Metode za podjelu tajne

Despotović, Josipa

PRIRODOSLOVNO–MATEMATIČKI FAKULTET
SVEUČILIŠTA U SPLITU

JOSIPA DESPOTOVIĆ

METODE ZA PODJELU TAJNE

DIPLOMSKI RAD

Split, veljača 2021.

PRIRODOSLOVNO–MATEMATIČKI FAKULTET
SVEUČILIŠTA U SPLITU

ODJEL ZA MATEMATIKU

METODE ZA PODJELU TAJNE

DIPLOMSKI RAD

Studentica:
Josipa Despotović

Voditeljica:
prof. dr. sc. Borka Jadrijević

Split, veljača 2021.

ZAHVALA

Na ovom mjestu bih se zahvalila mentorici prof. dr. sc. Borki Jadrijević na ukazanom povjerenju i vodstvu tijekom izrade ovoga rada te korisnim raspravama i savjetima. Posebno hvala i svim ostalim profesorima i djelatnicima Prirodoslovno-matematičkog fakulteta u Splitu te svim kolegama koji su vrijeme studiranja učinili ljepšim. Veliko hvala i svim prijateljima čije ogromne podrške nikad nije nedostajalo. Hvala ti Mateo, što si bio uz mene. I na kraju najveće hvala mojim roditeljima i sestri na neizmjernoj podršci, ljubavi i motivaciji kroz cijelo moje obrazovanje.

Sadržaj

Uvod

Sva računala priključena na internet, od našeg pametnog telefona ili prijenosnog računala do poslužitelja koji poslužuju sadržaje za masovno posjećene internetske stranice za web-prodaju, pronalaze se i komuniciraju pomoću brojeva, tzv. *IP adresa*. Kada otvorimo web preglednik ili šaljemo elektroničku poštu, ne moramo pamtiti i unositi taj dugi broj, umjesto toga dovoljno unijeti ime internetske domene, kao što je na primjer *www.pmfst.hr* i svejedno ćemo doći na pravo mjesto. DNS sustav (eng. *Domain Name System*) je globalno distribuirana usluga koja prevodi čovjeku čitljiva imena poput *www.amazon.com,* u računalu čitljive numeričke IP adrese poput 80.237.232.142, koje računala koriste za međusobno povezivanje. No, ako netko uspije "oponašati" rad DNS-a i "uvjeriti" naše računalo da se primjerice *www.amazon.com* nalazi na nekoj drugoj IP adresi, nije teško zamisliti s kakvim se sve problemima možemo suočiti. Da bi se zaštitili od ovakve vrste napada, uveden je DNSSEC, skup dodataka koji proširuju sigurnost DNS-a. DNSSEC koristi kriptografske algoritme i alate kako bi spriječio mogućnost zlonamjernog povezivanja IP adresa i domenskih imena. Kriptografija koja se koristi za provjeru autentičnosti DNS povezivanja svakako je vrlo zanimljiva, ali je ključno pitanje kome se može povjeriti glavni kriptografski ključ sustava? Neprofitna organizacija ICANN odgovorna za takve situacije je odabrala sljedeći način: glavni ključ je podijeljen na sedam dijelova koji su na pametnim karticama

dani sedmorici različitih ljudi koji se nalaze na geografski različitim mjestima u svijetu i koji svoje kartice čuvaju u sefovima. Najmanje pet članova ove grupe, svaki sa svojim dijelom ključa, bi se moralo naći u centru za podatkovnu sigurnost u Sjedinjenim Američkim Državama da bi restartalo DNSSEC u slučaju da sustav padne (što je vrlo malo vjerojatno).

"*If you round up five of these guys, they can decrypt (the root key) should the West Coast fall in the water and the East Coast get hit by a nuclear bomb.*" Richard Lamb, voditelj DNSSEC programa u ICANN-u

Kako je moguće da bilo kojih 5 od 7 članova ove grupe mogu rekonstruirati glavni ključ, ali primjerice 4 člana od njih 7 to ne mogu? Rješenje leži u kriptografskim alatima koji se nazivaju *metode (sheme) dijeljenja tajne* (eng. *secret-sharing schemes*). Navedeni primjer, na jednostavan način, opisuje koncept *dijeljenja tajne*. U kriptografiji, pod pojmom *shema za dijeljenje* ili *podjelu tajne* podrazumjevamo bilo koju metodu za raspodjelu tajne (tajnog ključa, informacije, podatka,...) među skupinom sudionika, tako da se svakome dodjeljuje dio tajne. Samo kombiniranjem određenog broja dijelova tajne ona može biti otkrivena. Na taj način se zapravo osigurava da niti jedan sudionik podjele, s dijelom tajne koju posjeduje, ne može sam otkriti cijelu tajnu, ali ni bilo kakvu informaciju o toj tajni.

U ovom radu prvo ćemo se upoznati sa svojstvima i važnoću metoda za podjelu tajne, njihovim vrstama i obilježjima te dati primjere njihove primjene u raznim područjima. Zatim ćemo detaljnije opisati osnovne metode za dijeljenje tajne, *Shamirovu* i *Blakleyevu shemu praga* te metode koje koriste *Kineski teorem o ostacima*. Na samom kraju rada obrađena je implementacija modificirane Shamirove sheme podjele tajne u svrhu podjele i rekonstrukcije lozinke, a rad cijele skripte koja provodi implementaciju, opisan je kroz primjer.

Poglavlje 1

Podjela tajne

U mnogom situacijama potrebno je skriti i zaštititi neku važnu informaciju (lozinku, ključ za šifriranje, tajni recept i sl.). Primjerice, podatke štitimo šifriranjem pa je jako važno zaštiti tajni ključ koji se koristi za to šifriranje. Zamislimo da svoje važne datoteke šifriramo tajnim ključem, ali ako se taj ključ izgubi, tada će sve važne datoteke biti nedostupne. Stoga su potrebni sigurni i učinkoviti mehanizmi upravljanja ključevima. Jedan od tih mehanizama su tzv. *metode* ili *sheme za podjelu tajne* koje nam omogućuju da tajnu podijelimo na nekoliko dijelova koje onda distribuiramo odabranim osobama. Tajna se može rekonstruirati kad dio tih osoba na neki način surađuje.

Začetnici ove ideje *podjele tajne* su izraelski kriptograf *Adi Shamir* i američki kriptograf i matematičar *George Blakley.* Oni su 1979. godine, neovisno jedan o drugome, osmislili prvu metodu za podjelu tajne tzv. *shemu praga* kao rješenje problema zaštite i sigurnosti kriptografskih ključeva. Sheme za podjelu tajne su potrebne jer su mnogi kriptosustavi koji koriste jedan glavni ključ ranjivi na različite načine. Na primjer, ako se glavni ključ javnosti otkrije slučajno ili nekim kriptografskim napadom, to će ugroziti cijeli sustav. Također, ako se izgubi glavni ključ, tada svi ostali ključevi koje on

štiti postaju nepristupačni. Isto tako, ako se pokaže da je vlasnik glavnog ključa nelojalan, tada će svi osjetljivi podaci procuriti do protivnika. Uz to, sheme za podjelu tajne su korisne i kada nemamo dovoljno povjerenja u neku osobu koja ima pristup tajnom ključu.

Osim za zaštitu tajnog ključa, sheme za podjelu tajne također se koriste za zaštitu drugih vrsta tajni, poput tajnog recepta za *Coca Colu* ili lozinke za otvaranje trezora banke, za kontrolu pristupa nuklearnom oružju i slično.

Sheme za podjelu tajne su dakle metode koje se koriste za skrivanje nekog podatka, kojeg ćemo nazivati *tajna,* dijeljenjem te tajne na djelove, koje ćemo nazivati *dionicama tajne* i njihovom raspodjelom određenim osobama, koje ćemo nazivati *sudionici podjele tajne.* Tajna se može rekonstruirati iz određenih podskupova dionica. Onoga tko bira tajnu, dijeli tajnu i dionice tajno distribuira sudionicima nazvamo *djelitelj tajne.*
Dakle, bilo koja shema za podjelu tajne sastoji od sljedeća dva dijela:

- *Postupak raspodjele dionica*: Odabrana tajna S se dijeli, ovisno o metodi, na n dionica tajne: $s_1, s_2, ..., s_n$ koje se onda tajno podijele sudionicima.

- *Postupak rekonstrukcije tajne:* Tajna se može rekonstruirati iz odgovarajućeg skupa dionica pomoću određenog algoritma (ovisno o metodi).

U sljedećem poglavlju definirat ćemo preciznije što je to shema praga te ćemo proučiti neke najpoznatije sheme praga. Osim s Shamirovom i Blakleyevom shemom, bavit ćemo se i s dvije sheme praga koje se temelje na Kineskom teoremo o ostatcima. Ali neovisno o kojoj se shemi praga radi, dva temeljna svojstva svake (t, n) - *sheme praga* su:

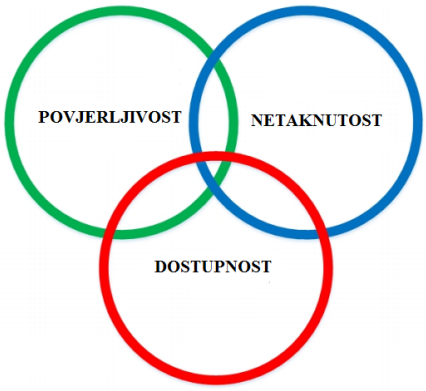
- *oporavljivost* - s bilo kojih t dionica tajne S, od njih ukupno n, možemo rekonstruirati cijelu tajnu S;

- *tajnost* - s manje od t dionica tajne S, tajna se ne može odrediti.

U nastavku ovog poglavlja upoznat ćemo se s osnovnim svojstvima i različitim vrstama metoda za podjelu tajne te ih pokušati klasificirati na temelju njihovih karakteristika. Također, vidjet ćemo gdje se sve danas koriste metode za podjelu tajne.

1.1 Osnovna svojstva metoda za podjelu tajne

Kao što smo već rekli, sheme za podjelu tajne idealne su za pohranu i zaštitu visoko osjetljivih i vrlo važnih informacija, npr. ključeva za šifriranje, kodova za lansiranje projektila, brojeva bankovnih računa, ... Svaka od ovih informacija mora se držati strogo povjerljivo, ali je također jako važno da se ne izgubi. Tradicionalne metode šifriranja nisu prikladne za istodobno postizanje visoke razine povjerljivosti i pouzdanosti. To je zato što prilikom spremanja tajnog ključa treba birati između čuvanja jedne kopije ključa na jednom mjestu radi maksimalne tajnosti i čuvanja više kopija ključa na različitim mjestima radi veće pouzdanosti. Povećavanjem pouzdanosti ključa pohranjivanjem više njegovih kopija očito se smanjuje se njegova povjerljivost jer ima više mogućnosti da kopija ključa padne u pogrešne ruke. Metode za podjelu tajne rješavaju ovaj problem jer omogućuju pro-



Slika 1.1: Svojstva metoda podjele tajne

izvoljno visoku razinu povjerljivosti i pouzdanosti. One su zasnovane na sasvim drugačijoj ideji. Umjesto da se čuva više kopija tajne, tajna se dijeli s više osoba i to na način da svatko dobije jednu dionicu te tajne, ali tako da nitko od sudionika podjele ne može pronaći tajnu koristeći samo svoju dionicu tajne. Ali ako dovoljan broj tih osoba udruži svoje dionice, tajna se može potpuno rekonstruirati. U protivnom, nije moguće pronaći tajnu, odnosno bilo kakvu informaciju o toj tajni. Stoga, metode za podjelu tajne zadovoljavalju tri temeljna kriterija informacijske sigurnosti:

- *Povjerljivost* (eng. *confidentiality*). Kada govorimo o povjerljivosti podataka, govorimo o mjerama za zaštitu podataka od neovlaštenog pristupa i zlouporabe.

- *Netaknutost* (eng. *integrity*). Netaknutost podataka odnosi se na zaštitu podataka od neovlaštenih izmjena. Mjere za zaštitu netaknutosti pružaju sigurnost u točnost i cjelovitost podataka.

- *Dostupnost* (eng. *availability*). Da bi informacijski sustav bio korištan mora biti kontinuirano dostupan ovlaštenim korisnicima. Mjere za zaštitu dostupnosti štite pravodobni i neprekidan pristup sustavu.

Sigurna shema za podjelu tajne je ona shema u kojoj je tajna podijeljena na dionice na način da svatko tko ima manje od t dionica tajne (gdje je t neki unaprijed određen broj) ima jednako informacija o tajni kao i onaj tko ne posjeduje niti jednu dionicu tajne.

Primjer 1.1 *Neka je naša tajna riječ "cryptography". Podijelit ćemo je na četiri dijela na sljedeći način*

$$cry - pto - gra - phy.$$

Osoba koja ne posjeduje niti jednu dionicu naše tajne zna samo da se tajna sastoji od 12 *slova te bi tajnu riječ morala tražiti između* $26^{12} \approx 9,542\,9 \cdot 10^{16}$ *mogućih riječi od* 12 *slova. Osoba koja pojeduje jednu dionicu tajne treba pronaći još* 9 *slova, odnosno treba ispitati* $26^9 \approx 5,429\,5 \cdot 10^{12}$ *mogućih riječi, uz pretpostavku da zna koju dionicu tajne riječi posjeduje. To je i dalje velik broj, ali dosta manji od prethodnog.*

Ovo je primjer podjele tajne kod koje su potrebne sve dionice tajne da bi tajna mogla biti rekonstruirana. Očito, ovo je i primjer *nesigurne* podjele tajne jer osoba koja posjeduje određeni broj dionica tajne ima mogućnost reducirati problem pronalaženja tajne budući da ima više informacija o tajni od onoga tko ne posjeduje niti jednu dionicu tajne.

Primjer 1.2 *Neka je naša tajna S. Pretpostvimo da imamo n sudionika podjele tajne. Svakom sudioniku P_j, $j = 1, ..., n$ dodjeljujemo njegov javni ključ e_j i njemu odgovarajući tajni ključ d_j. Zatim šifriramo tajnu S na sljedeći način*

$$e_1(e_2(...(e_n(S))) = Y \tag{1.1}$$

i sudioniku podjele tajne P_j dodjeljujemo dionicu tajne

$$(Y, e_j, d_j)\,,$$

gdje su Y i e_j javni podatci, a d_j je tajni podatak. Pretpostavimo dodatno da je za svaki $j = 1, ..., n$ dekriptiranje "nemoguće", točnije da je za dani y problem nalaženja x-a takvog da je $e_j(x) = y$ bez poznavanja tajnog ključa d_j, jako težak problem.

Sudionik P_1 ili napadač koji dođe u posjed tajnog ključa d_1 može ukloniti samo prvi (vanjski) sloj šifrirata u (1.1). Sudionici P_1 i P_2 ili svatko tko posjeduje tajne ključeve d_1 i d_2 može ukloniti prvi i drugi sloj šifrata, itd. Iz

ovoga vidimo da svatko tko ima manje od n ključeva ne može otkriti tajnu bez da prethodno dektiptira potrebne slojeve bez poznavnja tajnog ključa. No, uz poznavanje svih n tajnih ključeva d_j možemo redom dešifrirati sve vanjske slojeve u (1.1) i na taj način otkriti tajnu S.

Ovo je također primjer podjele tajne kod koje su potrebne sve dionice tajne da bi tajna mogla biti rekonstruirana. Međutim, ovo je primjer *sigurne podjele tajne* jer svatko tko ima manje od n dionica tajne nema niti jednu informaciju o tajni, isto kao i onaj tko ne posjeduje niti jednu dionicu tajne (uz uvjet da je dekriptiranje "nemoguće" za svaki $j = 1, ..., n$).

1.2 Vrste metoda za podjelu tajne

Osim Shamirove i Blakleyeve sheme praga, tijekom godina razvile su se i neke nove metode za podjelu tajne zasnovane na novim idejama i potrebama. Sheme za podjelu tajne mogu se klasificirati na različite načine i po različitim kriterijima. U ovom radu navest ćemo neke od njih.

