) = (036, 169, 191, 169, 021, 001) = 036169191169021001.$$

Marica prima poruku $y = 036169191169021001$ koju joj je Ivica poslao. Ona, znajući da je $d = 107$, može dešifrirati poruku koju je primila koristeći $d_K(y) \equiv y^d \pmod{n}$ i dijeleći y na blokove:

$$x_1 = 36^{107} \mod 215 = 6 \mod 215,$$

$$x_2 = 169^{107} \mod 215 = 9 \mod 215,$$

$$x_3 = 191^{107} \mod 215 = 26 \mod 215,$$

$$x_4 = 169^{107} \mod 215 = 9 \mod 215,$$
$$x_5 = 21^{107} \mod 215 = 11 \mod 215,$$
$$x_6 = 1^{107} \mod 215 = 1 \mod 215$$

te pretvarajući numerički ekvivalent poruke natrag u poruku dolazi do orginalne poruke FIZIKA.

No, umjesto numeričkog ekvivalenta iz $\mathbb{Z}_{26}$ u praksi se zapravo koriste ASCII kodovi koji niz znakova pretvaraju u bitove.

Decimal	Hexadecimal	Binary	Octal	Char	Decimal	Hexadecimal	Binary	Octal	Char	Decimal	Hexadecimal	Binary	Octal	Char
0	0	0	0	[NULL]	48	30	110000	60	0	96	60	1100000	140	`
1	1	1	1	[START OF HEADING]	49	31	110001	61	1	97	61	1100001	141	a
2	2	10	2	[START OF TEXT]	50	32	110010	62	2	98	62	1100010	142	b
3	3	11	3	[END OF TEXT]	51	33	110011	63	3	99	63	1100011	143	c
4	4	100	4	[END OF TRANSMISSION]	52	34	110100	64	4	100	64	1100100	144	d
5	5	101	5	[ENQUIRY]	53	35	110101	65	5	101	65	1100101	145	e
6	6	110	6	[ACKNOWLEDGE]	54	36	110110	66	6	102	66	1100110	146	f
7	7	111	7	[BELL]	55	37	110111	67	7	103	67	1100111	147	g
8	8	1000	10	[BACKSPACE]	56	38	111000	70	8	104	68	1101000	150	h
9	9	1001	11	[HORIZONTAL TAB]	57	39	111001	71	9	105	69	1101001	151	i
10	A	1010	12	[LINE FEED]	58	3A	111010	72	:	106	6A	1101010	152	j
11	B	1011	13	[VERTICAL TAB]	59	3B	111011	73	;	107	6B	1101011	153	k
12	C	1100	14	[FORM FEED]	60	3C	111100	74	<	108	6C	1101100	154	l
13	D	1101	15	[CARRIAGE RETURN]	61	3D	111101	75	=	109	6D	1101101	155	m
14	E	1110	16	[SHIFT OUT]	62	3E	111110	76	>	110	6E	1101110	156	n
15	F	1111	17	[SHIFT IN]	63	3F	111111	77	?	111	6F	1101111	157	o
16	10	10000	20	[DATA LINK ESCAPE]	64	40	1000000	100	@	112	70	1110000	160	p
17	11	10001	21	[DEVICE CONTROL 1]	65	41	1000001	101	A	113	71	1110001	161	q
18	12	10010	22	[DEVICE CONTROL 2]	66	42	1000010	102	B	114	72	1110010	162	r
19	13	10011	23	[DEVICE CONTROL 3]	67	43	1000011	103	C	115	73	1110011	163	s
20	14	10100	24	[DEVICE CONTROL 4]	68	44	1000100	104	D	116	74	1110100	164	t
21	15	10101	25	[NEGATIVE ACKNOWLEDGE]	69	45	1000101	105	E	117	75	1110101	165	u
22	16	10110	26	[SYNCHRONOUS IDLE]	70	46	1000110	106	F	118	76	1110110	166	v
23	17	10111	27	[ENG OF TRANS. BLOCK]	71	47	1000111	107	G	119	77	1110111	167	w
24	18	11000	30	[CANCEL]	72	48	1001000	110	H	120	78	1111000	170	x
25	19	11001	31	[END OF MEDIUM]	73	49	1001001	111	I	121	79	1111001	171	y
26	1A	11010	32	[SUBSTITUTE]	74	4A	1001010	112	J	122	7A	1111010	172	z
27	1B	11011	33	[ESCAPE]	75	4B	1001011	113	K	123	7B	1111011	173	{
28	1C	11100	34	[FILE SEPARATOR]	76	4C	1001100	114	L	124	7C	1111100	174	|
29	1D	11101	35	[GROUP SEPARATOR]	77	4D	1001101	115	M	125	7D	1111101	175	}
30	1E	11110	36	[RECORD SEPARATOR]	78	4E	1001110	116	N	126	7E	1111110	176	~
31	1F	11111	37	[UNIT SEPARATOR]	79	4F	1001111	117	O	127	7F	1111111	177	[DEL]
32	20	100000	40	[SPACE]	80	50	1010000	120	P					
33	21	100001	41	!	81	51	1010001	121	Q					
34	22	100010	42	"	82	52	1010010	122	R					
35	23	100011	43	#	83	53	1010011	123	S					
36	24	100100	44	$	84	54	1010100	124	T					
37	25	100101	45	%	85	55	1010101	125	U					
38	26	100110	46	&	86	56	1010110	126	V					
39	27	100111	47	'	87	57	1010111	127	W					
40	28	101000	50	(	88	58	1011000	130	X					
41	29	101001	51	)	89	59	1011001	131	Y					
42	2A	101010	52	*	90	5A	1011010	132	Z					
43	2B	101011	53	+	91	5B	1011011	133	[					
44	2C	101100	54	,	92	5C	1011100	134	\					
45	2D	101101	55	-	93	5D	1011101	135	]					
46	2E	101110	56	.	94	5E	1011110	136	^					
47	2F	101111	57	/	95	5F	1011111	137	_					

Slika 2.3: ASCII tablica znakova

Koristeći tablicu prikazanu na slici 2.3[6], za svaki znak iz riječi FIZIKA Ivica uzima njegovu binarnu vrijednost i dobiva odgovarajući ekvivalent poruke u binarnom zapisu

$$x = 100011010010011011010100100110010111000001$$

jer $F \to 1000110$, $I \to 1001001$, $Z \to 1011010$, $K \to 1001011$, $A \to 1000001$.

[6]Slika 2.3 preuzeta sa stranice https://en.m.wikipedia.org/wiki/File:ASCII-Table.svg

Pretvarajući taj binarni zapis u decimalni broj dobiva $x = (1\cdot 2^{41}) + (0\cdot 2^{40}) + (0\cdot 2^{39}) + (0\cdot 2^{38}) + (1\cdot 2^{37}) + (1\cdot 2^{36}) + (0\cdot 2^{35}) + (1\cdot 2^{34}) + (0\cdot 2^{33}) + (0\cdot 2^{32}) + (1\cdot 2^{31}) + (0\cdot 2^{30}) + (0\cdot 2^{29}) + (1\cdot 2^{28}) + (1\cdot 2^{27}) + (0\cdot 2^{26}) + (1\cdot 2^{25}) + (1\cdot 2^{24}) + (0\cdot 2^{23}) + (1\cdot 2^{22}) + (0\cdot 2^{21}) + (1\cdot 2^{20}) + (0\cdot 2^{19}) + (0\cdot 2^{18}) + (1\cdot 2^{17}) + (0\cdot 2^{16}) + (0\cdot 2^{15}) + (1\cdot 2^{14}) + (1\cdot 2^{13}) + (0\cdot 2^{12}) + (0\cdot 2^{11}) + (1\cdot 2^{10}) + (0\cdot 2^{9}) + (1\cdot 2^{8}) + (1\cdot 2^{7}) + (1\cdot 2^{6}) + (0\cdot 2^{5}) + (0\cdot 2^{4}) + (0\cdot 2^{3}) + (0\cdot 2^{2}) + (0\cdot 2^{1}) + (1\cdot 2^{0}) = 2424967423425$. Ponovno razbija dobiveni x u dvoznamenkaste blokove, počevši s lijeve strane. Sada je

$$x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7) = (24, 24, 96, 74, 23, 42, 05).$$

Poznajući javne $n = 215$ i $e = 11$ i koristeći $y = e_K(x) \equiv x^e \pmod{n}$, Ivica računa:

$$y_1 = 24^{11} \mod 215 = 14 \mod 215,$$

$$y_2 = 24^{11} \mod 215 = 14 \mod 215,$$
$$y_3 = 96^{11} \mod 215 = 101 \mod 215,$$
$$y_4 = 74^{11} \mod 215 = 189 \mod 215,$$
$$y_5 = 23^{11} \mod 215 = 197 \mod 215,$$
$$y_6 = 42^{11} \mod 215 = 128 \mod 215,$$
$$y_7 = 5^{11} \mod 215 = 120 \mod 215.$$

Dobiveni šifrat je

$$y = (y_1, y_2, y_3, y_4, y_5, y_6, y_7) = (014, 014, 101, 189, 197, 128, 120) = 014014101189197128120.$$

Marica prima poruku $y = 014014101189197128120$ koju joj je Ivica poslao. Ona, znajući da je $d = 107$, može dešifrirati poruku koju je primila koristeći $d_K(y) \equiv y^d \pmod{n}$ i dijeleći y na blokove:

$$x_1 = 14^{107} \mod 215 = 24 \mod 215,$$

$$x_2 = 14^{107} \mod 215 = 24 \mod 215,$$
$$x_3 = 101^{107} \mod 215 = 96 \mod 215,$$
$$x_4 = 189^{107} \mod 215 = 74 \mod 215,$$
$$x_5 = 197^{107} \mod 215 = 23 \mod 215,$$
$$x_6 = 128^{107} \mod 215 = 42 \mod 215,$$
$$x_7 = 120^{107} \mod 215 = 5 \mod 215$$

te pretvarajući numerički ekvivalent poruke u decimalnom zapisu natrag u poruku u binarnom zapisu i onda koristeći ASCII tablicu dolazi do orginalne poruke FIZIKA.

2.3 ElGamalov kriptosustav

ElGamalov kriptosustav nastao je 1985. godine, a predložio ga je Taher ElGamal[7]. On se temelji na teškom računanju diskretnog logaritma u grupi $(\mathbb{Z}_p^*, \cdot_p)$ gdje je p prosti broj i $\mathbb{Z}_p^* = \{1, 2, \ldots, p\}$, tj. $\mathbb{Z}_p$ bez neutralnog elementa zbrajanja (– nule).

Za neprazan skup G s binarnom operacijom *: G × G → G kažemo da je *grupa* ako vrijede sljedeća svojstva:

1. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, ∀ x, y, z ∈ G (asocijativnost)
2. (∃ e ∈ G): e $\cdot x = x \cdot e = x$, $\forall x \in G$ (neutralni element)
3. $(\forall x \in G)(\exists! x^{-1} \in G) : x \cdot x^{-1} = x^{-1} \cdot x = e$ (inverzni element).

Ako još vrijedi i svojstvo

$$x \cdot y = y \cdot x, \ \forall x, y \in G \ (\textit{komutativnost}),$$

onda kažemo da je G *Abelova* ili *komutativna grupa*.

Skup $\mathbb{Z}_p^*$ je zaista komutativna grupa s obzirom na operaciju množenja modulo p (pri čemu je p prosti broj). Vrijede asocijativnost (– koju nije sasvim lako za pokazati) i komutativnost množenja modulo p, 1 je očito neutralni element množenja, a svaki element a iz $\mathbb{Z}_p^*$ ima (multiplikativni) inverz jer kongruencija $ax \equiv 1 \pmod{p}$ ima jedinstveno rješenje u $\mathbb{Z}_p^*$. Nadalje, $\mathbb{Z}_p^*$ je tzv. konačna grupa (jer je broj elemenata grupe, tj. takozvani red grupe konačan, $|\mathbb{Z}_p^*| = p - 1$).

Kako bi grupa G bila prikladna za upotrebu u kriptografiji javnog ključa, ona bi trebala imati svojstvo da je logaritmiranje u njoj vrlo teško, ali da su operacije množenja i potenciranja u njoj jednostavne.

Problem diskretnog logaritma
Neka je $(G, *)$ konačna Abelova grupa te $g \in G$. Tada je skup $H = \{g^i : i \geq 0\}$ podgrupa od G generirana s g, tj. podskup od G koji je i sam grupa s obzirom na operaciju $*$. Za $h \in H$ najmanji nenegativni cijeli broj x takav da je

$$h = g^x = \underbrace{g * \cdots * g}_{x \ puta},$$

naziva se *diskretni logaritam* i označava se s $\log_g h$.

[7]Taher ElGamal, rođen 18. kolovoza 1955., egipatski kriptograf i poduzetnik. Izabran je u Nacionalnu inžinjersku akademiju (NAE) 2022. godine za doprinos kriptografiji, e-trgovini i protokolima za sigurne internetske transakcije.

Sam problem računanja diskretnog logaritma u grupi $(\mathbb{Z}_p^*, \cdot_p)$ pokazao se kao problem približno iste težine kao i problem faktorizacije složenog broja n uz zahtjev da su p i n istog reda veličine.

Diffie i Hellman su pri rješavanju problema razmjene ključeva također koristili činjenicu da postoje grupe u kojima je problem diskretnog logaritma težak. Njihov protokol za razmjenu ključeva „dešava se" u spomenutoj multiplikativnoj grupi $(\mathbb{Z}_p^*, \cdot_p)$, pri čemu je p dovoljno velik prosti broj. Napominjemo da je $\mathbb{Z}_p^*$ *ciklička* grupa, a njezin generator je *primitivni korijen* modulo p. Za broj $g \in \{1, 2, \ldots, p-1\}$ kažemo da je primitivni korijen modulo p ako je g^{p-1} najmanja potencija broja g koja daje ostatak 1 pri djeljenju s p, tj. $g^{p-1} \equiv 1 \pmod{p}$. Nadalje, tada je

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

Definicija 2.3.1. ***ElGamalov kriptosustav.*** *Neka je p prost broj i $\alpha \in \mathbb{Z}_p^*$ primitivni korijen modulo p. Neka je $\mathcal{P} = \mathbb{Z}_p^*$, $\mathcal{C} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ i $\mathcal{K} = \{(p, \alpha, a, \beta) : \beta = \alpha^a \mod p\}$.*
Vrijednosti p, α, β su javne, a vrijednost a je tajna.
Za $K \in \mathcal{K}$ i tajni slučajni broj $k \in \{0, 1, \ldots, p-1\}$ definiramo funkciju šifriranja

$$e_K(x, k) = (\alpha^k \mod p, x\beta^k \mod p).$$

Za $y_1, y_2 \in \mathbb{Z}_p^*$ definiramo funkciju dešifriranja

$$d_K(y_1, y_2) = y_2(y_1^a)^{-1} \mod p.$$

Provjerimo da je $d_K(y_1, y_2) = x$:

$$y_2(y_1^a)^{-1} \equiv x\beta^k \left((\alpha^k)^a\right)^{-1} \equiv x(\alpha^a)^k \left((\alpha^k)^a\right)^{-1} = x\alpha^{ak}(\alpha^{ak})^{-1} \equiv x \pmod{p}.$$

Uočimo da za dešifriranje možemo računati multiplikativni inverz od y_1^a rješavanjem kongruencije $y_1^a z \equiv 1 \pmod{p}$ (korištenjem proširenog Euklidovog algoritma) ili računanjem potencije

$$(y_1^a)^{-1} \equiv y_1^{p-1-a} \pmod{p}.$$

Zaista, prema Malom Fermatovom teoremu je

$$(y_1^a)^{-1} y_1^{p-1-a} \equiv y_1^{p-1} \equiv 1 \pmod{p}.$$

Šifriranje i dešifriranje u ElGamalovom kriptosustavu

Pretpostavimo da osoba B želi poslati osobi A poruku x koristeći se ElGamalovim kriptosustavom.

1. Osoba A bira prost broj p i $\alpha \in \mathbb{Z}_p^*$ primitivni korijen modulo p.

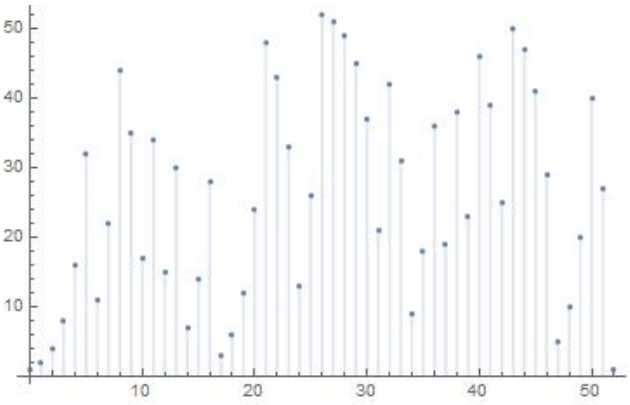
2. Potom osoba A nasumično odabire broj $a \in \{0, \ldots, p-2\}$ i računa $\beta = \alpha^a \mod p$.