Što se tiče broja tajni koje treba podijeliti, imamo dvije klase: metode za podjelu *jedine tajne* i metode za podjelu *više tajni*.

Ako metode klasificiramo s obzirom na vrstu dionica, razlikujemo: metode s *jednako ponderiranim dionicama* i *višestruko ponderiranim dionicama*. U *Shamirovoj hijerarhijskoj shemi* dijeljenja tajne, djelitelj tajne dodjeljuje veći broj dionica tajne sudionicima podjele koji su na višim razinama hijerarhije, tako da sudionici višoj razini posjeduju više dionica od sudionika koji su na nižoj razini u hijerarhiji. Tassa (2007.) poboljšao je ovaj koncept kvalitativnim razlikovanjem hijerarhijske razine, tj. dionice tajne sudionika s više razine sadrže više informacija o izvornoj tajni od dionica koje posjeduju sudionici podjele koji su na nižoj razini u hijerarhiji.

1.2. Vrste metoda za podjelu tajne

Metode za podjelu tajne možemo klasificirati i s obzirom na način podjele dionica. Tako razlikujemo:

- *Proaktivno dijeljenje tajne* - temeljna tehnika u protokolima proaktivne sigurnosti. Metoda se temelji na periodičnom ažuriranju distribuiranih dionica (ključeva) u nekoj shemi za podjelu tajne tako da napadač ima manje vremena za ugrožavanje dionica. Napadač može rekonstruirati tajnu samo ako pronađe dovoljno neažurnih dionica da dosegne prag potreban za rekonstrukciju tajne. Ako to ne uspije, sve neažurne dionice koje je do tada prikupio postaju beskorisne i tajna je sigurna.

- *Dinamičko dijeljenje tajne* - omogućuje promjenu strukture pristupa tajni. Djelitelj tajne ima mogućnost promijeniti broj dionica i/ili sudionika podjele tajne potrebnih za rekonstrukciju tajne (u različitim vremenskim trenucima).

- *Dijeljenje tajni uz mogućnost veta* - omogućuje blokiranje rekonstrukcije tajne. Ovlašteni skup sudionika podjele tajne može spriječiti bilo koji drugi skup sudionika podjele u rekonstrukciji tajne.

U praksi, sudionici podjele tajne (i dijelitelj tajne) imaju ograničene računalne resurse, stoga kod računalnih shema za podjelu tajne trebamo nešto drugačiju definiciju sigurnosti i provjerljivosti nego što je to kod teorijskih shema za podjelu tajne. S obzirom na to imamo sljedeću podjelu:

- *Računalno sigurno dijeljenje tajni* (eng. *computationally secure secret sharing*). Nedostatak bezuvjetno sigurnih shema za podjelu tajne je što takve sheme za pohranu i prijenos dionica zahtjevaju količinu memorije jednaku veličini tajne puta broj dionica. Ako je veličina tajne značajna, recimo 1 GB, a broj dionica 10, sudionici podjele moraju pohraniti

10 GB podataka. Stoga se kod računalno sigurnog dijeljenja tajni odustaje od zahtjeva za bezuvjetnom sigurnošću i koriste se zamjenske tehnike koje značajno povećavaju učinkovitost shema za podjelu tajne, a sigurnost sheme ovisi o nekim računalnim pretpostavkama.

- *Provjerivo dijeljenje tajne* (eng. *verifiable secret sharing* (VSS)). Za shemu podjele tajni kažemo da je *provjerljiva* ako postoje dodatni podatci koji sudionicima podjele tajne omogućuju da potvrde svoje dionice kao dosljedne. Na taj način se osigurava da čak i ako je djelitelj tajne zlonamjeran, tajna je dobro definirana i sudionici je mogu rekonstruirati (u standardnoj podjeli tajne pretpostavlja se da je djelitelj tajne dobronamjeran). Kod provjerljivog dijeljenja tajne, pošteni sudionici trebali bi moći rekonstruirati tajnu, a nepošteni sudionici ne bi smjeli dobiti nikakvu informaciju o tajni.

Tompa i Woll (1988.) uvode varanje u tajno dijeljenje. Pojedinačni sudionik zavara druge sudionike korištenjem krivih dionica tajne. Ogata i suradnici (1995.) su nakon toga predložili učinkovit način otkrivanja varanja u dijeljenju tajne:

- *Robustno dijeljenje tajne* (eng. *robust secret sharing* (RSS)). Robusno dijeljenje tajne ima sva uobičajena svojstva tajnog dijeljenja, ali se dodatno zahtijeva da kada u postupku rekonstrukcije tajne imamo najviše t krivih ili oštećenih dionica (od njih ukupno n) i dalje je moguće dobiti ispravnu tajnu (s dovoljno velikom vjerojatnošću). Koncept robusnog dijeljenja tajne (RSS) usko je povezan s konceptom provjerljivog dijeljenja tajne (VSS). Samo što RSS tolerira samo nepoštene sudionike podjele, dok VSS uz to tolerira i nepoštenog djelitelja tajne.

1.2. Vrste metoda za podjelu tajne

Na temelju tehnika koje se koriste, metode za podjelu tajne mogu se podijeliti na različite klase. Neke od njih su:

- *Dijeljenje tajne korištenjem polinoma* - ove sheme koriste polinome i polinomnu interpolaciju, posebno Lagrangeovu interpolaciju (Shamir, 1979.), Birkhoffovu interpolaciju (Tassa, 2007.), za podjelu i rekonstrukciju tajne. Dionice tajne su vijednosti slučajno generiranog polinoma u slučajno odabranim točakama.

- *CRT sheme* - ove sheme oslanjaju se na *Kineski teorem o ostatcima* (eng. *Chinese remainder theorem* (CRT)). Asmuthova i Bloomova (1983.) shema dijeljenja tajni, temeljena na CRT-u, dijeli tajnu S između n sudionika korištenjem modularne aritmetike tako da bilo kojih t sudionika može rekonstruirati tajnu pomoću CRT-a.

- *Anonimno dijeljenje tajne* - ovdje identiteti sudionika podjele nisu potrebni za rekonstrukciju tajne. Tajna se može rekonstruirati bez znanja koji sudionik ima koju dionicu tajne.

- *Sustavno dijeljenje tajni na temelju blok koda* - više skupova tajni spakira se u skup velikih tajni pomoću CRT-a, a zatim dijeli konstruiranjem tajnog polinoma čiji su koeficijenti te velike tajne (Chien i sur., 2000.).

- *Dijeljenje tajni u crnoj kutiji* - kod shema za podjelu tajne u crnoj kutiji dionice se izračunavaju iz tajne i slučajnih elemenata neke konačne Abelove grupe isključivo korištenjem grupovne operacije, tj. uzimajući $\mathbb{Z}$-linearne kombinacije tajne i slučajnih elemenata grupe. Sheme su neovisne o strukturi grupe ili redoslijedu izbora elemenata. Dijeljenje tajni u crnoj kutiji uveli su Desmedt i Frankel (1995.).

- *Vizualno dijeljenje tajne* - tajna i dionice tajne su (digitalne) slike. Šifriranjem piksela, slika se dijeli na n dionica (ovdje ih nazivano *folije*) i distribuira sudionicima. Samo "preklapanjem" dovoljnog broja folija rekonstruirana slika je čitljiva.

1.3 Primjena metoda podjele tajne

Kako što smo već rekli, metode za podjelu tajne primjenjuju se u situacijama kada važni podatci moraju biti sigurno pohranjeni i dobro zaštićeni. Pogledajmo sada nekoliko primjera gdje su sve zastupljene metode za podjelu tajne.

- *HSM moduli* (eng. *hardware security module*) su vrsta sigurnih kriptoprocesora zaduženih za upravljanje ključevima te ubrzanje kriptografskih procesa kao što su digitalni potpisi, provjere valjanosti i integriteta prilikom pristupa ključevima poslužiteljskih aplikacija itd. Svaki moderni HSM modul koristi Shamirovo tajno dijeljenje.

- Kod izgradnje sigurnih protokola za *provjere autentičnosti* sa slabim lozinkama, gdje curenje podataka jednog poslužitelja ne dopušta napade na lozinku.

- U situacijama kod kojih pristup važnom resursu mora biti ograničen (npr. otvaranje trezora banke ili lansiranje nuklearne rakete).

- U *bankarskim transakcijama* gdje korisnici putem mobilnog telefona imaju jednostavan pristup svojim računima i novcu. Uz druge kriptografske metode, metode za podjelu tajne poboljšavaju nedostatke tog sustava.

1.3. Primjena metoda podjele tajne

- Kod *elektroničkog glasovanja* (eng. *e-voting*) koji zamjenjuje tradicionalni sustav glasovanja. Sheme e-glasovanja koriste metode za podjelu tajne. Na taj način nisu zadovoljeni samo osnovni sigurnosni ciljevi kao što su nevaranje, univerzalna provjerljivost, povjerljivost i anonimnost, već se također postižu dodatna svojstva, uključujući bezuvjetnu sigurnost i "otpor prisili" (prislila je kad protivnik od "prisiljenih" glasača zahtijeva da glasuju na određeni način, suzdrže se od glasovanja ili čak da otkriju svoje tajne ključeve).

- U *vizualnoj kriptografiji*, koju su uveli Adi Shamir i Moni Naor (izraelski infomatičar) 1994. godine. Tajni podatak je ovdje digitalana slika (koja može sadržavati i neki tekst). Primjerice, prijenos *medicinske slike* preko lokalnih ili širokopojasnih mreža postao je popularan s brzim razvojem mrežnih tehnologija. Istraživanje sigurnog prijenosa medicinske slike ima dva cilja. Prvi cilj je osiguravanje netaknutosti i autentičnosti prenesene slike, a drugi je skrivanje elektroničkog kartona pacijenta (EPR-a) u slikama kako bi se uštedjelo na propusnosti i zahtjevu za pohranom. Za postizanje oba cilja koriste se razne steganografske tehnike ili tehnika vodenog žiga. Međutim, postoje dva sigurnosna problema svojstvena ovim tehnikama. Prvi problem je što se slika ne može oporaviti bez pogrešaka ako je medij namjerno oštećen tijekom prijenosa, a drugi problem je nedostatak povjerenja u nekog primatelja, što može rezultirati curenjem povjerljive medicinske dokumentacije. Za rješavanje ovih sigurnosnih problema koristi se Shamirova $(t, n)-$shema praga. Korištenjem ove metode moguće je pohraniti duže EPR nizove, osigurati netaknutost i autentičnost medicinske slike te istodobno zadovoljiti sve zahtjeve za sigurnost podataka.

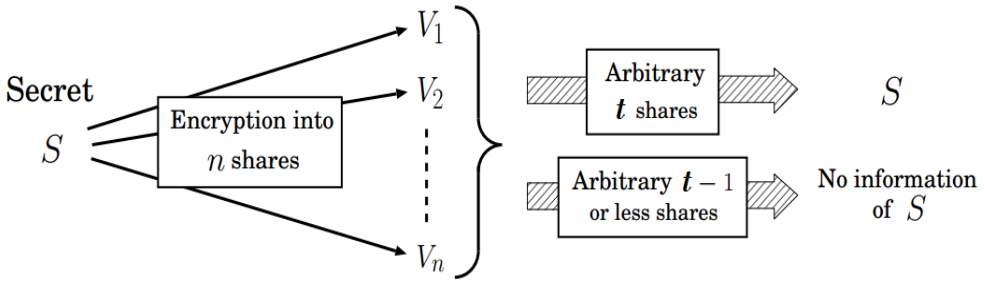
1.3. Primjena metoda podjele tajne

- *Računarstvo u oblaku* (eng. *cloud computing)* je revolucionarni koncept koji nudi novi način pristupa osobnim podacima i aplikacijama, koji više nisu smješteni na računalu već u "oblaku" – što znači da nekom programu i dokumentima možemo pristupiti s većeg broja uređaja, u bilo koje vrijeme i s različitih lokacija. Sve što je potrebno je internetska veza. Nezavisni pružatelji usluge u "oblak" okruženju moraju osigurati da pohranjivanje, pristup i obrada podataka u "oblaku" budu sigurni, povjerljivi, netaknuti i stalno dostupni. Stoga pružatelji usluge koriste paletu sigurnosnih mehanizama (primjerice kolokacije – podaci na više mjesta), dnevne sigurnosne kopije podataka, ali i razne kriptografske algoritme te sheme za podjelu tajne pa sigurnosni rizik praktično ne postoji.

Poglavlje 2

Osnovne metode za dijeljenje tajne

Shema za podjelu tajne, kao što smo već spomenuli, kriptografska je metoda koja šifrira tajnu informaciju S dijeleći je na n dijelova (dionica) $V_1, \ldots, V_n$. Svaki dio V_i sam za sebe nema nikakvu informaciju o tajni S te ona može biti rekonstruirana samo uz određeni broj prikupljenih dionica. Primjer jedne takve sheme je i *(t,n) - shema praga* koju smo također spomenuli i za koju ćemo u nastavku dati precizniju definiciju. Ideja (t, n) - sheme praga je ilustrirana na Slici 2.1.



Slika 2.1: (t,n) - shema praga

Sa Slike 2.1 vidimo da se s bilo kojih t od n dionica može rekonstruirati tajnu S, ali s bilo kojih $t-1$ ili manje dionica, to ne može učiniti. Stoga, čak i ako se $n-t$ dionica uništi, i dalje je tajnu moguće rekonstruirati pomoću preostalih t dionica. Također, čak i ako napadač ukrade $t-1$ dijelova, nikakvu informaciju o tajni S neće moći dobiti. To znači da je shema dijeljenja tajne *sigurna* u odnosu na informacije, ali i krađu. Možemo reći da je takva shema *bezuvjetno sigurna* jer se ne temelji na "teškim problemima" poput faktorizacije cijelih brojeva ili računanja diskretnog logaritama. Stoga je ova metoda prikladna za dugotrajno pohranjivanje podataka. U sljedećim poglavljima, vidjet ćemo kako su tvorci ideje (t, n) - sheme praga Shamir i Blakley konkretno realizirali ovu ideju. Definirajmo sada preciznije što je to shema praga.

Definicija 2.1 *Neka su t i n prirodni brojevi, tako da je $t \leq n$.* ***(t,n)** - **shema praga** (eng. threshold sheme) je metoda za podjelu tajne (ključa) K između članova skupa od n sudionika (označimo ga s $\mathcal{P}$), tako da bilo kojih t sudionika može rekonstruirati tajnu K, ali bilo koji skup sudionika čiji je broj članova manji od t ne može otkriti K.*

Za (t, n) - shemu praga imamo:

- Ako je $t = 1$, imamo trivijalno dijeljenje tajne jer je samo jedan sudionik potreban za njeno otkrivanje.
- Ako je $t = n$, svi dijelovi su potrebni da bi se rekonstruirala tajna. U tom slučaju postoji nekoliko shema podjele. Jedan primjer takve sheme je da kodiramo tajnu K kao binarni broj s proizvoljne duljine. Zatim svakom sudioniku P_i, osim zadnjem, damo slučajni binarni broj y_i iste duljine kao i s. Posljednjem sudioniku damo rezultat

$$y_n = s\, XOR\, y_1\, XOR\, y_2\, XOR ... XOR\, y_{n-1},$$

gdje je s XOR označena operacija *isključivo ili*. Tajna s se može dobiti kao XOR svih brojeva y_i dodijeljenih sudionicima P_i, $i = 1, .., n$.

- Za slučaj $1 < t < n$, imamo korisnu shemu u kojoj za rekonstrukciju tajne nisu potrebni svi sudionici.

U prethodnom poglavlju spomenuli smo da metode za podjelu tajne zadovoljavaju tri temeljna kriterija informacijske sigurnosti pa pogledajmo kako (t, n) - sheme praga zadovoljavaju te kriterije :

- *povjerljivost* - ako protivnik želi otkriti tajnu, mora "prevariti" najmanje t sudionika podjele i oteti njihove dionice.