3. Javni ključ osobe A je (p, α, β), dok je njen tajni ključ a.

4. Osoba B odabire neki slučajni tajni cijeli broj $k \in \{0, 1, \ldots, p-1\}$ (takozvani jednokratni ključ) i računa
$$y_1 \equiv \alpha^k \pmod{p}$$
i
$$y_2 \equiv x\beta^k \pmod{p}.$$
Tada osoba B šalje osobi A uređeni par (y_1, y_2).

5. Osoba A prima poruku (y_1, y_2) i računa
$$x \equiv y_1^{p-1-a} y_2 \pmod{p}.$$

Sigurnost ElGamalovog kriptosustava leži u teškoći određivanja tajnog eksponenta a, odnosno u rješavanju problema diskretnog logaritma
$$\alpha^a \equiv \beta \pmod{p}.$$



Slika 2.4: Vrijednosti $2^n \mod 53$ za $n \in \{0, 1, \cdots, 52\}$

Do danas nije poznat neki efikasni algoritam za računanje diskretnog logaritma. Naime, diskretni logaritam se, za razliku od klasičnog logaritma realnog broja, ponaša vrlo nepravilno i nalikuje generatoru slučajnih brojeva (slika 2.4[8]). Stoga da bi primjerice pronašli eksponent a za koji je

$$2^a \equiv 22 \pmod{53},$$

potrebno je redom računati potencije broja 2 modulo 53:

$$2^0 = 1, 2^1 = 1, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 32,$$

$$2^6 = 64 \equiv 11 \pmod{53}, 2^7 \equiv 11 \cdot 2 = 22 \pmod{53}.$$

Dakle, diskretni logaritam od 22 modulo 53 je broj 7. U ovom primjeru, diskretni logaritam se brzo pronašao, no općenito ova procedura ispitivanja redom sigurno nije efikasna posebice u slučaju velikog prostog broja p. Drugi pristup bio bi da uzimamo nasumične vrijednosti a, računamo α^a te provjeravamo vrijedi li $\alpha^a = \beta$.

Za sada ne postoji efikasan algoritam za rješavanje diskretnog logaritma, ali postoje neki algoritmi koji su efikasni u slučaju nekih posebnih oblika broja p. Spomenimo Pohlig–Hellmanov algoritam koji može vrlo uspješno riješiti problem diskretnog logaritma ako je $p - 1$ produkt malih prostih brojeva. Smatra se da je p siguran ako je oblika $2q + 1$, pri čemu je q veliki prosti broj jer se na taj način garantira da $p - 1 = 2q$ ima veliki prost broj kao faktor pa Pohlig-Hellmanov algoritam ne može lako riješiti problem diskretnog logaritma.

Ako bi napadač znao izračunati diskretni logaritam modulo p, onda bi on mogao odrediti tajni ključ a kao diskretni logaritam od β po bazi α. Napadač bi onda došao do otvorenog teksta koristeći formulu $x \equiv y_1^{p-1-a} y_2 \pmod{p}$, pri čemu su y_1 i y_2 kao ranije opisani. Za dovoljno velik prosti broj p ovaj problem je nerješiv, odnosno nije rješiv u *realnom* vremenu. Kako bi se očuvala sigurnost ElGamalovog kriptosustava, preporuča se korištenje prostih brojeva p od oko 1024 bita. Također, treba izbjegavati proste brojeve specijalnih oblika kako bi se spriječila upotreba nekih algoritama diskretnog logaritma koji su za njih donekle efikasni.

Nadalje, množenje otvorenog teksta x s β^k predstavlja vrstu kamuflaže koju može maknuti samo onaj koji posjeduje tajni eksponent a.

Sama operacija potenciranja modulo p može se efikasno provesti upotrebom metode takozvanog uzastopnog kvadriranja u kojoj se eksponent prikaže u bazi 2. Ilustrirajmo na primjeru metodu uzastopnog kvadriranja poznatu i kao metodu *kvadriraj i množi* ili *binarne ljestve*.

Primjer 2.3.2. *Izračunajmo* $7^{23} \mod 52$ *koristeći metodu kvadriraj i množi.*

[8] Slika nacrtana u online kalkulatoru od WolframAlphe, https://www.wolframalpha.com/input/?i=calculator, `DiscretePlot[Mod[`2^n`, 53], {`$n, 0, 52$`}]`

Rješenje. Prvo je potrebno odrediti binarni zapis broja 23:

$$23 = 10111_2.$$

Kako je

$$23 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4,$$

imamo

$$\begin{aligned} 7^{23} &= 7^{2^0} \cdot 7^{2^1} \cdot 7^{2^2} \cdot 7^{2^4} \\ &= 7 \cdot \left(7 \cdot 7^{2^1} \cdot 7^{2^3}\right)^2 \\ &= 7 \cdot \left(7 \cdot \left(7 \cdot 7^{2^2}\right)^2\right)^2 \\ &= 7 \cdot \left(7 \cdot \left(7 \cdot \left(7^2\right)^2\right)^2\right)^2 . \end{aligned}$$

Prema tome, računamo redom:

1. $7^2 \mod 52 = 49$
2. $49^2 \mod 52 = 9$
3. $(7 \cdot 9)^2 \mod 52 = 17$
4. $(7 \cdot 17)^2 \mod 52 = 17$
5. $7 \cdot 17 \mod 52 = 15.$

Općenito, broj koraka u algoritmu odgovara duljini binarnog zapisa. U svakom koraku (osim zadnjeg) izvršava se množenje s bazom i kvadriranje, ako je znamenka u binarnom zapisu jednaka 1, odnosno samo kvadriranje ako je znamenka jednaka 0. U zadnjem se koraku samo množi s bazom, ako je znamenka jednaka 1.

□

Primjer 2.3.3. *Ivica želi poslati Marici poruku $x = 5$. Marica je odabrala parametre $p = 53, \alpha = 2, a = 6$.*

Rješenje. Nakon što je Marica odabrala parametre p, α, a, mora odrediti parametar β:

$$\beta \equiv \alpha^a \pmod{p} = 2^6 \equiv 11 \pmod{53}.$$

Tada je njezin javni ključ $(p, \alpha, \beta) = (53, 2, 11)$, a tajni ključ je $a = 6$. Javni ključ šalje direktno Ivici ili ga postavlja u javni direktorij.

Ivica mora šifrirati poruku $x = 5$. Prvo odabire slučajni tajni broj (jednokratni ključ) $k = 3$ i računa

$$y_1 \equiv \alpha^k \pmod{p} = 2^3 \equiv 8 \pmod{53}$$

i

$$y_2 \equiv x\beta^k \pmod{p} = 5 \cdot 11^3 \equiv 30 \pmod{53}.$$

Dobiveni šifrat je $(y_1, y_2) = (8, 30)$.
Marica prima šifrat $(y_1, y_2) = (8, 30)$ koji joj je Ivica poslao. Ona ga može dešifrirati računajući

$$x = y_1^{p-1-a} y_2 \pmod{p} = 8^{53-1-6} \cdot 30 \equiv 5 \pmod{53}$$

i dolazi do orginalne poruke $x = 5$. □

2.4 Problem ruksaka

Kriptosustav koji se temelji na *problemu ruksaka* je **Merkle[9]-Hellmanov** kriptosustav iz 1978. godine. Problem ruksaka zasniva se na pretpostavci da imamo n predmeta s volumenima $v_1, v_2, \ldots, v_n$ i da njima želimo napuniti ruksak volumena V. Odnosno, potrebno je naći podskup, ako takav postoji, $J \subseteq \{1, 2, \ldots, n\}$ tako da vrijedi

$$\sum_{j \in J} v_j = V.$$

Problem ruksaka možemo opisati na još jedan način. Za dani skup $\{v_1, v_2, \ldots, v_n\}$ od n prirodnih brojeva i prirodan broj V, treba naći niz $m = (\epsilon_1, \epsilon_2, \ldots, \epsilon_n)$ od n binarnih znamenki tako da vrijedi

$$\epsilon_1 v_1 + \epsilon_2 v_2 + \cdots + \epsilon_n v_n = V,$$

ako takav m postoji.

Kako je potrebno pronaći niz od n binarnih znamenki, to znači da su $\epsilon_i \in \{0, 1\}, \forall i \in \{1, \ldots, n\}$. Ovako opisan opći problem ruksaka je vrlo težak, ali postoji poseban slučaj, tzv. *superrastući problem ruksaka*, koji je puno lakši. U tom slučaju je niz $v_1, v_2, \ldots, v_n$ rastući i vrijedi

$$v_j > v_1 + v_2 + \cdots + v_{j-1} \text{ za } j = 2, 3, \ldots, n,$$

a ruksak „punimo" na način da u njega pokušavamo staviti predmet najvećeg volumena i zatim redom predmete manjeg volumena. Primjer jednog takvog superrastućeg niza je niz $v_i = 2^{i-1}$, $i \geq 1$ u kojem su ϵ_i-ovi binarne znamenke broja V. Zaista,

$$v_1 + v_2 + \cdots + v_{i-1} = 1 + 2 + \cdots + 2^{i-2} = \frac{2^{i-1} - 1}{2 - 1} = 2^{i-1} - 1 < v_i, \ i \geq 2.$$

[9]Ralph Merkle, rođen 2. veljače 1952. godine, američki informatičar. Primljen je u Nacionalnu kuću slavnih izumitelja 2011. godine.

Ideja Merkle-Hellmanovog kriptosustava je zapravo zakamuflirati superrastući niz tako da izgleda kao potpuno slučajan niz. Takvo kamufliranje se provodi modularnim množenjem. Primatelj poruke može pročitati poruku rješavajući superrastući problem ruksaka jer zna kako ukloniti kamuflažu, ali svi drugi moraju rješavati opći problem ruksaka, koji je puno teži, pa ne mogu pročitati poruku. Slijedi definicija Merkle-Hellmanovog kriptosustava u terminima definicije 1.2.1.

Definicija 2.4.1. ***Merkle-Hellmanov kriptosustav.*** *Neka je* $v = (v_1, v_2, \ldots, v_n)$ *superrastući niz prirodnih brojeva,* $p > v_1 + v_2 + \cdots + v_n$ *prost broj i* $1 \leq a \leq p-1$. *Za* $i = 1, 2, \ldots, n$ *definiramo*

$$t_i = av_i \mod p$$

i označimo $t = (t_1, t_2, \ldots, t_n)$. *Neka je* $\mathcal{P} = \{0,1\}^n$, $\mathcal{C} = \{0, 1, \ldots, n(p-1)\}$ *i* $\mathcal{K} = \{(v, p, a, t)\}$, *gdje su* v, p, a *i* t *konstruirani na opisan način.*
Za $K \in \mathcal{K}$ *definiramo*

$$e_K(x_1, x_2, \ldots, x_n) = x_1t_1 + x_2t_2 + \cdots + x_nt_n.$$

Za $0 \leq y \leq n(p-1)$ *definiramo* $z = a^{-1}y \mod p$, *riješimo superrastući problem ruksaka za skup* $\{v_1, v_2, \ldots, v_n, z\}$ *i dobivamo*

$$d_K(y) = (x_1, x_2, \ldots, x_n).$$

Vrijednost t *je javna, a vrijednosti* p, a *i* v *su tajne.*

Istaknimo da je ideja Merkle-Hellmanovog kriptosustava korištenje jednostavnog specijalnog slučaja nekog teškog problema tako da se taj specijalni slučaj prekrije da izgleda kao opći. U odnosu na druge kriptosustave s javnim ključem, prednost Merkle-Hellmanovog kriptosustava jest brzina šifriranja. On je po brzini usporediv s najboljim simetričnim kriptosustavima. No, problem je što se ne može smatrati sigurnim kriptosustavom jer ispada da se ovako jednostavnim kamufliranjem vrlo specifičnog niza ne dobiva potpuno slučajan niz. Adi Shamir je 1982. godine pronašao polinomijalni algoritam za razbijanje Merkle-Hellmanovog kriptosustava.

Primjer 2.4.2. *Neka je* $v = (2, 7, 10, 21, 53, 97)$ *superrastući niz te neka je* $p = 193$ *i* $a = 121$. *Želimo poslati poruku* $x = 110101_2$.

Rješenje. Prvo iz broja elemenata superrastućeg niza, određujemo da je $n = 6$. Potom određujemo niz $t = (t_1, t_2, \ldots, t_6)$ koristeći $t_i = av_i \mod p$:

$$t_1 = 121 \cdot 2 \mod 193 = 49,$$

$$t_2 = 121 \cdot 7 \mod 193 = 75,$$

$$t_3 = 121 \cdot 10 \mod 193 = 52,$$
$$t_4 = 121 \cdot 21 \mod 193 = 32,$$
$$t_5 = 121 \cdot 53 \mod 193 = 44,$$
$$t_6 = 121 \cdot 97 \mod 193 = 157.$$

Odakle slijedi $t = (49, 75, 52, 32, 44, 157)$, a javni ključ K je

$$K = (v, p, a, t) = ((2, 7, 10, 21, 53, 97), 193, 121, (49, 75, 52, 32, 44, 157)).$$

Poruku $x = 110101_2 = (1, 1, 0, 1, 0, 1)$ šifriramo kao

$$e_K(x) = \sum_{i=1}^{6} x_i t_i = 1 \cdot 49 + 1 \cdot 75 + 0 \cdot 52 + 1 \cdot 32 + 0 \cdot 44 + 1 \cdot 157 = 313.$$

Da bismo dešifrirali šifrat $y = 313$ treba riješiti problem ruksaka za superrastući niz $(2, 7, 10, 21, 53, 97)$ i volumen

$$z = a^{-1}y \mod p = 121^{-1} \cdot 313 \mod 193 = 67 \cdot 313 \mod 193 = 127.$$

Kako bismo odredili x, zapisujemo z kao sumu elemenata iz v:

$$z = 127 = 2 + 7 + 21 + 97.$$

Do poruke x dolazimo tako da na i-to mjesto poruke stavimo znamenku 0 ako broj v_i nije pribrojnik sume z, a ako on je jedan od pribrojnika sume z, onda stavimo znamenku 1. Pribrojnici koji u sumi daju $z = 127$ su $2, 7, 21, 97$, a oni se nalaze na prvom, drugom, četvrtom i šestom mjestu u skupu v pa na prvo, drugo, četvrto i šesto mjesto traženog šesteroznamenkastog broja stavljamo znamenku 1, a na ostala znamenku 0. Dobivamo poruku

$$x = d_K(y) = 110101.$$

□

Poglavlje 3

Digitalni potpis

Digitalni ili *elektronički potpis* je u biti ekvivalent vlastoručnog potpisa koji se povezuje sa sadržajem dokumenta ili skupom podataka (npr. ugovori, bankovne transakcije) na koji se potpis odnosi. Stoga digitalni potpis mora zadovoljiti četiri temeljna zahtjeva:

1. **Povjerljivost:** poruku koju osoba *A* šalje osobi *B* ne može pročitati nitko drugi.
2. **Vjerodostojnost:** osoba *B* zna da je samo osoba *A* mogla poslati poruku koju je ona upravo primila.
3. **Netaknutost:** osoba *B* zna da poruka koju je poslala osoba *A* nije promijenjena prilikom slanja.
4. **Nepobitnost:** osoba *A* ne može kasnije zanijekati da je poslala poruku.

Navedene zahtjeve moguće je zadovoljiti pomoću matematičkih shema, odnosno kriptografskih protokola koji uključuju kriptosustave javnog ključa.

3.1 Zakonska regulativa

Standardizacija digitalnog potpisa počinje sredinom 1990-ih godina u Sjedinjenim Američkim Državama, a u Europi proces standardizacije počinje nekoliko godina kasnije. Danas u zemljama članicama Europske Unije digitalni potpis ima isti status kao i vlastoručni potpis što znači da sve što je digitalno potpisano zakonski obvezuje potpisanog na sve uvjete u njemu. Zakon o elektroničkom potpisu u Republici Hrvatskoj izglasan je 2002. godine, a dopunjen je 2008. godine.

Ovim je Zakonom[1], prema članku 1., uređeno pravo fizičkih i pravnih osoba na uporabu elektroničkog potpisa upravnim, sudskim i drugim postupcima, poslovnim i drugim radnjama te prava, obveze i odgovornosti fizičkih i pravnih osoba u svezi s davanjem usluga certificiranja elektroničkog potpisa.

Prema članku 2. i 3. elektronički potpis je skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju potpisnika i vjerodostojnosti potpisanoga elektroničkog dokumenta.

Prema članku 2. i 4. napredan elektronički potpis je onaj koji je povezan isključivo s potpisnikom, koji nedvojbeno identificira potpisnika, koji nastaje korištenjem sredstava kojima potpisnik može samostalno upravljati i koja su pod nadzorom potpisnika te koji sadržava izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka.