- *netaknutost* - ako protivnik želi uništiti ili izmijeniti tajnu, mora oteti najmanje $n - t + 1$ dionica.

- *dostupnost* - ako je vrijednost praga t dana i poznata, dostupnost tajne se povećava kako se povećava vrijednost n. Ako se povećava broj sudionika podjele n, onda će se poboljšavati povjerljivost i netaknutost tajne ukoliko se i t poveća.

Sada ćemo vidjeti kako izgleda *poopćena shema podjele tajne* te ćemo dati neke osnovne definicije koje ćemo koristiti u sljedećim poglavljima.

Definicija 2.2 *Neka je $\mathcal{P}$ skup sudionika te $\mathcal{A}$ neki skup podskupova od $\mathcal{P}$. Dijelovi tajne su konstruirani i distribuirani na način da bilo koji skup sudionika $A \in \mathcal{A}$ može rekonstruirati tajnu S, ali bilo koji skup sudionika $B \subseteq \mathcal{P}$ takav da $B \notin \mathcal{A}$ to ne može napraviti. Takvu shemu nazivamo* ***poopćena shema za podjelu tajne.***

Uočimo da su (t, n) - sheme praga specijalna klasa poopćenih shema za podjelu tajne kod kojih se skup $\mathcal{A}$ sastoji od podskupova skupa $\mathcal{P}$ jednake kardinalnosti t.

Definicija 2.3 *Poopćena shema podjele tajne je* ***savršena*** *ako bilo koji podskup sudionika $A \in \mathcal{A}$ može rekonstruirati tajnu S, dok bilo koji skup sudionika $B \subseteq \mathcal{P}$, $B \notin \mathcal{A}$ ne može otkriti niti jednu informaciju o tajni S.*

Efikasnost metoda za podjelu tajne mjeri se *brzinom protjecanja informacija.*

Definicija 2.4 *U shemama za podjelu tajne,* ***brzina protjecanja informacija*** *za pojedinog sudionika je omjer između veličine dijeljene tajne i veličine dionice tajne koju sudionik posjeduje. Brzina protjecanja informacija cijele sheme je minimum brzina protjecanja informacija svih sudionika.*

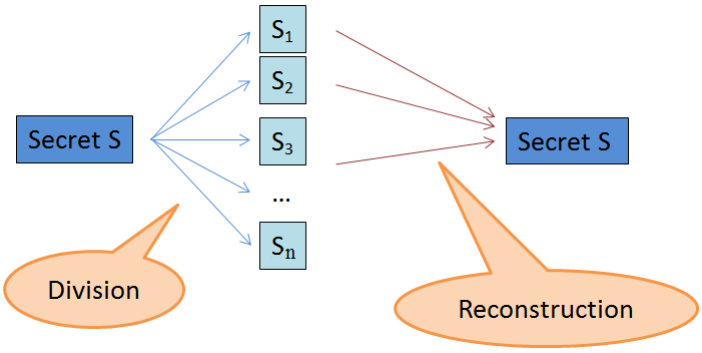
Savršena granica podjele: U bilo kojoj savršenoj shemi za podjelu tajne je veličina dionice svakog sudionika veća ili jednaka od veličine tajne. Stoga, sve savršene sheme podjele tajne imaju brzinu protjecanja informacija ≤ 1. Ako bi sudionik podjele tajne $P_i \in A \in \mathcal{A}$ imao dionicu tajne čija je veličina manja od veličine cijele tajne, tada bi ostali sudionici podjele tajne iz podskupa A, koristeći svoje dionice, mogli doći do nekih informacija o tajni budući da bi se tada rekonstrukcija tajne svela na rekonstukciju dionice koju posjeduje sudionik P_i, a njena veličina je manja od veličine tajne. No, tada shema po definiciji više nije savršena.

Definicija 2.5 *Metoda za podjelu tajne je* ***idealna*** *ako je savršena i ako joj je brzina protjecanja informacija jednaka* 1.

2.1 Shamirova metoda dijeljenja tajne

Shamirova shema tajnog dijeljenja je algoritam koji je 1979. godine predložio poznati izraelski kriptograf Adi Shamir. Pomoću ove metode moguće je podijeliti tajnu (obično tajni kriptografski ključ) na jedinstvene dijelove tzv. *dionice*, tako da je samo jedan dio tih dionica potreban za rekonstrukciju izvorne tajne.

U svom radu *How to Share a Secret* iz 1979. godine, Adi Shamir je objasnio koncept svoje ideje o (t, n) - shemi praga koju koristi kako bi efikasno podijelio tajnu na n dijelova. Označimo s K tajnu (ključ) koji *djelitelj tajne* $\mathcal{D}$ mora podijeliti unutar grupe $\mathcal{P}$ koja ima n članova tzv. *sudionika*. Pretpostavljamo da $\mathcal{D} \notin \mathcal{P}$. Djelitelj $\mathcal{D}$ dijeli tajnu K tako da svaki sudionik $P_i \in \mathcal{P}$, $i = 1, .., n$, dobije svoju dionicu tajne**.** Raspodjela dionica je tajna te niti jedan sudionik ne zna nikakvu informaciju o dionicama ostalih sudionika. Za rekonstrukciju izvorne tajne K, nisu potrebne sve dionice tajne, nego Shamirova shema zahtijeva *minimalan* broj dionica i taj se minimum t naziva *pragom* (vidjeti Definiciju 2.1).



Slika 2.2: Shamirova metoda podjele tajne

2.1.1 Shamirova (t, n)-shema praga

Shamirova (t,n)-shema praga

INICIJALIZACIJA:

1. Djelitelj tajne $\mathcal{D}$ odabire n različitih ne-nul elemenata iz $\mathbb{Z}_p$, u oznaci x_i, $1 \leq i \leq n$. Ovdje je p prost broj takav da je $n + 1 \leq p$. Za $1 \leq i \leq n$, djelitelj $\mathcal{D}$ vrijednosti x_i daje sudioniku $\mathcal{P}_i$. Vrijednosti x_i su javne.

RASPODJELA DIONICA:

2. Neka je tajna (ključ) koju djelitelj $\mathcal{D}$ želi podijeliti neki element K iz $\mathbb{Z}_p$. Djelitelj $\mathcal{D}$ prvo tajno i nasumično odabire $t - 1$ elemenata $a_1, \ldots, a_{t-1}$ iz $\mathbb{Z}_p$.

3. Za $1 \leq i \leq n$, $\mathcal{D}$ računa vrijednosti $y_i = a(x_i)$, gdje

$$a(x) = K + \sum_{j=1}^{t-1} a_j x^j \pmod{p}. \tag{2.1}$$

4. Za svaki $1 \leq i \leq n$, $\mathcal{D}$ daje dionicu y_i sudioniku P_i.

Sada ćemo detaljnije objasniti konstrukciju navedene Shamirove (t, n)-sheme praga. Neka je $\mathcal{P} = \{P_i : 1 \leq i \leq n\}$ skup svih sudionika podjele tajne, $\mathcal{S}$ skup svih mogućih dionica tajne i $\mathcal{K}$ skup svih mogućih tajni (ključeva) K. Podskupina sudionika $\mathcal{B} \subseteq \mathcal{P}$ udružuje svoje dionice kako bi rekonstruirali tajnu $K \in \mathcal{K}$. Ako je $|\mathcal{B}| \geqslant t$, onda sudionici u podskupini $\mathcal{B}$ mogu izračunati vrijednost tajne (ključa) K kao funkciju dionica koje svaki od njih posjeduje. U protivnom, tj. ako je $|\mathcal{B}| \leq t - 1$, ne mogu izračunati tajnu K.

Neka je $\mathcal{K} = \mathbb{Z}_p$, gdje je $p \geqslant n+1$ prost broj. Dakle, skup svih mogućih tajni (ključeva) je $\mathbb{Z}_p$, tj. polje ostataka modulo p. Također, neka je i skup $\mathcal{S} = \mathbb{Z}_p$. Dakle, tajna K i pojedine dionice tajne y_i dodijeljene sudionicima P_i su elementi polja $\mathbb{Z}_p$. U Shamirovoj (t, n) - shemi praga, djelitelj $\mathcal{D}$ konstruira tajni polinom $a(x) \in \mathbb{Z}_p[x]$ stupnja najviše $t-1$ oblika (2.1), u kojem je $K \in \mathcal{K}$ fiksan. Svakom sudioniku P_i dodijeljena je točka $(x_i, y_i) := (x_i, a(x_i))$, gdje je x_i javan, a y_i tajan podatak, tj. poznat samo sudioniku P_i.
Pretpostavimo sada da je podskup skupa skudionika $\mathcal{B}$ kardinalnosti $|\mathcal{B}| = t$. Pogledajmo sada kako sudionioci iz $\mathcal{B}$ mogu rekonstruirati tajnu K. Za rekonstrukciju se koristi polinomna interpolacija. Stoga se prvo podsjetimo što je to *interpolacijski polinom.*

INTERPOLACIJSKI POLINOM

Pretpostavimo da istražujemo nepoznatu funkciju $x \to f(x)$ te da imamo niz podataka

$$(x_0, f(x_0)),\ (x_1, f(x_1)), \ldots,\ (x_n, f(x_n)), \tag{2.2}$$

gdje su svi x_i različiti. Pretpostavimo nadalje da je f realna funkcija realne varijable. Tada uređeni parovi iz (2.2) u ravnini predstavljaju točke grafa Γ_f funkcije f. Dakle, poznate su nam vrijednosti funkcije f u točkama $x_0, \ldots, x_n$, ali sama funkcija nam nije poznata. No, što ako želimo izračunati približne vrijednosti funkcije f u točkama x za $x \neq x_i$? U tom slučaju nepoznatu funkciju f možemo zamijeniti drugom, nama poznatom funkcijom, koja poprima iste vrijednosti kao f u zadanim točkama $x_0, \ldots, x_n$. Najjednostavnija takva funkcija je polinom. Dakle, kriterij za odabir polinoma p je da vrijedi $p(x_i) = f(x_i) = y_i$ za sve $i = 0, 1, \ldots, n$. To nas vodi do pojma *interpolacijskog polinoma.* Vrijedi sljedeći teorem.

Teorem 2.6 *Neka je $n \in \mathbb{N}_0$. Za dane točke $(x_k, f(x_k))$, $k = 0, ..., n$, gdje je $x_i \neq x_j$ za $i \neq j$, postoji jedinstveni (interpolacijski) polinom nad $\mathbb{R}$ stupnja najviše n oblika*

$$P_n(x) = a_0 + a_1 x + ... + a_n x^n,$$

za koji vrijedi $P_n(x_k) = f(x_k)$, za sve $k = 0, 1, ..., n$.

Dokaz. Ako u $P_n(x)$ uvrstimo redom točke x_k, $k = 0, 1, ..., n$, dobivamo sustav

$$\begin{aligned} a_0 + a_1 x_0 + \ldots + a_n x_0^n &= f(x_0) \\ a_0 + a_1 x_1 + \ldots + a_n x_1^n &= f(x_1) \\ &\vdots \\ a_0 + a_1 x_n + \ldots + a_n x_n^n &= f(x_n) \end{aligned}$$

od $n+1$ linearnih jednadžbi s $n+1$ nepoznanica a_0, $a_1, ..., a_n$. Ovaj sustav možemo zapisati matrično kao $Va = y$, pri čemu je

$$V = \begin{bmatrix} 1 & x_0 & x_0^2 & x_0^3 & \ldots & x_0^{n-1} & x_0^n \\ 1 & x_1 & x_1^2 & x_1^3 & \ldots & x_1^{n-1} & x_1^n \\ . & . & . & . & \ldots & . & . \\ . & . & . & . & \ldots & . & . \\ . & . & . & . & \ldots & . & . \\ 1 & x_n & x_n^2 & x_n^3 & \ldots & x_n^{n-1} & x_n^n \end{bmatrix}, \; a = \begin{bmatrix} a_0 \\ a_1 \\ . \\ . \\ . \\ a_n \end{bmatrix} \text{ i } \; y = \begin{bmatrix} y_0 = f(x_0) \\ y_1 = f(x_1) \\ . \\ . \\ . \\ y_n = f(x_n) \end{bmatrix}.$$

Matrica V je *Vandermondeova matrica* i za nju vrijedi da je

$$\det V = \begin{vmatrix} 1 & x_0 & x_0^2 & x_0^3 & \ldots & x_0^{n-1} & x_0^n \\ 1 & x_1 & x_1^2 & x_1^3 & \ldots & x_1^{n-1} & x_1^n \\ . & . & . & . & \ldots & . & . \\ . & . & . & . & \ldots & . & . \\ . & . & . & . & \ldots & . & . \\ 1 & x_n & x_n^2 & x_n^3 & \ldots & x_n^{n-1} & x_n^n \end{vmatrix} = \prod_{i<j} (x_i - x_j) \neq 0,$$

budući da je $x_i \neq x_j$ za $i \neq j$. Stoga je matrica sustava V invertibilna pa sustav linearnih jednadžbi ima jedinstveno rješenje dano s $a = V^{-1}y$, iz čega direktno slijedi tvrdnja teorema. ■

Vratimo se sada na Shamirovu shemu praga i pretpostavimo da skup od t sudionika želi otkriti tajni ključ K. Označimo te sudionike s $P_{i_1}, ..., P_{i_t}$. Za svaki $1 \leq j \leq t$, znamo vrijednosti

$$x_{i_j} \quad \text{i} \quad y_{i_j} = a(x_{i_j}),$$

gdje je a tajni polinom kojeg je odabrao djelitelj $\mathcal{D}$. Budući da je a polinom stupnja najviše $t-1$, možemo ga zapisati u obliku

$$a(x) = a_0 + a_1 x + \ldots + a_{t-1}x^{t-1}, \tag{2.3}$$

gdje su koeficijenti $a_0, ..., a_{t-1}$ nepoznati elementi iz $\mathbb{Z}_p$ i $a_0 = K$ je traženi ključ. Dakle, vrijednost polinoma a u točki $x = 0$ jednaka je vrijednosti ključa K. Kako je $y_{i_j} = a(x_{i_j})$, $1 \leq j \leq t$, dobivamo t linearnih jednadžbi s t nepoznanica $a_0, ..., a_{t-1}$. Bez smanjenja općenitosti pretpostavimo da je $i_1 = 1$, $i_2 = 2, ..., i_{t-1} = t-1$. Na taj način dobili smo sustav od t linearnih jednadžbi s t nepoznanica $a_0, ..., a_{t-1}$ nad poljem $\mathbb{Z}_p$ oblika

$$\begin{aligned} a_0 + a_1 x_1 + \ldots + a_n x_1^{t-1} &= y_1 \\ a_0 + a_1 x_2 + \ldots + a_{t-1} x_2^{t-1} &= y_2 \\ &\vdots \\ a_0 + a_1 x_t + \ldots + a_{t-1} x_t^{t-1} &= y_t. \end{aligned} \tag{2.4}$$

Matrični zapis ovog sustava je

$$\begin{bmatrix} 1 & x_1 & x_1^2 & x_1^3 & \dots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & x_2^3 & \dots & x_2^{t-1} \\ . & . & . & . & \dots & . \\ . & . & . & . & \dots & . \\ . & . & . & . & \dots & . \\ 1 & x_t & x_t^2 & x_t^3 & \dots & x_t^{t-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ . \\ . \\ . \\ a_{t-1} \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ . \\ . \\ . \\ y_{t-1} \end{bmatrix},$$

i vrijedi

$$\det \begin{bmatrix} 1 & x_1 & x_1^2 & x_1^3 & \dots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & x_2^3 & \dots & x_2^{t-1} \\ . & . & . & . & \dots & . \\ . & . & . & . & \dots & . \\ . & . & . & . & \dots & . \\ 1 & x_t & x_t^2 & x_t^3 & \dots & x_t^{t-1} \end{bmatrix} = \prod_{1 \le j < i \le t} (x_i - x_j) \pmod{p}.$$

Pretpostavili smo da su odabrani x_i međusobno različiti pa su razlike $x_i - x_j$ za $i \neq j$, različite od 0. Produkt tih razlika računamo modulo p, tj. računamo produkt ne-nul elemenata $\mathbb{Z}_p$. Budući da je $\mathbb{Z}_p$ je polje (jer je p prost broj), produkt ne-nul elemenata u $\mathbb{Z}_p$ je također različit od 0 (jer u polju nema djelitelja 0). Dakle, zaključujemo da je gornja determinanta različita od 0 pa sustav (2.4) ima jedinstveno rješenje nad $\mathbb{Z}_p$.