Napredan elektronički potpis prema članku 5. ima istu pravnu snagu i zamjenjuje vlastoručni potpis.

Napredni elektronički potpis izrađuje se sredstvima za izradu naprednog elektroničkog potpisa, a ona moraju osigurati da se podaci za izradu mogu pojaviti samo jednom te da je ostvarena njihova sigurnost, da se podaci za izradu naprednog elektroničkog potpisa ne mogu ponoviti te da je potpis zaštićen od krivotvorenja, da podatke potpisnik može pouzdano zaštiti protiv korištenja od strane drugih. Također, sredstva za izradu ne smiju prilikom izrade naprednog elektroničkog potpisa promijeniti podatke koji se potpisuju ili onemogućiti potpisniku uvid u te podatke prije procesa izrade potpisa. Ovo slijedi iz članaka 8. i 9. Zakona o elektroničkom potpisu.

Prema članku 26. potpisnik je dužan pažljivo koristiti i čuvati sredstva i podatke za izradu elektroničkog potpisa, zaštiti i čuvati sredstva i podatke za izradu elektroničkog potpisa od neovlaštenog pristupa i uporabe.

Prema članku 39. novčanom kaznom od 2.000,00 do 10.000,00 kuna kaznit će se za prekršaj fizička osoba koja neovlašteno pristupi i uporabi podatke i sredstva za izradu elektroničkog potpisa i naprednog elektroničkog potpisa.

Stupanjem na snagu Zakona[2] o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o električkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ prestaje važiti Zakon o elektroničkom potpisu. Taj zakon je na snazi od 2017. godine, a njime se utvrđuju tijela za inspekcijski nadzor nad provedbom Uredbe, određuje se tijelo nadležno za akreditaciju tijela za ocjenu sukladnosti te se utvrđuju prava, obveze i odgovornosti potpisnika i pružatelja usluga te se određuju prekršajne odredbe za postupanje protivno Uredbi. Uredbom se nastojalo povećati povjerenje u elektroničke transakcije.

[1]Izvor: https://narodne-novine.nn.hr/clanci/sluzbeni/$2002_0 1_1 0_2 42$.*html*

[2]Izvor: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32014R0910

Prema članku 8. ove Uredbe svaki potpisnik je dužan poduzeti sve potrebne mjere zaštite od gubitaka i šteta koje može uzrokovati drugim potpisnicima, pružateljima usluga povjerenja ili trećim osobama.

Prema članku 9. potpisnik je dužan pažnjom dobrog domaćina koristiti i čuvati sredstva i podatke za izradu elektroničkog potpisa, koristiti sredstva i podatke za izradu elektroničkog potpisa u skladu s odredbama ovoga Zakona, zaštititi i čuvati sredstva i podatke za izradu elektroničkog potpisa od neovlaštenog pristupa i uporabe.

Prema članku 11. imatelj sredstva elektroničke identifikacije dužan je poduzeti sve potrebne mjere kako bi sredstva za elektroničku identifikaciju bila pod njegovim nadzorom te kako bi spriječio krađu, gubitak ili neovlašteno ustupanje svojih sredstava elektroničke identifikacije. Dužan je odmah kod izdavatelja sredstva elektroničke identifikacije opozvati svoju elektroničku identifikaciju ako utvrdi da je ona izgubljena, ukradena ili neovlašteno ustupljena drugima.

Prema članku 18. novčanom kaznom od 2.000,00 do 10.000,00 kuna kaznit će se za prekršaj fizička osoba koja neovlašteno pristupi i uporabi podatke i sredstva za izradu elektroničkog potpisa, naprednog elektroničkog potpisa, kvalificiranoga potpisa, elektroničkog pečata, naprednog elektroničkog pečata, kvalificiranog elektroničkog pečata.

3.2 Matematički koncept digitalnog potpisa

Ideju digitalnog potpisa opisali su 1976. godine Diffie i Hellman, začetnici ideje kriptosustava s javnim ključem kojeg smo opisali u prethodnom poglavlju. Naime, svaki kriptosustav s javnim ključem može poslužiti kao jednostavan model digitalnog potpisa. Dakle, ako osoba A šalje osobi B poruku x ona će ju šifrirati s javnim ključem osobe B i javnim kanalom poslati šifrat $e_B(x) = y$, a osoba B će poruku y dešifrirati pomoću svog tajnog ključa d_B i dobiti $d_B(e_B(x)) = x$. Na ovaj način omogućen je zahtjev *povjerljivosti* poruke jer samo osoba B posjeduje svoj tajni ključ d_B. No, može nastati problem *vjerodostojnosti* ili autentičnosti poruke jer osoba B ne može biti sigurna da je poruku poslala upravo osoba A. Budući da svatko ima pristup funkciji za šifriranje e_B postoji mogućnost da se netko lažno predstavlja kao osoba A. Taj problem može se ukloniti korištenjem javnog i tajnog ključa osobe A, odnosno funkcija e_A i d_A.

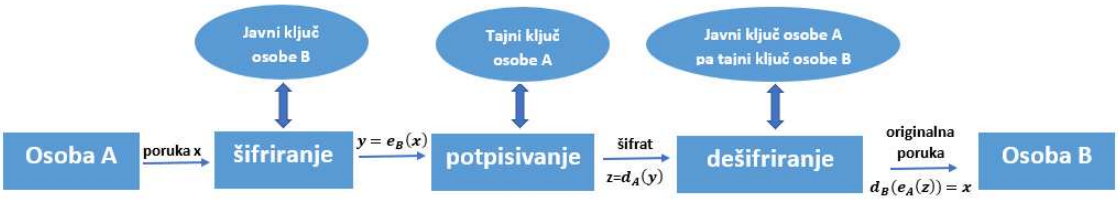
Pretpostavimo da raspolažemo kriptosustavom s javnim ključem čiji je prostor otvorenog teksta jednak prostoru šifrata, tj. $\mathcal{P} = C$. Nadalje, neka su e_A i d_A javni i tajni ključ osobe A, a e_B i d_B javni i tajni ključ osobe B. Tada osoba A može osobi B poslati potpisanu poruku x na način da ju najprije šifrira s javnim ključem osobe B, a zatim dodatno „potpiše" svojim tajnim ključem, odnosno konkretno da pošalje šifrat

$$z = d_A(y) = d_A(e_B(x)).$$

Kada osoba B primi poruku za koju smatra da ju je poslala osoba A, najprije primijeni javni ključ e_A, a potom svoj tajni ključ d_B čime dolazi do x, tj.

$$d_B(e_A(z)) = d_B(e_A(d_A(e_B(x)))) = x.$$

Tada osoba B zna da je poruku sigurno poslala osoba A, a s druge strane osoba A ne može zanijekati slanje poruke jer samo ona posjeduje svoj tajni ključ d_A čime je ovom shemom omogućen i zahtjev *nepobitnosti*.



Slika 3.1: Shematski prikaz upotrebe kriptografije javnog ključa za potpisivanje poruke

3.3 Shema digitalnog potpisa

Svaka shema digitalnog potpisa sastoji se od tri dijela:

1. Algoritam za generiranje tajnog i javnog ključa za potpisivanje
2. Algoritam za generiranje digitalnih potpisa
3. Algoritam za verificiranje digitalnog potpisa.

Algoritam za generiranje digitalnog potpisa podrazumijeva potpisivanje poruke, tj. generiranje poruke koju nazivamo potpis. Taj algoritam koristi tajni ključ za potpisivanje. Algoritam za verificiranje, tj. provjeru digitalnog potpisa koristi javni ključ za verifikaciju.

Osoba A može potpisati poruku m tako da uz m priloži šifrat šifriran njezinim tajnim ključem $d_A(m)$. Osoba B prima poruku $(d_A(m), m)$ i može pomoću javnog ključa e_A provjeriti je li uistinu osoba A potpisala poruku m, tj. vrijedi li

$$e_A(d_A(m)) = m.$$

Na upravo opisani način kriptosustavi s javnim ključem omogućuju digitalno potpisivanje uz napomenu da se poruka m nikad ne šalje javnim kanalom, već se prethodno i ona šifrira

(može i nekom simetričnom šifrom). Stoga ova shema predstavlja *školski* model digitalnog potpisa.

3.4 RSA potpis

Pretpostavimo da osoba A osobi B želi poslati potpisani dokument m.