Time smo pokazali da *bilo koji podskup od t sudionika podjele, koristeći svoje dionice, može rekonstruirati ključ K* pomoću Shamirove sheme praga.

Primjer 2.7 *Neka je $p = 19$, $t = 3$ i $n = 5$ te neka su javne vrijednosti $x_i = i$, $1 \le i \le 5$. Neka je zadan podskup sudionika $\mathcal{B} = \{P_1, P_2, P_3\} \subset \mathcal{P}$ čiji članovi žele otkriti tajni ključ K i neka su dionice y_i, za $i = 1, 2, 3$ redom*

$11, 9, 3$. *Polinom* $a(x)$ *zapišimo u obliku*

$$a(x) = a_0 + a_1 x + a_2 x^2.$$

U konačnom polju $\mathbb{Z}_{19}$ *računamo vrijednosti* $a(1)$, $a(2)$, $a(3)$ *te dobivamo sustav od tri linearne konruencije*

$$\begin{aligned} a_0 + a_2 + a_2 &\equiv 11 \pmod{19} \\ a_0 + 2a_2 + 4a_2 &\equiv 9 \pmod{19} \\ a_0 + 3a_2 + 9a_2 &\equiv 3 \pmod{19}. \end{aligned}$$

Rješavanjem sustava dobije se jedinstveno rješenje polju $\mathbb{Z}_{19}$, $a_0 = 9$, $a_1 = 4$, $a_2 = 17$ *pa je ključ* $K = a_0 = 9$.

Pretpostavimo sada da imamo skupinu od $t-1$ sudionika koji pokušavaju otkriti tajni ključ K. Svaki od sudionika posjeduje uređeni par (x_i, y_i), gdje je $y_i = a(x_i)$ za sve $i = 1, 2, ..., t-1$ i a je tajni polinom dan s (2.3). Neka je njihova pretpostavka da je tajni ključ jednak $y_0 \in \mathbb{Z}_p$. Uz ovu pretpostavku imamo da je $a_0 = a(0) = y_0$. Analogno kao u prethodnom slučaju dobivamo $t-1$ linearnih jednadžbi s t nepoznanica $a_0, ..., a_{t-1}$. Ako tom sustavu dodamo jednadžbu $a_0 = y_0$, dobijamo sustav od t jednadžbi s t nepoznanica. Matrica tog sustava je Vandermondeova matrica čija je determinanta različita od 0 (jer je $x_i \neq 0$, za $i = 1, 2, ..., t-1$ i $x_t = 0$) pa postoji jedinstveni polinom a_{y_0} takav da vrijedi

$$y_i = a_{y_0}(x_i), \text{ za sve } i \in \{1, ..., t-1\} \text{ i } y_0 = a_{y_0}(0).$$

Iz ovoga zaključujemo da za svaki $y_0 \in \mathbb{Z}_p$ svih $t-1$ uređenih parova (dionica) (x_i, y_i), $i = 1, ..., t-1$, zadovoljava traženi uvjet $y_i = a_{y_0}(x_i)$ i da je $y_0 = a_{y_0}(0)$ ključ. Time smo dokazali da *bilo koji podskup od* $t-1$ *sudionika ne može otkriti tajni ključ* K *te niti jednu informaciju o tom ključu jer, uz* $t-1$ *dionica koje ukupno imaju, svaki element iz* $\mathbb{Z}_p$ *može biti ključ.*

Primjer 2.8 *Pretpostavimo da sudionici P_1 i P_3 iz Primjera 2.7 žele otkriti ključ K. Sudionik P_1 ima vrijednost dionice $y_1 = 11$, a P_3 vrijednost $y_3 = 3$. Za bilo koju vrijednost y_0, postoji jedinstveni polinom $a_{y_0}(x)$ koji poprima vrijednost 11 za $x = 1$, vrijednost 3 za $x = 3$ i vrijednost y_0 za $x = 0$. Podskup $\{P_1, P_3\}$ nema nikakvu informaciju koji od tih polinoma je traženi polinom te stoga nema nikakvu informaciju ni o ključu K.*

2.1.2 Shamirova metoda i Lagrangeov interpolacijski polinom

Za pronalazak koeficijenata interpolacijskog polinoma, nije nužno potrebno rješavati sustav linearni jednadžbi (2.4). Interpolacijski polinom P_n stupnja $\leq n$, za koji vrijedi $P_n(x_k) = f(x_k)$, za sve $k = 0, 1, ..., n$, možemo zapisati korištenjem tzv. *Lagrangeove baze* $\{p_n^{(k)},\ k = 0, ..., n\}$, pri čemu su $p_n^{(k)}$ polinomi stupnja $\leq n$ takvi da je

$$p_n^{(k)}(x_i) = \begin{cases} 0, & i \neq k \\ 1, & i = k \end{cases} = \delta_{ik}.$$

Definirajmo

$$L_n(x) := \sum_{k=0}^{n} f(x_k) p_n^{(k)}(x).$$

Tada je L_n polinom stupnja $\leq n$ i očito vrijedi $L_n(x_k) = f(x_k)$, za sve $k = 0, 1, ..., n$. Odredimo sada polinome $p_n^{(k)}(x)$. Sve točke x_i, za $i = 1, 2, ..., n$ i $i \neq k$ su nultočke polinoma $p_n^{(k)}$ pa $p_n^{(k)}$ možemo zapisati u obliku

$$p_n^{(k)}(x) = C_k(x - x_0)(x - x_1) \cdot \ldots \cdot (x - x_{k-1})(x - x_{k+1}) \cdot \ldots \cdot (x - x_n),$$

gdje je C_k konstanta. Iz uvjeta $p_n^k(x_k) = 1$ dobivamo

$$1 = C_k(x_k - x_0)(x_k - x_1) \cdot \ldots \cdot (x_k - x_{k-1})(x_k - x_{k+1}) \cdot \ldots \cdot (x_k - x_n).$$

Ako su $p_n^{(k)}$ polinomi nad nekim poljem, onda je

$$(x_k - x_0)(x_k - x_1) \cdot \ldots \cdot (x_k - x_{k-1})(x_k - x_{k+1}) \cdot \ldots \cdot (x_k - x_n)$$

ne-nul element tog polja (budući da su svi x_i, $i = 0, 1, ..., n$ međusobno različiti) pa je stoga i invertibilan. Sada je

$$C_k = \frac{1}{(x_k - x_0)(x_k - x_1) \cdot \ldots \cdot (x_k - x_{k-1})(x_k - x_{k+1}) \cdot \ldots \cdot (x_k - x_n)}$$

pa je

$$\begin{aligned} p_n^{(k)}(x) &= \frac{(x - x_0)(x - x_1) \cdot \ldots \cdot (x - x_{k-1})(x - x_{k+1}) \cdot \ldots \cdot (x - x_n)}{(x_k - x_0)(x_k - x_1) \cdot \ldots \cdot (x_k - x_{k-1})(x_k - x_{k+1}) \cdot \ldots \cdot (x_k - x_n)} \\ &= \prod_{j=0, j\neq k}^{n} \frac{x - x_j}{x_k - x_j}. \end{aligned}$$

Dakle, dobili smo da je

$$L_n(x) = \sum_{k=0}^{n} f(x_k) \prod_{j=0, j\neq k}^{n} \frac{x - x_j}{x_k - x_j},$$

što nazivamo *Lagrangeov oblik interpolacijskog polinoma.* Iz ovoga i Teorema 2.6 direktno dobivamo sljedeći teorem.

Teorem 2.9 (Lagrangeova interpolacijska formula) *Neka je p prost broj i $x_0, x_1, ..., x_n$ različiti elementi iz $\mathbb{Z}_p$. Neka su $y_0, y_1, ..., y_n$ (ne nužno različiti) elementi iz $\mathbb{Z}_p$. Tada postoji jedinstveni polinom $A(x) \in \mathbb{Z}_p[x]$ stupnja najviše n, takav da je $A(x_i) = y_i$, $0 \leq i \leq n$. Polinom $A(x)$ je oblika*

$$A(x) = \left(\sum_{k=0}^{n} y_k \prod_{j=0, j\neq k}^{n} \frac{x - x_j}{x_k - x_j} \right) \pmod{p}.$$

Vratimo se sada na Shamirovu shemu praga. Pretpostavimo da skupina $\mathcal{B}$ od t sudionika želi otkriti tajni ključ K. Označimo te sudionike (bez smanjenja općenitosti) s $P_1, ..., P_t$. Za svaki $1 \leq j \leq t$, znamo vrijednosti

$$x_j \quad \text{i} \quad y_j = a(x_j),$$

gdje je a tajni polinom stupnja najviše $t-1$ kojeg je odabrao djelitelj $\mathcal{D}$. Iz Teorema 2.9 slijedi da je traženi polinom a jedinstven te da je oblika

$$a(x) = \left(\sum_{j=1}^{t} y_j \prod_{1 \leq k \leq t, k \neq j} \frac{x - x_k}{x_j - x_k} \right) \pmod{p}. \tag{2.5}$$

Dakle, skupina $\mathcal{B}$ od t sudionika, koristeći svoje dionice, može pronaći polinom a pomoću interpolacijske formule (2.5). Ali oni ne moraju izračunati sve koeficijente polinoma a, nego im je dovoljno odrediti samo njegov slobodni koeficijent a_0 budući da je $a_0 = a(0) = K$ pa je situacija puno jednostavnija. Ako uvrstimo $x = 0$ u Lagrangeovu interpolacijsku formulu (2.5), dobivamo

$$K = \left(\sum_{j=1}^{t} y_j \prod_{1 \leq k \leq t, k \neq j} \frac{x_k}{x_k - x_j} \right) \pmod{p}.$$

Također, možemo definirati

$$b_j = \prod_{1 \leq k \leq t, k \neq j} \frac{x_k}{x_k - x_j} \pmod{p}, \quad \text{za sve } j,\ 1 \leq j \leq t. \tag{2.6}$$

Vrijednosti b_j se mogu izračunati jer su vrijednosti od x_k za sve $1 \leq k \leq t$ javne. Sada imamo

$$K = \sum_{j=1}^{t} b_j y_j \pmod{p}. \tag{2.7}$$

Ključ K je dakle, linearna kombinacija (modulo p) od t dionica tajne.

Primjetimo da u postupku računanja b_j-va zapravo moramo izračunati modularnu vrijednost razlomka. Što zapravo znači $\frac{a}{b} \pmod{m}$ i kako to izračunati? Bez smanjenja općenitosti možemo pretpostaviti da su a i b iz $\mathbb{Z}_m$, gdje je $b \neq 0$. Izraz $\frac{a}{b} \pmod{m}$ je zapravo drugačiji zapis od $a \cdot b^{-1} \pmod{m}$ pa je potrebno prvo izračunati $b^{-1} \pmod{m}$, tj. naći multiplikativni inverz od b u $\mathbb{Z}_m$, ako on postoji. Stoga je $b^{-1} \pmod{m}$ (jedinstveno) rješenje linearne kongruencije $b \cdot x \equiv 1 \pmod{m}$, ako ono postoji. Lako se vidi da samo brojevi $b \in \mathbb{Z}_m^*$ koji su relativno prosti s m imaju multiplikativni inverz, a neki od načina kako pronaći taj inverz su:

- Naivna metoda: računamo redom $b \cdot i \pmod m$, za $0 \leq i \leq m-1$. Onaj i za koji je $b \cdot i \pmod m = 1$ je multiplikativni inverz od b u $\mathbb{Z}_m$. Ovo možemo primjeniti, ako je m dovoljno mali broj;

- Prošireni Euklidov algoritam - puno brža metoda (vidjeti npr. [2, str. 27.]).

Uočimo da prilikom računanja b_j-va moramo izračunati $\frac{x_k}{x_k - x_j} \pmod p$ za sve $1 \leq k \leq t$, pri čemu je $k \neq j$. Dakle, potrebno izračunati $(x_k - x_j)^{-1} \pmod m$ za sve $1 \leq k \leq t$. Kako je $x_k \neq x_j$, onda je $(x_k - x_j) \pmod m$ nenul element iz $\mathbb{Z}_p$ pa on ima multiplikativan inverz budući da je svaki nenul elementi iz $\mathbb{Z}_p$ relativno prosti s p jer je p prost broj.

Primjer 2.10 *Vratimo se ponovno na Primjer 2.7 te izračunajmo, za dane vrijednosti dionica sudionika P_1, P_2, P_3, pripadne b_j, $j = 1, 2, 3$. Udruživanjem svojih dionica sudionici P_1, P_2, P_3 računaju b_1, b_2, b_3 korištenjem formule (2.6) na sljedeći način*

$$b_1 = \frac{x_2 x_3}{(x_2 - x_1)(x_3 - x_1)} \pmod{19} = 2 \cdot 3 \cdot 1^{-1} \cdot 2^{-1} \pmod{19} = 3,$$
$$b_2 = \frac{x_1 x_3}{(x_1 - x_2)(x_3 - x_2)} \pmod{19} = 1 \cdot 3 \cdot (-1)^{-1} \cdot 1^{-1} \pmod{19} = 16,$$
$$b_3 = \frac{x_1 x_2}{(x_1 - x_3)(x_2 - x_3)} \pmod{19} = 1 \cdot 2 \cdot (-2)^{-1} \cdot (-1)^{-1} \pmod{19} = 1.$$

Pripadni y_i za $i = 1, 2, 3$ su redom $11, 9, 3$ pa uvrštavanjem u (2.7) dobivamo

$$K = (3 \cdot 11 + 16 \cdot 9 + 1 \cdot 3) \pmod{19} = 9.$$

Što bi se dogodilo ukoliko podskup $\mathcal{B}$ od $t-1$ sudionika pokuša otkriti ključ K? Pretpostavimo da je $y_0 \in \mathbb{Z}_p$ ključ. U Shamirovoj shemi praga ključ je $a_0 = a(0)$. U ovom slučaju za svaki $1 \leq j \leq t-1$, znamo vrijednosti x_j

i $y_j = a(x_j)$. Kako je $a(0) = y_0$, iz Teorema 2.9 slijedi da postoji jedinstveni polinom $a_{y_0}(x)$ takav da je

$$y_j = a_{y_0}(x_j), \;\; 1 \leq j \leq t-1 \text{ i } y_0 = a_{y_0}(0).$$

Kako je to vrijedi za bilo koju vrijednost $y_0 \in \mathbb{Z}_p$, niti jednu vrijednost ključa ne možemo isključiti. Stoga grupa od $t-1$ sudionika ne može otkriti niti jednu informaciju o ključu K.

Vratimo se na Primjer 2.7. Pretpostavimo da sudionici P_1 i P_3 pokušavaju otkriti ključ K s dionicama koje svaki od njih posjeduje. Tada, uz pretpostavku da je proizvoljan y_0 iz $\mathbb{Z}_{19}$ ključ, postoji jedinstveni polinom $a_{y_0}(x)$ koji poprima vrijednost 11 za $x = 1$, vrijednost 3 za $x = 3$ i vrijednost y_0 za $x = 0$. Korištenjem interpolacijske formule (2.5) dobivamo da je taj polinom oblika

$$a_{y_0}(x) = 13y_0(x-1)(x-3) + 4x(x-3) + 10x(x-1) \pmod{19}.$$

Bilo koji član skupa $\{P_1, P_3\}$ ne može znati koji od ovih polinoma je traženi polinom pa samim time ne može dobiti nikakvu informaciju o vrijednosti ključa K.

2.1.3 Pojednostavljena (t, t) - shema praga

U ovom dijelu opisat ćemo konstrukciju pojednostavljene sheme praga za poseban slučaj $n = t$. Konstrukcija vrijedi za skup ključeva $\mathcal{K} = \mathbb{Z}_m$ za koji je i $\mathcal{S} = \mathbb{Z}_m$, gdje je sa $\mathcal{S}$, kao i prije, označen skup svih mogućih dionica ključa. Također, u ovom slučaju m ne mora biti prost broj te ne mora vrijediti $m \geqslant n+1$. Označimo s $K \in \mathbb{Z}_m$ tajnu (ključ) koji djelitelj tajne $\mathcal{D}$ mora podijeliti unutar grupe $\mathcal{P}$ koja ima n sudionika. Sljedeći algoritam opisuje korake koje mora napraviti djelitelj $\mathcal{D}$.

Pojednostavljena (t,t)-shema praga

1. Djelitelj tajne $\mathcal{D}$ tajno i nasumično odabire $t-1$ elemenata iz $\mathbb{Z}_m$, $y_1, ..., y_{t-1}$.

2. Neka je tajna (ključ) K element iz $\mathbb{Z}_m$. $\mathcal{D}$ računa

$$y_t = \left(K - \sum_{i=1}^{t-1} y_i \right) \pmod{m}.$$

3. Za $1 \leq i \leq t$, $\mathcal{D}$ daje dionicu y_i sudioniku P_i.

Očito je da t sudionika ključ K može izračunati koristeći formulu

$$K = \sum_{i=1}^{t} y_i \pmod{m}. \tag{2.8}$$

Pitamo se može li podskup od $t-1$ sudionika izračunati K ? Odgovor je očito ne, jer su dionice $y_1, ..., y_{t-1}$ nasumično i neovisno odabiranih $t-1$ elemenata iz $\mathbb{Z}_m$ (pa je takav i y_t). Promotrimo $t-1$ sudionika iz skupa $\mathcal{P} \setminus \{P_i\}$, gdje je $1 \leq i \leq t$. Oni posjeduju dionice

$$y_1, ..., y_{i-1}, y_{i+1}, ..., y_t.$$

Iz (2.8) dobivamo da je da je

$$K - y_i = \left(\sum_{j=1,\, j \neq i}^{t} y_j \right) \pmod{m}.$$

Dakle, sumiranjem svojih dionica, $t-1$ sudionika iz $\mathcal{P} \setminus \{P_i\}$, $1 \leq i \leq t$, može izračunati $K - y_i$, ali budući da ne znaju nasumično odabranu vrijednost $y_i \in \mathbb{Z}_m$, ne mogu dobiti niti jednu informaciju o vrijednosti ključa K, odnosno, ključ K može biti bilo koji element iz $\mathbb{Z}_m$.

Primjer 2.11 *Promotrimo sljedeću konstrukciju $(t,t)-$sheme praga. Neka je $m = 10$ i $t = 4$ te neka su dionice za četiri sudionika podjele ključa sljedeće*

$$y_1 = 7, \quad y_2 = 2, \quad y_3 = 4, \quad y_4 = 2.$$

Tada je ključ

$$K = (y_1 + y_2 + y_3 + y_4) \pmod m = (7 + 2 + 4 + 2) \pmod{10} = 5.$$

Pretpostavimo sada da prvih troje sudionika žele otkriti ključ K*. Poznato im je* $(y_1 + y_2 + y_3) \pmod{10} = 3 = K - y_4$*, ali ne znaju vrijednost* y_4*. Budući da* y_4 *može poprimiti* 10 *različitih vrijednosti i ključ* $K = (3 + y_4) \pmod{10}$ *može poprimiti* 10 *različitih vrijednosti. Imamo sljedeću korespodenciju:*

$$y_4 = 0 \Longleftrightarrow K = 3, \quad y_4 = 1 \Longleftrightarrow K = 4, \quad \ldots \quad , \; y_4 = 9 \Longleftrightarrow K = 2.$$

2.1.4 Svojstva Shamirove metode podjele tajne

Navest ćemo neka svojstva Shamirove (t, n)-sheme praga.

- *Savršena* - bilo kojih $t-1$ sudionika ne mogu dobiti nikakvu informaciju o tajni. Pojednostavljena (t, t)-shema praga je također savršena, što smo pokazali u prethodnom dijelu poglavlja.

- *Idealna* - jer je savršena i brzina protjecanja informacija je jednaka 1 jer su dionice tajne i sama tajna iz skupa $\mathbb{Z}_p$. Analogno vrijedi i za pojednostavljenu (t, t)-shemu praga.

- *Omogućava dodavanje novih sudionika* - nove dionice tajne (za nove sudionike) mogu se konstruirati i distribuirati bez da to utječe na postojeće dionice trenutnih sudionika.

- *Varirajući nivo kontrole i fleksibilnost* - dodijeljivanjem više dionica jednom sudioniku (od većeg povjerenja) omogućava se veća kontrola nad sudionicima, a time i veća sigurnost. U organizacijama gdje je hijerarhija važna, sudionicima se može dati veći broj dionica ovisno o njihovoj važnosti u organizaciji.

- *Dinamičnost* - sigurnost se može poboljšati povremenim mijenjanjem polinoma (uz fiksni slobodni član) i novom podjelom dionica među istim sudionicima bez da se tajna promijeni.

- *Ne temelji se na nedokazanim tvrdnjama* - za razliku od mnogih kriptografskih metoda, sigurnost ove sheme ne oslanja se na niti jednoj nedokazanoj tvrdnji.

2.2 Blakleyeva metoda za podjelu tajne

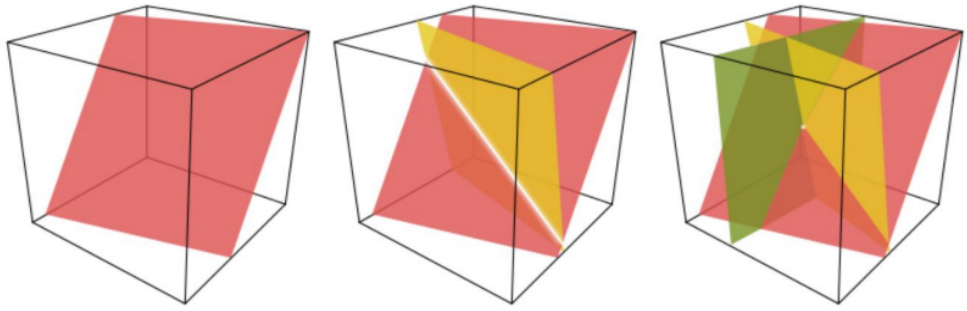
Kao što smo vidjeli, Shamirova shema podjele tajne je (t, n) - shema praga se temelji na polinomnoj interpolaciji nad konačnim poljem $\mathbb{Z}_p$.
Blakeyeva metoda podjele tajne je također (t, n) - shema praga, ali Blakley je koristio geometrijski pristup kako bi konstruirao shemu praga. On pretpostavlja da je tajna neka točka u $t-$dimenzionalnom afinom prostoru nad konačnim poljem i da su dionice tajne hiperravnine koje prolaze kroz tu tajnu točku.

Neformalno, u $t-$dimenzionalnom realnom afinom prostoru, hiperravninu možemo promatrati kao $t-1$ dimenzionalan objekt koji taj prostor dijeli na dva disjunktna dijela - poluprostora, tako da su oba dijela povezana i u uniji s tom hiperravninom daju cijeli prostor. Stoga je u jednodimenzionalnom prostoru hiperravnina točka, u dvodimenzionalnom prostoru to je pravac, dok je trodimenzionalnom prostoru hiperravnina ravnina.

Afina hiperravnina u $t-$dimenzionalnom prostoru nad poljem $\mathbb{F}$ može se opisati linearnom jednadžbom oblika

$$a_1x_1 + a_2x_2 + ... + a_tx_t = b, \quad a_1, a_2, ..., a_n, b \in \mathbb{F}.$$

Dvije različite hiperravnine ili su paralelne ili se sijeku. Blakleyjeva (t, n) -



Slika 2.3: Presjek tri različite međusobno neparalelne hiperravnine

shema praga se temelji na činjenici da se bilo kojih t međusobno neparalelnih hiperravnina $t-$dimenzionalnog prostora siječe u jednoj točki. Primjerice Blakleyjevoj shemi za trodimenzionalan prostor, koja je dana Slikom 2.3, svaka dionica je ravnina, a tajna je točka u kojoj se te tri ravnine sijeku. Dvije dionice nisu dovoljne za rekonstrukciju tajne, ali one ipak daju dovoljno informacija o tajnoj točki budući da ona leži na pravcu koji je presjek te dvije ravnine. Stoga Blakleyeva metoda *nije savršena.*

U Blakeyevoj (t, n) - shemi praga djelitelj tajne $\mathcal{D}$ prvo bira prost broj p i prirodan broj $t \geq 2$. Zatim, u $t-$dimenzionalnom prostoru nad konačnim poljem $\mathbb{Z}_p$ odabire tajnu točku $Q = (x_1^{(0)}, ..., x_t^{(0)})$ i bira n, $n \geq t$ različitih međusobno neparalelnih afinih hiperravnina

$$a_{i1}x_1 + a_{i2}x_2 + ... + a_{it}x_t = c_i, \quad i = 1, ..., n \tag{2.9}$$

tako da svaka od tih hiperravnina prolazi kroz tajnu točku Q. Svakom od n sudionika podjele tajne $P_1, ..., P_n$ djelitej $\mathcal{D}$ daje jednadžbu jedne od hiperravnina i to su odgovarajućih n dionica tajne. Koeficijenti $a_{i1}, ..., a_{it}$ mogu biti javni dok je c_i tajan podatak. Točka presjeka ovih n hiperravnina je točka Q, ali za odrediti tajnu točku Q dovoljno je naći presjek bilo kojih t hiperravnina, od njih ukupno n. Tajna (ključ) K može biti bilo koja od koordinata tajne točke Q ili bilo koja funkcija tih koordinata. Obično se za

K uzima prva koordinata točke presjeka Q.

Pretpostavimo sada da skup od t sudionika podjele želi otkriti tajnu K. Označimo te sudionike (bez smanjenja općenitosti) s $P_1, ..., P_t$. Koristeći jednadžbe svojih hiperravnina (2.9) oni formiraju sustav od t jednadžbi s t nepoznanica $x_1, x_2, ..., x_t$ koji matrično možemo zapisati kao

$$A_t X = C_t,$$

gdje je $A_t = [a_{ij}]$, $X = [x_i]$ i $C_t = [c_i]$. Matrica sustava A_t je regularna (jer su odabrane međusobno neparalelne hiperravnine) pa sustav ima jedinstveno rješenje. Rješavanjem sustava dobivamo koordinate točke Q, odnosno ključ K. Ako je ključ K funkcija svih koordinata točke Q, onda je to opasnost za sigurnost jer svaki sudionik podjele ima dodatnu informaciju o ključu budući da točka Q leži u njegovoj hiperravnini.

Stoga, kod Blakeyeve (t, n) - shema praga, slično kao i kod Shamirove sheme, t sudionika podjele tajne trebaju riješiti sustav od t jednadžbi s t nepoznanica kako bi rekonstruirali tajnu pa su obje ove sheme *linearne sheme praga*. Međutim, kao što smo već vidjeli, Blakleyeva metoda, za razliku od Shamirove, *nije savršena* jer $t-1$ hiperravnina (dionica tajne) nije dovoljnu za rekonstrukciju tajne, ali one ipak daju dovoljno informacija o tajnoj točki budući da ona leži u presjeku tih $t-1$ hiperravnina.

Opišimo sada proces podjele dionica tajne u trodimenzionalnom prostoru nad poljem $\mathbb{Z}_p$ ($(3, n)$ - shema praga).

Blakleyeva (3,n) - shema praga

1. Djelitelj tajne $\mathcal{D}$ odabire prost broj p (promatramo shemu u polju $\mathbb{Z}_p$).

2. Neka je tajna (ključ) $K = x_0$ element iz $\mathbb{Z}_p$. Djelitelj $\mathcal{D}$ tajno i nasumično odabire vrijednosti y_0 i z_0 iz $\mathbb{Z}_p$ i definira točku presjeka $Q(x_0, y_0, z_0)$.

3. Za svaki $i = 1, ..., n$, $\mathcal{D}$ izabere vrijednosti a_i i b_i iz $\mathbb{Z}_p$ te pronađe vrijednost c_i tako da vrijedi

$$c_i \equiv z_0 - a_i x_0 - b_i y_0 \pmod{p}.$$

   Pomoću dobivenih vrijednosti za a_i, b_i i c_i, definira hiperravninu s $z \equiv a_i x + b_i y + c_i \pmod{p}$.

4. Za svaki $i = 1, ..., n$, djelitelj $\mathcal{D}$ daje dionicu tajne (jednadžbu hiperravnine) $z \equiv a_i x + b_i y + c_i \pmod{p}$ sudioniku P_i.

Svakom sudioniku P_i, $i = 1, ..., n$, dodijeljena je jedna hiperravnina dana jednadžbom $z \equiv a_i x + b_i y + c_i \pmod{p}$, koja prolazi točkom $Q(x_0, y_0, z_0)$. Na primjer, u Blakleyevoj $(3, 5)$ - shema praga, dionice tajne za pet sudionika P_i, $i = 1, ..., 5$ možemo zapisati na sljedeći način

$$\begin{aligned}
a_1 x + b_1 y - z &\equiv -c_1 \pmod{p}, \\
a_2 x + b_2 y - z &\equiv -c_2 \pmod{p}, \\
a_3 x + b_3 y - z &\equiv -c_3 \pmod{p}, \\
a_4 x + b_4 y - z &\equiv -c_4 \pmod{p}, \\
a_5 x + b_5 y - z &\equiv -c_5 \pmod{p}.
\end{aligned}$$

Pretpostavimo da bilo kojih troje sudionika P_{i_k}, $k = 1, 2, 3$ želi naći tajnu K. Oni prvo rješavaju sustav

$$\begin{aligned} a_{i_1}x + b_{i_1}y - z &\equiv -c_{i_1} \pmod{p} \\ a_{i_2}x + b_{i_2}y - z &\equiv -c_{i_2} \pmod{p} \\ a_{i_3}x + b_{i_3}y - z &\equiv -c_{i_3} \pmod{p} \end{aligned}$$

nad poljem $\mathbb{Z}_p$. Matrično, gornji sustav možemo zapisati kao kao $AX = C \pmod{p}$, pri čemu je

$$A = \begin{bmatrix} a_{i_1} & b_{i_1} & -1 \\ a_{i_2} & b_{i_2} & -1 \\ a_{i_3} & b_{i_3} & -1 \end{bmatrix}, \; X = \begin{bmatrix} x \\ y \\ z \end{bmatrix} \text{ i } \; C = \begin{bmatrix} c_{i_1} \\ c_{i_2} \\ c_{i_3} \end{bmatrix}.$$

Ovaj sustav je rješiv jer je $(x, y, z) = (x_0, y_0, z_0)$ jedno rješenje tog sustava. Ako je

$$\det A = \left(\sum_{1 \le l < k \le 3} (-1)^{k+1} \left(a_{i_l} b_{i_k} - a_{i_k} b_{i_l} \right) \right) \pmod{p} \neq 0,$$

onda će sustav imati jedinstveno rješenje $(x, y, z) = (x_0, y_0, z_0)$ i sudionici će moći otkriti tajni ključ $K = x_0$.

Ako je p dovoljno velik, vrlo je vjerojatno da će matrica A imati inverz nad $\mathbb{Z}_p$, ili ekvivalentno da će biti $\det A \neq 0 \pmod{p}$, premda to nije garancija. U slučaju trodimenzionalnog prostora nije teško odabrati takve a_i i b_i, $i = 1, .., n$ da bi svaka matrica A, od ukupno $\binom{n}{3}$ mogućih, imala inverz. Tu zapravo nalazimo sličnost izmedu ove metode i Shamirove metode. Kod obje metode problem nalaženja ključa, uz poznavanje t dionica tog ključa, se svodi na rješavanje sustava od t linearnih jednadžbi s t nepoznanica. No, kao što smo vidjeli u Shamirovoj metodi, matrica tog sustava je uvijek Vandermondeova pa uvijek postoji jedinstveno rješenje sustava. Stoga se Shamirova metoda može promatrati kao specijalni slučaj Blakelyeve metode.