1. **Generiranje tajnog i javnog ključa** osobe A sastoji se od odabira:
   - dva velika prosta broja p i q te računanja $n = pq$;
   - *tajnog* eksponenta e za kojeg vrijedi
   $$1 < e < \varphi(n) = (p-1)(q-1),\ \text{nzd}(e, \varphi(n)) = 1;$$
   - *javnog* eksponenta d za kojeg vrijedi
   $$1 < d < (p-1)(q-1),\ de \equiv 1 \pmod{(p-1)(q-1)}.$$

   Javni ključ osobe A: (n, e); *tajni ključ* osobe A: d.

2. **Generiranje digitalnog potpisa** osobe A:
   $$s = m^d \mod n.$$
   Osoba A šalje osobi B poruku (s, m).

3. **Verifikacija digitalnog potpisa** osobe A:
   Osoba B računa
   $$m' = s^e \mod n.$$
   Ako je $m = m'$, potpis je *valjan*, a u suprotnom, tj. ako je $m \neq m'$, potpis je *falsifikat* ili *krivotvorina*.

Napadi

Na ovako opisani RSA digitalni potpis postoji više različitih mogućih napada.

Jedan od mogućih napada koristi činjenicu da je osobi B za verifikaciju potpisa osobe A potreban njezin javni ključ. Ako napadač zamijeni javni ključ osobe A sa svojim javnim ključem bez da osoba B to primijeti, onda se napadač može potpisati u ime osobe A. Iz tog

razloga je važno da osoba B zna da ima autentičan javni ključ osobe A. Jedno od mogućih rješenja protiv takvog napada je takozvana *infrastruktura javnog ključa* koja omogućava sigurnosne standarde i tehnike prijenosa podataka putem interneta. To je sustav protokola u kojem treća strana od povjerenja jamči za identitete osoba, tj. njihovih ključeva. Dakle, kako bi se izbjegli ovakvi napadi važno je uključiti davatelja usluga certificiranja ili ovjeritelja javnog ključa. Autoritet koji jamči za identitete osoba naziva se središnji autoritet, kraće CA (engl. Certifying Authoritity). CA izdaje certifikate, tj. digitalno potpisane poruke u kojima se nalaze osobni podaci nositelja javnog ključa i javni ključ te ih potpisuje svojim ključem. Dakle, jedini javni ključ u koji treba imati povjerenja je javni ključ od CA, a u identitete ostalih ključeva možemo imati povjerenje samo ako za njih postoje certifikati. Ovlašteni izdavatelj certifikata za izradu elektroničkog potpisa u Hrvatskoj je Fina. Spomenimo i moguće alternativno rješenje – *mreža povjerenja*. Iz naziva možemo naslutiti na čemu se temelji ovo rješenje, a riječ je o tome da korisnici jamče jedni za druge u mreži povjerenja. Recimo da osoba A i osoba B imaju zajedničkog prijatelja, osobu C, koja je potpisala ključ osobe B. Tada osoba A može vjerovati osobi B.

Drugi mogući napad bio bi da napadač odabere $s \in \{0, \ldots, n-1\}$ i da tvrdi da je s RSA potpis osobe A. Kada osoba B želi provjeriti potpis, ona računa $m = s^e \mod n$ i vjeruje da je osoba A potpisala m. Kažemo da je napadač uspio falsificirati ili krivotvoriti potpis osobe A ako je m neki smisleni tekst. To se naziva *egzistencijalni falsifikat*.

Treća opasnost slijedi iz činjenice da je šifriranje u RSA kriptosustavu multiplikativna operacija, tj. iz dva valjana RSA digitalna potpisa, treći se može odrediti. Napadač tada može koristiti multiplikativnost RSA potpisa da krivotvori valjani potpis za bilo koji dokument. Neka su $m_1, m_2 \in \{0, \ldots, n-1\}$ te $s_1 = m_1^d \mod n$ i $s_2 = m_2^d \mod n$ redom potpisi od m_1 i m_2 tada je

$$s = s_1 s_2 \mod n = (m_1 m_2)^d \mod n$$

potpis od $m = m_1 m_2$. Dakle, napadač želi krivotvoriti potpis za neki dokument $m \in \{0, \ldots, n-1\}$. On posjeduje potpisanu poruku $m_1 \in \{0, \ldots, n-1\}$ različitu od m, ali tako da vrijedi $\text{nzd}(m_1, n) = 1$. Potom računa $m_2 = m m_1^{-1} \mod n$, pri čemu je m_1^{-1} multiplikativni inverz od $m_1 \mod n$. Napadač računa valjane RSA potpise s_1 i s_2 za m_1 i m_2 te računa potpis $s = s_1 s_2 \mod m$ od m.

Konačno, jedan od napada može biti i tzv. *algoritamske* naravi koji se odnosi na razbijanje RSA-kriptosustava. Napomenimo i da ako napadač može faktorizirati n, tada on može odrediti i tajni ključ d osobe A te može potpisivati dokumente u njeno ime. Stoga, jednako kao i u RSA kriptosustavu, p i q moraju biti odabrani tako da faktorizacija od n nije moguća ili barem da nije moguća u neko razumno vrijeme.

Demonstrirajmo upotrebu RSA digitalnog potpisa i jedan mogući napad (egzistencijalni falsifikat) na primjeru.

Primjer 3.4.1. *Marica je odabrala* $p = 11$, $q = 17$ *i* $e = 7$ *te želi obaviti bankovnu transakciju u visini od* 110 kn.

Marica računa

$$n = pq = 11 \cdot 17 = 187$$

i

$$\varphi(n) = (p-1)(q-1) = 10 \cdot 16 = 160.$$

Provjerava uvjet $\text{nzd}(e, \varphi(n)) = 1$ *te računa d tako da vrijedi* $de \equiv 1 \pmod{\varphi(n)}$. *Koristeći prošireni Euklidov algoritam računa*

$$160 = 7 \cdot 22 + 6$$

$$7 = 6 \cdot 1 + 1,$$

tj.

$$1 = 7 - 6 \cdot 1 = 7 - (160 - 7 \cdot 22) = 7 \cdot 23 - 160$$

iz čega slijedi da je $d = 23$. *Tada je Maričin javni ključ*

$$(n, e) = (187, 7),$$

a tajni ključ je

$$(p, q, d) = (11, 17, 23).$$

Marica želi obaviti bankovnu transakciju u visini od 110 kn *te potpisuje* $m = 110$ *tako da računa*

$$s = m^d \mod n = 110^{23} \mod 187 = 66.$$

Kada zaprimi njezinu poruku, aplikacija računa

$$m = s^e \mod n = 66^7 \mod 187 = 110$$

i tada zna da Marica želi obaviti bankovnu transakciju u visni od 110 kn (što može i dokazati) te ju provodi.

Pretpostavimo da napadač želi podići novac s Maričinog računa. On nasumično bira potpis, na primjer $s = 111$ *i računa* $s^e \mod n = 111^7 \mod 187 = 155$. *Banci šalje „potpisanu" poruku* $(s, m) = (111, 155)$ *što aplikacija prihvaća jer je* $m = s^e \mod n$, *no to nije istina jer Marica nikad nije potpisala* 155 kn.

Promotrimo kako možemo spriječiti neke od napada na RSA potpis.

Potpis s redudancijom

Jedan od načina spriječavanja napada koji se oslanja na multiplikativnosti RSA potpisa i napada „egzistencijalni falsifikat" je korištenje takozvanog *potpisa s redudancijom*. On funkcionira tako što se prilikom potpisivanja poruci dodaje nešto suvišno, a zatim ju se potpisuje. Nakon dešifriranja poruke u algoritmu verifikacije provjerava se ima li dobivena poruka ispravnu redundanciju. Dobar primjer redundantne funkcije je konkatenacija sa samim sobom, tj. funkcija koja originalnu poruku spoji s tom istom porukom. Na primjer ako je m poruka u binarnom obliku, tj. $m \in \{0,1\}^n$, $m \in \{0,1,\ldots,n-1\}$, onda se potpisuje poruka koja ima dvije identične polovice $m \,\|\, m \in \{0,1\}^{2n}$ (gdje smo s $\|$ označili konkatenaciju). Dobiveni potpis naziva se *potpis sa zalihom* ili *potpis s redudancijom*.

Kada bi se potpisivali samo dokumenti oblika $m \,\|\, m$, napad „egzistencijalni falsifikat" bi puno teže funkcionirao jer bi napadač morao osmisliti lažni potpis $s \in \{0,1,\ldots,n-1\}$ tako da binarni zapis od $m = s^e \mod n$ bude oblika $m \,\|\, m$ što je gotovo nemoguće.