U sljedećem primjeru ćemo vidjeti kao sudionici podjele tajne mogu otkriti tajni ključ u jednoj Blakleyevoj $(3,5)$ - shemi praga.

Primjer 2.12 *Neka je $p = 73$ te neka su sudionicima P_i, $i = 1, ..., 5$, dodijeljene sljedeće jednadžbe hiperravnina:*

$$\begin{aligned} z &\equiv 4x + 19y + 68 \pmod{73}, \\ z &\equiv 52x + 27y + 10 \pmod{73}, \\ z &\equiv 36x + 65y + 18 \pmod{73}, \\ z &\equiv 57x + 12y + 16 \pmod{73}, \\ z &\equiv 34x + 19y + 49 \pmod{73}). \end{aligned}$$

Pretpostavimo da tri sudionika P_1, P_2 i P_3 žele odrediti tajnu točku (x_0, y_0, z_0), odnosno pronaći ključ $K = x_0$. Za to učiniti moraju riješiti sljedeći sustav

$$\begin{bmatrix} 4 & 19 & -1 \\ 52 & 27 & -1 \\ 36 & 65 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} -68 \\ -10 \\ -18 \end{bmatrix} \pmod{73}.$$

Budući da je

$$\det A = \det \begin{bmatrix} 4 & 19 & -1 \\ 52 & 27 & -1 \\ 36 & 65 & -1 \end{bmatrix} \pmod{73} = 19 \neq 0,$$

sustav ima jedinstveno rješenje dano s

$$\begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix} = A^{-1}C \pmod{73} = \begin{bmatrix} 2 & 36 & 35 \\ 70 & 67 & 9 \\ 23 & 30 & 19 \end{bmatrix} \begin{bmatrix} -68 \\ -10 \\ -18 \end{bmatrix} \pmod{73} = \begin{bmatrix} 42 \\ 29 \\ 57 \end{bmatrix}.$$

pa je traženi ključ $K = x_0 = 42$. Na analogan način, bilo koja druga tri sudionika bi mogli rekonstruirati tajni ključ (uz uvjet da je odgovarajuća matrica A invertibilna nad $\mathbb{Z}_{73}$).

2.2.1 Svojstva Blakleyeve metode za podjelu tajne

Sada ćemo navest neka svojstva Blakleyeve sheme, ali i neke njene nedostatke.

- *Nije savršena* - točka koja predstavlja tajnu leži u svim hiperravninama koje su dane sudionicima kao dionice i to je informacija koju svaki sudionik zna.

- *Blakleyeva metoda je manje je prostorno učinkovita od Shamirove metode.* Dionice tajne u Blakleyevoj shemi su t puta veće od same tajne, gdje t predstavlja najmanji broj potrebnih dionica tajne za njenu rekonstrukciju. Primjerice, u Blakleyevoj $(3, n)$ - shemi praga, tajna je $x_0 \in \mathbb{Z}_p$ dok su dionice tajne određene uređenom trojkom $(a_i, b_i, c_i) \in \mathbb{Z}_p^3$. Stoga je kod Blakleyeve sheme brzina protjecanja informacija je manja od 1.

- *Nije idealna* - Blakleyeva shema nije savršena, a brzina protjecanja informacija je manja od 1 pa shema nije idealna.

- *Blakleyevoj shemi nedostaje stvarna implementacija.* Blakley i suradnici su samo opisali smjernice za konstrukciju matrice odgovarajućeg sustava linearnih jednadžbi koja bi osigurala savršenu tajnost, ali sama matrica nije navedena.

Upravo zbog ovih razloga, Shamirova shema je puno popularnija u odnosnu na Blakleyjevu shemu.

2.3 Kineski teorem o ostacima i dijeljenje tajne

U ovom dijelu rada proučit ćemo konstrukciju dvije najvažnije sheme za podjelu tajne koje koriste Kineski teorem o ostatcima, a to su *Mignotteova* i *Asmuth-Bloomova* shema praga. Kineski teorem o ostacima je čest alat u kriptografiji. Njegovu primjenu možemo naći u brojnim kriptografskim algoritmima pa tako i u navedenim metodama za podjelu tajne koje ćemo u nastavku detaljnije opisati. No, prije toga, podsjetit ćemo se kako glasi Kineski teorem o ostacima.

Teorem 2.13 (Kineski teorem o ostatcima) *Neka su $m_1, m_2, ..., m_t$ u parovima relativno prosti prirodni brojevi te neka su $a_1, a_2, ..., a_t$ cijeli brojevi. Tada sustav kongruencija*

$$x \equiv a_1 \pmod{m_1},\ \ x \equiv a_2 \pmod{m_2}, \ldots,\ \ x \equiv a_t \pmod{m_t} \tag{2.10}$$

ima rješenje. Ako je x_0 jedno rješenje, onda su sva rješenja sustava dana s $x \equiv x_0 \pmod{m_1 m_2 \cdots m_t}$.

Ako su $m_1, m_2, ..., m_t$ u parovima relativno prosti prirodni brojevi, Kineski teorem o ostacima nam kaže da postoji jedinstveno rješenje sustava (2.10) koje se nalazi između 0 i $m_1 \cdots m_t - 1$, odnosno u skupu $\mathbb{Z}_{m_1 \cdots m_t}$. Sam dokaz Teorema 2.13 nam daje i način kako to rješenje pronaći (vidjeti npr. [2, str. 49, dokaz Teorema 3.7]). Ideja je da se konstruira shema koja će omogućiti da uz bilo kojih t dionica tajne S (u ovom slučaju ostataka od S modulo m_i) možemo otkriti traženu tajnu, dok s manje od t dionica to ne možemo učiniti. Tajna se može rekonstruirati rješavanjem odgovarajućeg sustava od t linearnih kongruencija pomoću Kineskog teorema o ostatcima kako bi se dobilo jedinstveno rješenje tog sustava (u zadanom intervalu), koje je zapravo tražena tajna. Pogledajmo sada kako su, korištenjem ove ideje, konstruirane dvije metode za podijelu tajne.

2.3.1 Mignotteova (t, n) - shema praga

Mignotteova shema praga koristi poseban niz cijelih brojeva takozvani *Mignotteov niz*, koji se sastoji od n, u parovima relativno prostih prirodnih brojeva takvih da je produkt t najmanjih od njih veći od produkta $t-1$ najvećih među njima. Taj uvjet je jako važan jer se shema temelji na odabiru tajne kao cijelog broja između ta dva produkta. Ovaj uvjet također osigurava da je najmanje t dionica tajne potrebno za rekonstrukciju tajne, bez obzira na to koje su dionice odabrane.

Definicija 2.14 *Neka su dani prirodni brojevi n i t takvi da je $2 \leq t \leq n$. Za niz u parovima relativno prostih prirodnih brojeva $m_1 < m_2 < \cdots < m_n$ kažemo da je $(\mathbf{t}, \mathbf{n})$-**Mignotteov niz** ako vrijedi $m_{n-t+2} \cdots m_n < m_1 \cdots m_t$.*

Mignotteovu shemu možemo opisati na sljedeći način:

Mignotteova (t, n) - shema praga

1. Neka je dan (t, n) - Mignotteov niz $m_1 < m_2 < \cdots < m_n$ i neka je tajna S je slučajno odabran prirodan broj takav da je $\beta < S < \alpha$, gdje je $\alpha = m_1 \cdots m_t$ i $\beta = m_{n-t+2} \cdots m_n$.

2. Za svaki $i = 1, ..., n$, djelitelj tajne $\mathcal{D}$ računa vrijednosti $I_i \equiv S \pmod{m_i}$ i daje dionicu tajne I_i sudioniku podjele tajne P_i.

3. Pomoću t različitih dionica tajne $I_{i_1}, \ldots, I_{i_t}$, tajna S se može rekonstruirati rješavanjem sustava kongruencija

$$x \equiv I_{i_1} \pmod{m_{i_1}}, \ldots, x \equiv I_{i_t} \pmod{m_{i_t}} \tag{2.11}$$

korištenjem Kineskog teorema o ostacima.

Uočimo da, prema Teoremu 2.13, sustav kongruencija (2.11) ima jedinstveno rješenje modulo $m_{i_1} \cdots m_{i_t}$. Budući da je tajna S jedno rješenje navedenog sustava te ono leži u $\mathbb{Z}_{m_{i_1} \cdots m_{i_t}}$ jer je $0 < S < \alpha \leq m_{i_1} \cdots m_{i_t}$, prema Teoremu 2.13, tajna S je jedino rješenje sustava (2.11) koje leži u $\mathbb{Z}_{m_{i_1} \cdots m_{i_t}}$ pa tajnu S možemo rekonstruirati pomoću t različitih dionica tajne.

Pretpostavimo da tajnu S želimo rekonstruirati s $t-1$ dionica $I_{i_1}, \ldots, I_{i_{t-1}}$, za neke $i_1, \ldots, i_{t-1} \in \{1, 2, \ldots, n\}$. Neka je x_0 jedinstveno rješenje sustava

$$x \equiv I_{i_1} \pmod{m_{i_1}}, \ldots, x \equiv I_{i_{t-1}} \pmod{m_{i_{t-1}}}$$

u skupu $\mathbb{Z}_{m_{i_1} \cdots m_{i_{t-1}}}$. Očito je $S \equiv x_0 \pmod{m_{i_1} \cdots m_{i_{t-1}}}$, ali kako je

$$S > \beta = m_{n-t+2} \cdots m_n \geq m_{i_1} \cdots m_{i_{t-1}} > x_0,$$

onda je $S \neq x_0$. Dakle, S je oblika $x_0 + l m_{i_1} \cdots m_{i_{t-1}}$ za neki $l \in \mathbb{Z},\ l \neq 0$ takav da je $\beta < x_0 + l m_{i_1} \cdots m_{i_{t-1}} < \alpha$. Zbog toga, kako bismo osigurali veću razinu sigurnosti, (t, n) - Mignotteov niz mora imati što veći faktor $\frac{\alpha - \beta}{\beta}$, tako da postoji što više mogućih vrijednosti za tajnu S. Iz ovoga očito slijedi da $t-1$ sudionika ne može rekonstruirati tajnu S, ali ipak mogu dobiti nekakvu informaciju o toj tajni pa je Mignotteova metoda je *nije savršena.* Uočimo da Mignotteova shema ima brzinu protjecanja informacija (puno) veću od 1 jer je svaka dionica I_i, $i = 1, ..., n$, puno manja od tajne S budući da vrijedi

$$0 \leq I_i < m_i \leq m_n \leq m_{n-t+2} \cdots m_n < S < m_1 \cdots m_t.$$

Ipak, Mignotteova metoda se koristi u primjenama i to u situacijama kada je veličina dionica odlučujući faktor.

Primjer 2.15 *Neka je zadan niz:* $m_1 = 5$, $m_2 = 7$, $m_3 = 11$, $m_4 = 13$, $m_5 = 17$. *Ovaj niz je* $(3, 5)$ *- Mignotteov niz budući da su brojevi* $m_1, ..., m_5$ *u parovima relativno prosti prirodni brojevi i budući da je*

$$\beta = m_4 m_5 = 221 < 385 = m_1 m_2 m_3 = \alpha.$$

2.3. Kineski teorem o ostacima i dijeljenje tajne

Neka je tajna $S = 297$*, koja očito zadovoljava potreban uvjet* $\beta < S < \alpha$*. Tada su pripadne dionice tajne redom*

$$I_1 \equiv 297 \pmod 5 = 2,\ I_2 \equiv 297 \pmod 7 = 3,\ I_3 \equiv 297 \pmod{11} = 0$$
$$I_4 \equiv 297 \pmod{13} = 11,\ I_5 \equiv 297 \pmod{17} = 8.$$

Pomoću tri različite dionice možemo rekonstruirati tajnu S*. Odaberimo dionice* I_1, I_3 *i* I_4*. Pomoću Kineskog teorema o ostacima rješavamo sustav kongruencija*

$$x \equiv 2 \pmod 5,\ x \equiv 0 \pmod{11},\ x \equiv 11 \pmod{13}. \tag{2.12}$$

Neka je $N = 5 \cdot 11 \cdot 13 = 715$*,* $N_1 = 11 \cdot 13 = 143$*,* $N_2 = 5 \cdot 13 = 65$ *te* $N_3 = 5 \cdot 11 = 55$*. Tada je jedno rješenje sustava (2.12) oblika*

$$x_0 = 143x_1 + 65x_2 + 55x_3,$$

gdje x_1, x_2, x_3 *zadovoljavaju*

$$143x_1 \equiv 2 \pmod 5, \quad 65x_2 \equiv 0 \pmod{11}, \quad 55x_3 \equiv 11 \pmod{13},$$

odnosno

$$3x_1 \equiv 2 \pmod 5, \quad 10x_2 \equiv 0 \pmod{11}, \quad 3x_3 \equiv 11 \pmod{13}.$$

Rješavanjem linearnih kongruencija ("naivnom" metodom ili pomoći proširenog Euklidova algoritma) dobivamo da je $x_1 = 4$*,* $x_2 = 11, x_3 = 8$*. Sada je*

$$x_0 = 143 \cdot 4 + 65 \cdot 11 + 55 \cdot 8 = 1727$$

pa su sva rješenja sustava (2.12) dana s

$$x \equiv 1727 \equiv 297 \pmod{715}.$$

Budući da je $297 \in \mathbb{Z}_{715}$, *onda je tajna* $S = 297$. *Uočimo da su sva rješenja sustava (2.12) dana s* $x_l = 297 + 715l$, $l \in \mathbb{Z}$, *a mi tražimo ono koje se nalazi u intervalu* $(221, 385)$ *i to je očito* $x_0 = 297$.
Pretpostavimo sada da tajnu S *želimo rekonstruirati pomoću dionica* I_1 *i* I_2. *Rješavanjem sustava*

$$x \equiv 2 \pmod 5, \ x \equiv 3 \pmod 7$$

dobili bismo da je $S \equiv 17 \pmod{35}$. *Iz ovoga vidimo da se tajna* S *nalazi u skupu*

$$\{17 + 35l : 221 < 17 + 35l < 385, \ l \in \mathbb{Z}\} = \{227, \ 297, \ 332, \ 367\}.$$

Dakle, sudionici podjele tajne P_1 *i* P_2 *ne mogu rekonstruirati tajnu* S, *ali ipak mogu dobiti nekakvu informaciju o toj tajni.*

Mignotteovu shemu podjele tajni možemo poopćiti pomoću *generaliziranog Mignotteovog niza* čiji članovi nisu nužno u parovima relativno prosti. U tom slučaju, za rekonstrukciju tajne, koristi se općenitija verzija Kineskog teorema o ostacima, a shema se konstruira isto kao (k, n)-Mignotteova shema.

2.3.2 Asmuth-Bloomova (t, n) - shema praga

Asmuth-Bloom shemu podjele tajni predložili su 1983. godine Asmuth i Bloom i ona se također temelji na Kineskom teoremu o ostacima. Za razliku od Mignotteove (t, n) - sheme praga, za koju smo zaključili da nije savršena, Asmuth-Bloomova shema je *savršena.*

Asmuth-Bloomova shema praga također koristi specijalan niz cijelih brojeva kojeg definiramo na sljedeći način.

Definicija 2.16 *Neka su t i n prirodni brojevi takvi da je $2 \leq t \leq n$ i neka su $r, m_1, m_2, \ldots, m_n$ u parovima relativno prosti prirodni brojevi takvi da je $m_1 < m_2 < \ldots < m_n$. Kažemo da je taj niz brojeva $(\mathbf{t}, \mathbf{n})-$**Asmuth-Bloomov niz** ako vrijedi*

$$r \cdot m_{n-t+2} \cdots m_n < m_1 \cdots m_t. \tag{2.13}$$

Opišimo sada Asmuth-Bloomovu shemu praga.