Također, ni multiplikativnost RSA se više ne može iskoristiti jer je malo vjerojatno da je $m = m_1 m_2 \mod n$ oblika $m \,\|\, m$ ako su m_1 i m_2 toga oblika.

Potpis s hash funkcijom

Osim na opisan način, za generiranje RSA digitalnog potpisa mogu se koristiti i kriptografske *hash funkcije*. Funkcije koje za ulazni podatak, datoteku ili poruku, proizvoljne veličine računaju vrijednost unaprijed određene veličine, obično izražene u bitovima (npr. 128 bitova), nazivaju se hash funkcije. Za hash funkcije koristimo oznaku h. Za ulazni podatak x, vrijednost $h(x)$ nazivamo *hash* od x ili *sažetak* od x. Hash funkcije imaju veliku primjenu pa se tako koriste za brzo pretraživanje, uspoređivanje, identifikaciju i sl. Za primjenu u kriptografiji postoje određeni zahtjevi koje *hash* funkcije moraju zadovoljiti.

1. Funkcija h radi s blokovima proizvoljne veličine (tj. kao ulazne vrijednosti su poruke proizvoljne duljine).
2. Izlazne vrijednosti funkcije h su fiksne duljine (u bitovima).
3. Za svaku ulaznu vrijednost x lako je izračunati $h(x)$.
4. Za zadani y efektivno je nemoguće naći x takav da je $h(x) = y$.
5. Za zadani x_1 efektivno je nemoguće naći x_2 takav da je $h(x_1) = h(x_2)$.

6. Efektivno je nemoguće naći par (x_1, x_2) takav da je $h(x_1) = h(x_2)$.

Hash funkcije koje zadovoljavaju svojstva (1)-(6) nazivaju se *kriptografskim hash funkcijama.* Često se hash funkcije uspoređuju s otiscima prstiju te se kaže da hash funkcije služe za dobivanje *digitalnog otiska.*

Najjednostavnije metode za generiranje hash vrijednost su *metoda dijeljenja* i *metoda srednjih znamenki kvadrata*. U metodi dijeljenja računa se ostatak pri dijeljnju s M gdje je M tzv. veličina hash tablice,

$$h(x) = x \mod M.$$

Metoda srednjih znamenki kvadrata kao hash vrijednost uzima središnjih r znamenki vrijednosti kvadrata ulaznog parametra. Na primjer, hash vrijednost od $x = 66$ za $r = 2$ je $h(x) = 35$ jer je $x^2 = 4356$.

Dobar primjer jednostavne hash funkcije je i

$$h(x) = x^2 \mod M.$$

Ako osoba A želi potpisati proizvoljno dugačak dokument m, onda ona koristi javno poznatu hash funkciju koja iz niza bitova proizvoljne veličine računa vrijednost unaprijed zadane veličine

$$h : \{0,1\}^* \to \{0, \ldots, n-1\}.$$

Tada je potpis dokumenta m:

$$s = h(m)^d \mod n$$

i osoba B prima poruku (s, m). Za verifikaciju potpisa osoba B računa

$$y = s^e \mod n,$$

zatim računa hash vrijednost od $m - h(m)$, te provjerava je li $y = h(m)$. Napominjemo da osoba B ne može rekonstruirati čitav dokument m, već samo njegovu hash vrijednost.

Upotreba hash funkcija u generiranju digitalnog potpisa onemogućuje napade koje smo ranije naveli. Napad koji se temelji na multiplikativnosti RSA više se ne može primijeniti jer je gotovo nemoguće naći takav m da vrijedi $h(m) = h(m_1)h(m_2) \mod n$.

Jednako tako napadač ne može zamijeniti dokument m koji je potpisala osoba A s nekim drugim dokumentom m' jer iz svojstva kriptografskih hash funkcija slijedi $h(m) \neq h(m')$.

Također, napad „egzistencijalni falsifikat" nije moguće ostvariti jer je hash funkcija jednosmjerna funkcija. Pretpostavimo da napadač odabere potpis s. Kako on mora zajedno s potpisom poslati i dokument m osobi B, napadač mora naći takav m da vrijedi $h(m) = s^e \mod n$, tj. odrediti prasliku od $s^e \mod n$ (tj. $h^{-1}(s^e \mod n)$) što je efektivno nemoguće.

3.5 ElGamalov potpis

ElGamalov digitalni potpis zasniva se na ElGamalov kriptosustavu čija sigurnost se temelji na teškoći računanja diskretnog logaritma u grupi $(\mathbb{Z}_p^*, \cdot_p)$, pri čemu je p prosti broj.

Pretpostavimo da osoba A osobi B želi poslati potpisani dokument m.

1. **Generiranje tajnog i javnog ključa** osobe A sastoji se od odabira:

   - prostog broja p,
   - $\alpha \in \mathbb{Z}_p^*$ primitivnog korijena modulo p (generatora grupe $\mathbb{Z}_p^*$),
   - slučajnog broja $a \in \{0, \ldots, p-2\}$.

   Osoba A računa $\beta = \alpha^a \mod p$.

   Javni ključ osobe A: (p, α, β), *tajni ključ* osobe A: a.

2. **Generiranje digitalnog potpisa** osobe A:

   Odabire se slučajni jednokratni ključ $k \in \{1, \ldots, p-2\}$ koji je relativno prost s $p-1$, tj. $\text{nzd}(k, p-1) = 1$ i računa digitalni potpis

   $$(r, s) = (\alpha^k \mod p, (m - a \cdot r) \cdot k^{-1} \mod (p-1)), \tag{3.1}$$

   pri čemu je k^{-1} multiplikativni inverz modulo $p-1$.

   Osoba A šalje osobi B poruku $((r, s), m)$.

3. **Verifikacija digitalnog potpisa** osobe A:

   Osoba B računa

   $$t = \beta^r r^s \mod p.$$

   Ako je $t \equiv \alpha^m \pmod p$, potpis je *valjan*, a ako je $t \not\equiv \alpha^m \pmod p$, potpis je *falsifikat*.

Pokažimo da je ovakvo verificiranje valjano. Ako su r i s izračunati pomoću izraza (3.1), onda vrijedi

$$\beta^r r^s = \alpha^{ar} \alpha^{kk^{-1}(m-ar)} \equiv \alpha^{ar+m-ar} \equiv \alpha^m \pmod p.$$

Obrnuto, ako

$$\beta^r r^s \equiv \alpha^m \pmod p$$

vrijedi za par (r, s) i ako je k diskretni logaritam od r po bazi α, onda je

$$\alpha^{ar+ks} \equiv \alpha^m \pmod p.$$

Kako je α primitivni korijen modulo p, slijedi

$$ar + ks \equiv m \pmod{(p-1)}.$$

Ako su k i $p-1$ relativno prosti, onda je

$$s = k^{-1}(m - ar) \pmod{(p-1)}.$$

Kao što smo spomenuli kod RSA potpisa i ovdje se u pravilu koristi hash funkcija. Tada je umjesto (3.1) potpis poruke m dan s

$$(r, s) = (\alpha^k \mod p, (h(m) - a \cdot r) \cdot k^{-1} \mod (p-1))$$

i šalje se $((r, s), h(m))$, gdje je $h(m)$ hash vrijednost poruke m. Za verifikaciju potpisa ispituje se vrijedi li relacija

$$\beta^r r^s \equiv \alpha^{h(m)} \pmod{p}.$$

Sigurnost

Promotrimo kako izbor parametara p i k može utjecati na sigurnost.

Ako napadač može izračunati diskretni logaritam modulo p, onda on može odrediti tajni ključ osobe A i generirati digitalni potpis u njezino ime. Stoga p mora biti odabran tako da računanje diskretnog logaritma modulo p bude nemoguće ili vremenski neisplativo. S obzirom na danas poznate algoritme diskretnog logaritma to znači da bi p morao imati najmanje 200 znamenki. Iako su za proste brojeve određenih oblika neki algoritmi za određivanje diskretnog logaritma djelomično uspješni, najčešće se prosti brojevi biraju nasumično.