Asmuth-Bloomova (t, n) - shema praga

1. Neka je dan (t, n)-Asmuth-Bloomov niz $r, m_1, m_2, \ldots, m_n$ i neka je tajna S neki element iz skupa $\mathbb{Z}_r$.

2. Za svaki $i = 1, ..., n$, djelitelj tajne $\mathcal{D}$ računa vrijednosti $I_i \equiv (S + \gamma \cdot r) \pmod{m_i}$, gdje je γ tajni cijeli broj kojeg bira $\mathcal{D}$ i za kojeg vrijedi
$$0 < S + \gamma \cdot r < \prod_{i=1}^{t} m_i.$$

3. Pomoću t različitih dionica tajne $I_{i_1}, \ldots, I_{i_t}$, korištenjem Kineskog teorema o ostacima, nađemo jedinstveno rješenje $x_0 \in \mathbb{Z}_{m_{i_1} \cdots m_{i_t}}$sustava
$$x \equiv I_{i_1} \pmod{m_{i_1}}, \ldots, x \equiv I_{i_t} \pmod{m_{i_t}}. \tag{2.14}$$
Tada je tajna S jedinstven element iz $\mathbb{Z}_r$ takav da je $S \equiv x_0 \pmod{r}$.

Uočimo da je $S + \gamma \cdot r$ rješenje sustava (2.14) i sustava

$$x \equiv I_1 \pmod{m_1}, \ldots, x \equiv I_t \pmod{m_t}. \tag{2.15}$$

Kako je

$$0 < S + \gamma \cdot r < m_1 \cdots m_t \leq m_{i_1} \cdots m_{i_t},$$

onda je i $S + \gamma \cdot r \in \mathbb{Z}_{m_{i_1} \cdots m_{i_t}}$ pa je, po Teoremu 2.13, $S + \gamma \cdot r = x_0$. Stoga je $x_0 \pmod r = S$.

Pokažimo sada da je Asmuth-Bloomova shema *savršena*. Pretpostavimo da tajnu S želimo rekonstruirati s $t-1$ dionica $I_{i_1}, \ldots, I_{i_{t-1}}$, za neke $i_1, \ldots, i_{t-1} \in \{1, 2, \ldots, n\}$. Neka je x_0' jedinstveno rješenje sustava

$$x \equiv I_{i_1} \pmod{m_{i_1}}, \ldots, x \equiv I_{i_{t-1}} \pmod{m_{i_{t-1}}} \tag{2.16}$$

u skupu $\mathbb{Z}_{m_{i_1} \cdots m_{i_{t-1}}}$. Budući da je $m_{i_1} \cdots m_{i_{t-1}} \leq m_{n-t+2} \cdots m_n$, iz (2.13) slijedi da je

$$r \cdot m_{i_1} \cdots m_{i_{t-1}} < m_1 \cdots m_t$$

pa je $x_0' + j m_{i_1} \cdots m_{i_{t-1}} < m_1 \cdots m_t$ za $j < r$. Kako je $\gcd\left(r, m_{i_1} \cdots m_{i_{k-1}}\right) = 1$, brojevi $S_j \in \mathbb{Z}_r$, $0 \leq j < r$, definirani s

$$S_j = \left(x_0' + j m_{i_1} \cdots m_{i_{k-1}}\right) \pmod r, \tag{2.17}$$

su svi različiti i ima ih r, stoga je $\{S_j : 0 \leq j < r\} = \mathbb{Z}_r$. Na taj način smo pokazali da uz poznavanje $t-1$ dionica tajne, svaki element iz $\mathbb{Z}_r$ može biti tajna S. Naime, iz (2.17) slijedi da za svaki j, $0 \leq j < r$ postoji $\gamma_j \in \mathbb{Z}$ takav da je $S_j + \gamma_j \cdot r = x_0' + j m_{i_1} \cdots m_{i_{t-1}}$. Tada je

$$S_j + \gamma_j \cdot r \equiv x_0' \pmod{m_{i_1} \cdots m_{i_{t-1}}},$$

pa je $S_j + \gamma_j \cdot r$ rješenje sustava (2.16) za koje vrijedi

$$\begin{aligned} 0 &< S_j + \gamma_j \cdot r = x_0' + j m_{i_1} \cdots m_{i_{t-1}} < (j+1)\, m_{i_1} \cdots m_{i_{t-1}} \\ &\leq r m_{i_1} \cdots m_{i_{t-1}} < m_1 \cdots m_t, \end{aligned}$$

što pokazuje da svaki S_j, $0 \leq j < r$, može biti tajna. Stoga, bilo kojih $t-1$ sudionika ne može otkriti tajnu S te niti jednu informaciju o toj tajni, što

znači da je Asmuth-Bloomova shema savršena. Razlog tome je odabir cijelog broja γ koji je neovisan o tajni S.

Može se pokazati da je kod Asmuth-Bloomova sheme brzina protjecanja informacija manja od 1 (posebno za dovoljno male module $m_1, m_2, \ldots, m_n$), stoga Asmuth-Bloomova shema *nije idealna*. Ali pokazano je da je Asmuth-Bloomova shema s modulima koji su uzastopni prosti brojevi *asimptotski idealna*.

Primjer 2.17 *Neka je zadan niz:* $r = 3, m_1 = 11, m_2 = 13, m_3 = 17, m_4 = 19$*, u parovima relativno prostih prirodnih brojeva. Primjetimo da vrijedi*

$$r \cdot m_3 \cdot m_4 = 3 \cdot 17 \cdot 19 < 11 \cdot 13 \cdot 17 = m_1 \cdot m_2 \cdot m_3,$$

stoga je navedeni niz $(3, 4)$*-Asmuth-Bloomov niz.*
Neka je tajna $S = 2$*. Odaberimo tajni cijeli broj* γ *za kojeg vrijedi*

$$0 < 2 + \gamma \cdot 3 < m_1 \cdot m_2 \cdot m_3 = 2431.$$

Neka je $\gamma = 51$*. Tada je* $2 + \gamma \cdot 3 = 2 + 51 \cdot 3 = 155$ *pa su pripadne dionice redom*

$$I_1 \equiv 155 \pmod{11} = 1, \quad I_2 \equiv 155 \pmod{13} = 12,$$
$$I_3 \equiv 155 \pmod{17} = 2, \quad I_4 \equiv 155 \pmod{19} = 3.$$

Tajnu možemo rekonstruirati koristeći bilo koje tri dionice korištenjem Kineskog teorema o ostatcima. Uzmimo dionice $I_1 = 1, I_2 = 12$ *i* $I_3 = 2$*. Odgovarajući sustav kongruencija je*

$$x \equiv 1 \pmod{11}, \quad x \equiv 12 \pmod{13}, \quad x \equiv 2 \pmod{17}. \tag{2.18}$$

Sva rješenja sustava su dana s

$$x \equiv 5017 \equiv 155 \pmod{2431}$$

pa je $S + 3\gamma = 155$. *Stoga je tajna* $S = 155 \pmod 3 = 2$.

Pretpostavimo sada da tajnu S *želimo rekonstruirati pomoću dionica* I_1 *i* I_4. *Rješavanjem sustava*

$$x \equiv 1 \pmod{11},\ x \equiv 3 \pmod{19}$$

dobili bismo da je $S + 3\gamma \equiv 155 \pmod{209}$. *Stoga je* $S + 3\gamma = 155 + 209j$, *za neki* $j \in \{0, 1, ..., 10\}$ *jer je* $0 < S + 3\gamma < 2431$. *Kako je* $S \in \mathbb{Z}_3$ *dovoljno je promatrati* $j = 0, 1, 2$, *da bismo uočili kako za svaki* $S \in \mathbb{Z}_3$ *postoji* $\gamma \in \mathbb{Z}$ *takav da je* $S + 3\gamma = 155 + 209j$. *Za* $j = 0, 1, 2$, *redom dobivamo* $(S, \gamma) = (2, 51)\,,\ (1, 121)\,,\ (0, 191)\,.$ *Ovo pokazuje da dva sudionika ne mogu otkriti tajnu* S *te niti jednu informaciju o toj tajni jer svaki element iz* $\mathbb{Z}_3$ *može biti tajna.*

I Asmuth-Bloomova metoda se može poopćiti tako da se promatra *generalizirani Asmuth-Bloomov* kod kojeg prirodni brojevi $r, m_1, m_2, \ldots, m_n$ ne moraju nužno biti u parovima relativno prosti.

2.4 Usporedba metoda i njihova primjena

Nakon što smo opisali osnovne metode za podjelu tajne, u ovom dijelu rada sažet ćemo njihove karakteristike.

Metoda	***Godina***	***Tehnika na kojoj se metoda temelji***	***Savršena***	***Idealna***
Shamir	1979.	polinomna interpolacija	Da	Da
Blakley	1979.	geometrija hiperravnine	Ne	Ne
Mignotte	1982.	Kineski teorem o ostacima	Ne	Ne
Ashmut-Bloom	1983.	Kineski teorem o ostacima	Da	Ne

Tablica 2.1: Usporedba temeljnih metoda podjele tajni

2.4. Usporedba metoda i njihova primjena

Iako svaka od navedenih metoda ima svoje prednosti i nedostatke, možemo zaključiti da je Shamirova metoda među boljim metodama u konstrukciji shema za podjelu tajne pa se upravo ona najčešće i koristi. Dva glavna problema Shamirove metode su velika količina memorije koja je potrebna za spremanje svih dionica tajne te *"računski trošak"* potreban za računanje tih dionica, kao i za rekonstrukciju tajne (polinom stupnja $t-1$).
S druge strane, Blakleyeva metoda je svakako zanimljiva jer je ona jedna od prvih metoda podjele tajni koja je potpuno promijenila pristup te se okrenula geometriji hiperravnine kao rješenju problema podjele tajne. Manje je prostorno učinkovita od Shamirove metode, ali ukoliko se dodaju odgovarajuća ograničenja na hiperravnine kao dionice u podjeli tajne, novostvorena shema postaje ekvivalentna Shamirovoj shemi.
Mignotteova i Asmuth-Bloomova metoda koriste klase kongruencije i Kineski teorem o ostacima za konstrukciju sheme praga, a glavna prednost ovih metoda u odnosu na Shamirovu (i Blakleyevu) je računalna složenost rekonstrukcije tajne koja iznosi $\mathcal{O}(t)$, dok je za Shamirovu to $\mathcal{O}(t \log t^2)$ (gdje je t minimalni broj dionica potreban za rekonstrukciju tajne). No, obje sheme su sklone *"curenju informacija"* što ih čini ranjivima u smislu povjerljivosti.

Poglavlje 3

Implementacija Shamirove sheme podjele tajne

U ovom poglavlju opisat ćemo implementaciju Shamirove (t, n) - sheme praga. Implementacija je napravljena u programskom jeziku *Python* uz male modifikacije koje su provedene radi pojednostavljenja i izbjegavanja velikih izračuna.

Python je programski jezik opće namjene, interpretiran i visoke razine kojeg je stvorio Guido van Rossum 1990. godine. Ime dobiva po televizijskoj seriji *Monty Python's Flying Circus*. Po automatskoj memorijskoj alokaciji, Python je sličan programskim jezicima kao što su Perl, Ruby, Smalltalk itd. Python dopušta programerima korištenje nekoliko stilova programiranja kao što su objektno orijentirano, strukturno i aspektno orijentirano programiranje pa je zbog ove fleksibilnosti programski jezik Python sve popularniji. Python se najviše koristi na Linuxu, no postoje i inačice za druge operacijske sustave. Osim toga, Python omogućava brzo i izražajno pisanje kratkih skripti. Skripta je skup naredbi zapisanih u tekstualnoj datoteci, dizajniranih u svrhu rješavanja određenog problema, koja se izvršava kao program.

Zadatak moje Python skripte je omogućiti korisniku unos *lozinke*, *ukupnog broja dionica* na koje se ta lozinka dijeli te unos *minimalnog broja potrebnih dionica* za rekonstrukciju lozinke. Skripta zatim maskira lozinku na način koji ćemo opisati, generira dionice, nasumično izabire dovoljno ponuđenih dionica (minimalan broj potreban za rekonstrukciju) te ponovno rekonstruira tajnu lozinku.

3.1 Opis implementacije

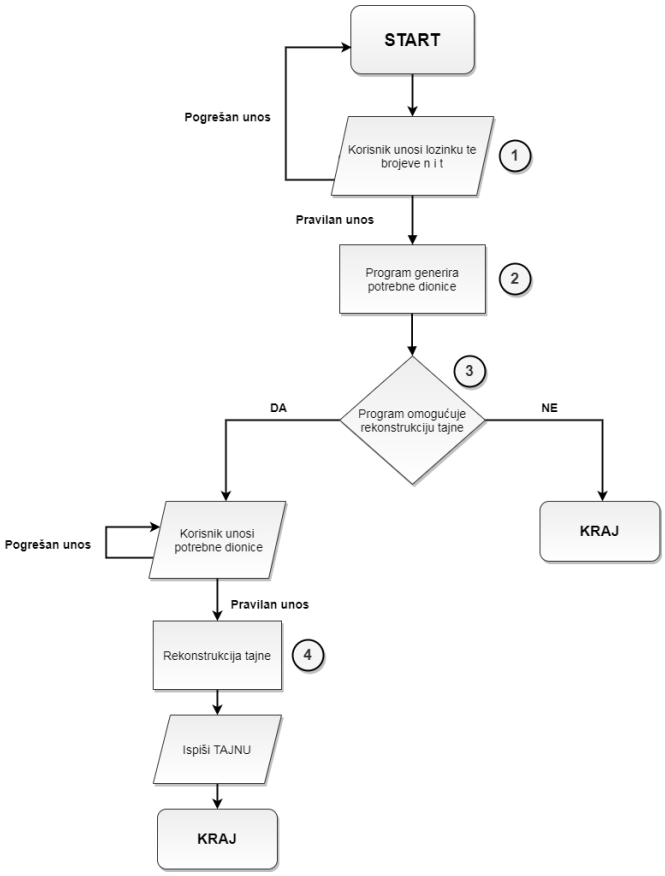
Opišimo kako program radi te koje su modifikacije provedene u Shamirovoj shemi praga. Za početak ćemo, uz pomoć dijagrama toka cijelog programa, opisati osnovne karakteristike te procese koji se izvode kada se program pokrene. Nakon toga ćemo opis popratiti primjerom.

Kada se pokrene Python skripta, od korisnika se traži da unese *lozinku* te brojeve n i t. U koraku **(1)** na Slici 3.1, program provjerava je li unesene vrijednosti (za lozinku, n i t) zadovoljavaju sljedeće uvjete:

- Lozinka mora biti niz znakova, velikih slova engleske abecede i/ili brojeva od 0 - 9, duljine od 4 - 8. Označimo je sa K.
- Ukupni broj dionica n mora biti prirodan broj takav da vrijedi $n+1 \leq p$, gdje je p generirani prost broj čija veličina ovisi o unesenoj lozinci.
- Minimalan broj dionica t mora biti prirodan broj manji ili jednak n.

Duljina i izgled lozinke su ograničeni navedenim uvjetima kako bismo osigurali da brojevi u izračunima ne budu preveliki.