Za svaki novi digitalni potpis potrebno je odabrati novi parametar k što se naglašava i u samom algoritmu jer se k naziva *jednokratni* ključ. Pokažimo kako bi se mogao odrediti tajni ključ ako bi se dva potpisa s_1 i s_2 generirala pomoću istog k. Neka su s_1 i s_2 redom potpisi dokumenata x_1 i x_2 generirani s istim k. Tada je i broj $r = \alpha^k \mod p$ jednak za oba potpisa pa vrijedi

$$s_1 - s_2 \equiv k^{-1}(h(x_1) - h(x_2)) \pmod{(p-1)}.$$

Ako je $h(x_1) - h(x_2)$ invertibilan modulo $p-1$, onda se iz gornje kongruencije može odrediti k. Potom se iz $k, s_1, r, h(x_1)$ može odrediti i tajni ključ a osobe A jer je

$$s_1 = k^{-1}(h(x_1) - ar) \pmod{(p-1)},$$

a onda je

$$a = r^{-1}(h(x_1) - ks_1) \pmod{(p-1)}.$$

Napad egzistencijalni falsifikat

Ako se u ElGamalovoj shemi digitalnog potpisa ne koristi hash funkcija, onda je mogući napad egzistencijalni falsifikat. Kongruencija za verifikaciju potpisa je tada jednaka

$$\beta^r r^s \equiv \alpha^x \pmod{p}.$$

Pokažimo kako odabrati r, s, x da se zadovolji navedena kongruencija. Kako bi krivotovorio potpis, napadač bira dva cijela broja u, v tako da je $\text{nzd}(v, p-1) = 1$. Potom računa

$$r = \alpha^u \beta^v \mod p, s = -rv^{-1} \mod (p-1), x = su \mod (p-1).$$

S tako dobivenim vrijednostima r i s, vrijedi kongruencija za verificiranje potpisa

$$\beta^r r^s \equiv \beta^r (\alpha^u \beta^v)^s \equiv \beta^r \alpha^{su} \beta^{sv} \equiv \beta^r \alpha^{su} \beta^{-r} \equiv \beta^{r-r} \alpha^x \equiv \alpha^x \pmod{p}.$$

Ovakav postupak funkcionira i ako se koristi hash funkcija otporna na kolizije. No, napadač ne može pronaći dokument x tako da je generirani potpis upravo potpis od x jer je hash funkcija jednosmjerna funkcija.

Pokažimo kako se novi potpisi mogu generirati iz starih ako se ne zahtjeva uvjet $1 \leq r' \leq p-1$. Neka je (r, s) ElGamalov potpis dokumenta x te neka je x' neki drugi dokument. Kako bi potpisao x' i uz pretpostavku da je $h(x)$ invertibilna modulo $p-1$, napadač računa

$$u = h(x')h(x)^{-1} \mod (p-1)$$

i

$$s' = su \mod (p-1).$$

Koristeći Kineski teorem o ostacima koji govori da ako su m i n relativno prosti prirodni brojevi, onda za svaki par cijelih brojeva a, b postoji jedinstveno modulo mn rješenje sustava kongruencija $x \equiv a \pmod{m}, x \equiv b \pmod{n}$, napadač određuje r' koje je rješenje sustava kongruencija

$$r' \equiv ru \pmod{(p-1)},\ r' \equiv r \pmod{p}.$$

Tada je potpis dokumenta x' par (r', s').

Verifikacija ovako dobivenog potpisa također funkcionira

$$\beta^{r'} (r')^{s'} \equiv \beta^{ru} r^{su} \equiv \alpha^{u(ar+ks)} \equiv \alpha^{h(x')} \pmod{p}.$$

No pokažimo da je tada narušen uvjet $1 \leq r' \leq p-1$ jer je $r' \geq p$. S jedne strane imamo

$$1 \leq r \leq p-1, r \equiv r' \mod p, \tag{3.2}$$

a s druge strane

$$r' \equiv ru \not\equiv r \pmod{(p-1)}. \tag{3.3}$$

To slijedi iz $u \equiv h(x')h(x)^{-1} \not\equiv 1 \pmod{(p-1)}$ i činjenice da je h otporna na kolizije što znači da je za zadani x efektivno nemoguće pronaći y takav da vrijedi $h(x) = h(y)$. Sada iz 3.3 slijedi $r \neq r'$ i iz 3.2 slijedi $r' \geq p$.

Promotrimo ElGamalovu shemu digitalnog potpisa na primjeru.

Primjer 3.5.1. *Marica i Ivica komuniciraju ElGamalovim kriptosustavom s parametrima* $p = 43$ *i* $\alpha = 3$. *Marica želi potpisati dokument x čija je hash vrijednost* $h(x) = 11$.

Marica bira nasumičan eksponent $a = 7$ *i računa*

$$\beta = \alpha^a \mod p = 3^7 \mod 43 = 37.$$

Maričin javni ključ je tada $(p, \alpha, \beta) = (43, 3, 37,)$ *a tajni ključ je* $a = 23$.

Marica želi potpisati dokument x, čija je hash vrijednost $h(x) = 11$. *Ona bira* $k \in \{1, ..., p-2\}$ *prost s* $p - 1 = 42$, $k = 19$ *i dobiva*

$$r = \alpha^k \mod p = 3^{19} \mod 43 = 19.$$

Inverz od k modulo $p - 1 = 42$ *je* $k^{-1} = 31$ *pa slijedi*

$$s = k^{-1} \cdot (h(x) - a \cdot r) \mod (p-1) = 31 \cdot (11 - 7 \cdot 19) \mod 42 = 40.$$

Maričin potpis je par $(r, s) = (19, 40)$.

Ivica želi provjeriti potpis. Prvo provjerava vrijedi li $1 \leq r \leq p - 1$ *što vrijedi jer je* $1 \leq 19 \leq 42$. *Kako je taj uvjet zadovoljen, dalje provjerava vrijedi li kongruencija*

$$\beta^r r^s \equiv \alpha^{h(x)} \mod p,$$

tj. računa

$$\beta^r r^s \mod p = 37^{19} \cdot 19^{40} \mod 43 = 30$$

i

$$\alpha^{h(x)} \mod p = 3^{11} \mod 43 = 30.$$

Ivica zaključuje da je potpis valjan.

Efikasnost ElGamalove sheme digitalnog potpisa

Za generiranje ElGamalovog potpisa potrebna je jedna primjena proširenog Euklidovog algoritma kako bi se izračunao inverz od k modulo $p-1$, tj. k^{-1} i jedno modularno potenciranje modulo p za računanje $r = \alpha^k \mod p$. Ovo su mogući predračuni i oni ne ovise o dokumentima koji će se potpisati. No, rezultati ovih predračuna trebaju biti sigurno spremljeni i čuvani tajnima. Stvarni potpis tada zahtjeva samo dva modularna potenciranja te je vrlo brz.

Sama verifikacija ElGamalovog potpisa zahtjeva tri modularna potenciranja te je dulja od verifikacije RSA potpisa.

Bibliografija

[1] J.A. Buchmann, *Introduction to cryptography*, Springer-Verlag, New York, 2004.

[2] A. Dujella, *Teorija brojeva*, Školska knjiga, 2019.

[3] A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.

[4] Z. Franušić, *O matematici digitalnog potpisa*, MiŠ 115, lipanj 2022., 195-207.

[5] I. Kiš, N. Pavetić, J. Sugnetić, A. Završki, A. Zrinušić, *Linearna kriptoanaliza*, `https://security.foi.hr/wiki/index.php/Linearna_kriptoanaliza.html` (srpanj 2022.)

[6] Hrvatska enciklopedija, mrežno izdanje, *Kriptografija*, `http://www.enciklopedija.hr/Natuknica.aspx?ID=33988` (srpanj 2022.)

Sažetak

Digitalni potpis omogućava potpisivanje elektroničkih dokumenata što je izuzetno važno u današnje vrijeme kada se sve više koristi rad na daljinu, internet kupovina i bankarstvo. To je vrsta kriptografskog protokola koji služi kao elektronička zamjena za vlastoručni potpis, a zasniva se na kriptografiji javnog ključa. U ovom radu uz kratki uvid u kriptografiju, posebice kriptografiju javnog ključa, opisani su matematički modeli nekih digitalnih potpisa.

Summary

The digital signature enables signing of electronic documents, which is extremely important nowadays when remote work, online shopping and banking are increasingly used. It is a type of cryptographic protocol that serves as an electronic substitute for a handwritten signature and it is based on public key cryptography. In this thesis, along with a brief insight into cryptography, especially public key cryptography, mathematical models of some digital signatures are described.

Životopis

Rođena sam u Čakovcu 27.8.1998. godine. Pohađala sam III. osnovnu školu u Čakovcu, a nakon toga upisujem Gimnaziju Josipa Slavenskog Čakovec koju završavam s odličnim uspjehom i 2017. godine upisujem Integrirani preddiplomski i diplomski sveučilišni studij Matematika i fizika, smjer nastavnički na Prirodoslovno matematičkom fakultetu u Zagrebu.