3.1. Opis implementacije



Slika 3.1: Dijagram toka programa

Funkcija *provjeraLozinke()* provjerava ispravnost unesene lozinke te ukoliko nisu zadovoljeni navedeni uvjeti, program će tražiti ponovni unos od korisnika sve dok korisnik ne unese vrijednosti pravilno. Ako je korisnik unio pravilnu lozinku, ta ista lozinka se *maskira* pomoću funkcije *maskirajLozinku()* koja lozinku modificira na način da:

1. Generira tajni pomak (nasumičan broj iz $\{0, 1, 2, \ldots, 9\}$).
2. Svakom znaku u lozinci pridruži odgovarajući ASCII kod.
3. ASCII kodu svakog znaka pridoda tajni pomak te kao rezultat vrati novostvorenu maskiranu lozinku koju ćemo označiti s K_M.

```
def maskirajLozinku(lozinka):
    pomak = random.randint(0,9)
    niz_simbola = split(lozinka)
    rez = []
    for el in niz_simbola:
        temp = ord(el) + pomak
        rez.append(str(temp))
    return [int("".join(rez)),pomak]
```

Kod 3.2: Program za "maskiranje" lozinke

Na temelju generirane maskirane lozinke, funkcija *generirajProsti_p()* generira prosti broj p na način da nađe prvi prosti broj veći od maskirane lozinke. Nakon toga se provjeravaju unesene vrijednosti za n i t. Kao i prije, u slučaju pogrešnog unosa, program ga ponavlja dok unesene vrijednosti nisu ispravne.

U koraku **(2)** program generira n *dionica* oblika (x_i, y_i), $1 \leq i \leq n$. Funkcija *random_Xi()* odabire n različitih ne-nul elemenata x_i, $i = 1, ..., n$ iz polja $\mathbb{Z}_p$, a funkcija *random_Ai()* odabire $t-1$ elemenata a_i, $i = 1, ..., t-1$, iz $\mathbb{Z}_p$. Zatim funkcija *a_Funkcija()* računa vrijednosti $y_i = a(x_i)$, gdje je a polinom iz algoritma za Shamirovu shemu dan s (2.1), odnosno s

$$a(x) = K_M + \sum_{j=1}^{t-1} a_j x^j \pmod{p},$$

gdje je K_M maskirana lozinka te se na sučelju ispišu sve generirane dionice.

```
def a_Funkcija(lozinka,t,x_i,a_i,p):
    rez_yi = []
    for x in x_i: # za svaki x_i
        suma = 0
        # izračunamo sumu svih aj * xj, za j=1,...,t-1
        for i in range(1,t):
            suma += a_i[i-1]*pow(x,i)
        # rezultantnom nizu pridružimo vrijednost a(x_i)
        rez_yi.append((lozinka+suma)%p)
    return rez_yi
```

Kod 3.3: Program za računanje dionica tajne korištenjem tajnog polinoma

Slijedi korak **(3)** u kojem je korisniku omogućena rekonstrukcija tajne. Uko-

liko odluči odustati od rekonstrukcije, program završava, a ako se odluči za rekonstrukciju mora znati minimalno t dionica kako bi proces rekonstrukcije bio uspješan.

Pretpostavimo da se korisnik odlučio za rekonstrukciju lozinke. Kod unosa nepostojeće dionice ili ponovljenog unosa već unesene dionice, program će na to upozoriti te će zahtijevati unos dionica sve dok unos ne bude pravilan.

Osim ovog "ručnog unosa" dionica, implementirana je i funkcija *odaberi_Dionice()* koja odabire t nasumičnih dionica od mogućih n. Rekonstrukcija pomoću navedene funkcije je brža (jer ne trebamo unositi podatke), ali nam ovdje više služi kao alat kojem provjeravamo ispravnosti rekonstrukcije.

Neka je korisnik unio pravilnih t dionica. Slijedi korak **(4)**, odnosno sama rekonstrukcija. Lozinku rekonstruiramo pomoću *Lagrangeove interpolacijske formule* na već opisan način

$$K_M = \left(\sum_{j=1}^{t} y_j \prod_{1 \le k \le t, k \ne j} \frac{x_k}{x_k - x_j} \right) \pmod{p}.$$

Možemo prvo izračunati

$$b_j = \left(\prod_{1 \le k \le t, k \ne j} \frac{x_k}{x_k - x_j} \right) \pmod{p}, \quad \text{za sve } j,\ 1 \le j \le t. \tag{3.1}$$

Za izračun b_j zadužena je funkcija *izracunaj_b()*.

Sada kada imamo sve potrebno, funkcija *rekonstrukcija_Lozinke()* rekonstruira lozinku koristeći

$$K_M = \left(\sum_{j=1}^{t} b_j y_j \right) \pmod{p}. \tag{3.2}$$

Podsjetimo se da smo ovim korakom dobili našu *maskiranu* lozinku pa lozinku još moramo vratiti u njen orginalni format, odnosno izgled K.

To nam radi funkcija *odmaskiraj_Lozinku()* koja uzima vrijednost dobivene maskirane lozinke, podijeli je na elemente duljine 2, oduzme *tajni pomak* dodan na početku te za tako dobivene brojeve (ASCII kodove) pronađe odgovarajući znak.

```
def odmaskiraj_Lozinku(lozinka,tajni_pomak):
    lozinka_str = str(lozinka)
    # podijelimo lozinku na podnizove duljine 2
    lista_slova = [lozinka_str[i:i+2] for i in range(0, len(lozinka_str), 2)]
    kodovi = []
    for el in lista_slova:
        kodovi.append(int(el)-tajni_pomak)
    rez = []
    for el in kodovi:
        rez.append(chr(el))
    return "".join(rez)
```

Kod 3.4: Program za "odmaskiranje" lozinke

Na kraju nam je otkrivena naša početna lozinka K.

Time je opisan način rada Python skripte za implementaciju modificirane Shamirove sheme praga. Pogledajmo sada kako program radi na konkretnom primjeru.

3.1.1 Implementacija kroz primjer

Neka je naša unesena lozinka K = **D1PL0MA**. Želimo ju podijeliti na ukupno $\mathbf{n = 5}$ dionica uz minimalan broj potrebnih dionica za rekonstrukciju $\mathbf{t = 3}$.

1. KONSTRUKCIJA DIONICA

Nakon unosa lozinke *D**1**PL**0**MA*, funkcija *maskirajLozinku()* nasumično izabire cijeli broj iz skupa $\{0, 1, \ldots, 9\}$ te ga pridružuje varijabli *pomak*. Zatim "maskira" lozinku na već opisan način: rastavljanjem na znakove, određivanjem njihovih ASCII kodova te pribrajanjem generiranog pomaka. Za bolji opis

pogledajmo kako se to provede na našem primjeru gdje je generirani *tajni pomak* jednak **4**.

	D	**1**	**P**	**L**	**0**	**M**	**A**
ASCII kod	68	49	80	76	48	77	65
ASCII kod + pomak(4)	72	53	84	80	52	81	69
K_M (maskirana lozinka)	**72538480528169**						

Tablica 3.1: Primjer maskiranja unesene lozinke

Na temelju tako generirane maskirane lozinke, funkcija *generirajProsti_p()* generira prosti broj p na način da nađe prvi prosti broj veći od maskirane lozinke. U našem primjeru generiran je $p =$ **72538480528187** te se na temelju njega provjeravaju uneseni n i t.

Nakon pravilnog unosa ulaznih parametara i generiranog p, funkcija *random_Xi()* odabire $n = 5$ različitih ne-nul elemenata x_i iz $\mathbb{Z}_p$, a funkcija *random_Ai()* odabire $t - 1 = 3 - 1 = 2$ elemenata a_i iz $\mathbb{Z}_p$. U našem slučaju odabrani su

$x_1 = 42931023675932,$ $x_4 = 20023884484441,$ $a_1 = 71881262939352,$

$x_2 = 26717890194823,$ $x_5 = 16077556201937,$ $a_2 = 58628765542159.$

$x_3 = 51870904834393,$

Primijetimo da je ovo slučajan odabir u jednoj provedbi programa te da u ponovnoj provedbi ne bi nužno bili generirani dobiveni brojevi.

Zatim, prateći korake u Shamirovoj shemi praga, pomoću

$$a(x) = K_M + \sum_{j=1}^{t-1} a_j x^j \pmod{p}$$

gdje je $K_M = 72538480528169$ naša maskirana lozinka, funkcija *a_Funkcija()* računa vrijednosti $y_i = a(x_i)$ za $1 \leq i \leq n = 5$.

Na taj način dobili smo dionice:

1. $(x_1, y_1) = (42931023675932, 43794554715864)$;
2. $(x_2, y_2) = (26717890194823, 7764923365371)$;
3. $(x_3, y_3) = (51870904834393, 42063328429627)$;
4. $(x_4, y_4) = (20023884484441, 5062836049069)$;
5. $(x_5, y_5) = (16077556201937, 49603509122046)$.

Nakon što su dionice izračunate, korisnik može i ne mora htjeti rekonstruirati svoju lozinku. Ukoliko želi rekonstruirati lozinku potrebno je da zna minimalno $t = 3$ dionica podjele.

1. REKONSTRUKCIJA LOZINKE

Pretpostavimo da se korisnik odlučio za rekonstrukciju lozinke. U ovom primjeru pokazat ćemo rekonstrukciju lozinke pomoću ručnog unosa dionica, a na kraju rada donosimo primjer kako rekonstrukcija izgleda koristeći funkciju *odaberi_Dionice()*.

Pretpostavimo, dakle, da korisnik unosi potreban broj ispravnih dionica kako bi rekonstruirao svoju lozinku. U protivnom će ga program upozoriti na grešku.
Za naš primjer uzet ćemo prvu, treću i petu dionicu

1. $(x_1, y_1) = (42931023675932, 43794554715864)$
2. $(x_3, y_3) = (51870904834393, 42063328429627)$
3. $(x_5, y_5) = (16077556201937, 49603509122046)$

Redoslijed njihova unosa ne utječe na proces rekonstrukcije.
Lozinku ćemo rekonstruirati pomoću formule (3.2), gdje su b_j-ovi definirani s (3.1). Za odabranih t dionica $(x_{j_1}, y_{j_1}), ..., (x_{j_t}, y_{j_t})$ imamo

3.1. Opis implementacije

$$K_M = \left(\sum_{i=1}^{t} b_{j_i} y_{j_i} \right) \pmod{p}$$

Funkcija *izracunaj_b()* izračuna sve potrebne b_j-ove te ih spremi u listu b.

Primjer kako smo izračunali b_1:

$b_1 = \left(\frac{x_2}{x_2 - x_1} \cdot \frac{x_3}{x_3 - x_1} \right) \mod 72538480528187$

$= \left(\frac{51870904834393}{51870904834393 - 42931023675932} \cdot \frac{16077556201937}{16077556201937 - 42931023675932} \right) \mod 72538480528187$

$= \left(\frac{51870904834393}{8939881158461} \cdot \frac{16077556201937}{-26853467473995} \right) \mod 72538480528187$

$= \left(\frac{833957387720279093050819241}{-240066807910113203991721695} \right) \mod 72538480528187$

$= 48758448489174$

Na isti način dobijemo i $b_3 = 41879840389221$, $b_5 = 54438672177980$.

Nakon izračuna svih potrebnih b_j-ova, za $j = 1, 3, 5$, računamo vrijednost ključa, odnosno naše lozinke

$$K_M = (b_1 y_1 + b_3 y_3 + b_5 y_5) \mod 73548581538317 = 72538480528169$$

Podsjetimo se da smo ovim korakom dobili *maskiranu* lozinku, te je moramo vratiti u njen originalni oblik K.

Proces "odmaskiranja" dobivenog rezultata obavlja funkcija *odmaskiraj_Lozinku()*.

	72538480528169						
podjela na podnizove duljine 2	72	53	84	80	52	81	69
podniz - pomak(4)	68	49	80	76	48	77	65
odgovarajući znak	D	1	P	L	0	M	A
K (originalna lozinka)	**D1PL0MA**						

Tablica 3.2: Primjer "odmaskiranja" lozinke

Kao rezultat dobivamo originalnu lozinku te je time završena rekonstrukcija.

Na idućoj slici donosimo ispis Python skripte gdje se generiraju dionice za

lozinku "5HAM1R" te se nasumičnim odabirom dionica ta ista lozinka ponovno rekonstruira.

```
************************************************************
  S H  A M I R O V A    S H E M A    Z A    L O Z I N K E
************************************************************
Lozinka mora biti niz od velikih slova eng.abecede i/ili brojeva 0-9, duljine 4-8 te ne smije sadržavati razmake.

Unesite Vašu lozinku : 5HAM1R
Unesite na koliko dijelova želite podijeliti Vašu lozinku: 7
Unesite minimalan broj dionica potrebnih za rekonstrukciju lozinke: 4

*********************************************************
MASKIRANA LOZINKA:  618073855790
TAJNI POMAK:  8
GENERIRANI PROSTI BROJ (za Zp):  618073855801
UKUPAN BROJ DIONICA:  7
MINIMALAN BROJ DIONICA POTREBNIH ZA REKONSTRUKCIJU:  4
*********************************************************

Nasumični xi :  [567359881459, 273962579014, 339151608643, 436239212223, 29065806266, 528016435736, 124716018911]
Nasumični ai :  [591050966756, 517845656580, 420785713697]
Dobiveni yi :  [65214346149, 421556829572, 14538194507, 259084562870, 62431178276, 44186792020, 506346678358]
*********************************************************
 DOBIVENE DIONICE
[567359881459, 65214346149]
[273962579014, 421556829572]
[339151608643, 14538194507]
[436239212223, 259084562870]
[29065806266, 62431178276]
[528016435736, 44186792020]
[124716018911, 506346678358]
*********************************************************

Da li želite rekonstruirati lozinku (y/n)? Y


*********************************************************
R E K O N S T R U K C I J A    L O Z I N K E
*********************************************************
Nasumično su odabrane sljedeće dionice:
1 .  [124716018911, 506346678358]
2 .  [567359881459, 65214346149]
3 .  [273962579014, 421556829572]
4 .  [339151608643, 14538194507]

Odabrane su sljedeće dionice za rekonstrukciju tajne
------------------------------------------------------------------------
1 .   [124716018911, 506346678358]
2 .   [567359881459, 65214346149]
3 .   [273962579014, 421556829572]
4 .   [339151608643, 14538194507]

Dobiveni b_j-ovi :  [235912179724, 410201226378, 296745436929, 293288868572]

------------------------------------------------------------------------
Vaša maskirana lozinka je:  618073855790
VAŠA IZVORNA LOZINKA JE:  5HAM1R
------------------------------------------------------------------------
```

Slika 3.5: Primjer rezultata Python skripte za lozinku 5HAM1R uz nasumičan odabir dionica.

Literatura

[1] I. N. Bozkurt, K. Kaya, A. A. Selçuk, A. M. Güloglu, *Threshold Cryptography Based on Blakley Secret Sharing* (2008). Preuzeto s: `https://users.cs.duke.edu/\protect\char126\relaxilker/papers/conference/isc2008.pdf` (listopad, 2020.)

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

[3] A. Endurthi, O. B. Chanu, A. N. Tentu, V. C. Venkaiah, *Reusable Multi-Stage Multi-Secret Sharing Schemes Based on CRT*, Journal of Communications Software and Systems, **11(1)** (2015), 15-24. `https://doi.org/10.24138/jcomss.v11i1.113`

[4] S. Iftene, *General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting*, Electronic Notes in Theoretical Computer Science, **186** (2007), 67-84. `https://doi.org/10.1016/j.entcs.2007.01.065`

[5] M. Iwamoto, *General Construction Methods of Secret Sharing Schemes and Visual Secret Sharing Schemes*, doktorska disertacija, 2003. Preuzeto s: `https://www.iw-lab.jp/users/mitsugu/research/Thesis/Thesis-iwamoto.pdf` (listopad, 2020.)

[6] K. Kaya, A. A. Selcuk, Z. Tezcan, *Threshold Cryptography Based on Asmuth-Bloom Secret Sharing*, Computer and Information Sciences – ISCIS 2006, Lecture Notes in Computer Science, **4263** (2006), 935-942, Springer, Berlin, Heidelberg. https://doi.org/10.1007/11902140_97

[7] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996., *Secret sharing* : 524-528, 538-540

[8] Y. Ning, F. Miao, W. Huang, K. Meng, Y. Xiong, X. Wang., *Constructing Ideal Secret Sharing Schemes Based on Chinese Remainder Theorem*, Advances in Cryptology – ASIACRYPT 2018, Lecture Notes in Computer Science, **11274** (2018), 310-331, Springer, Cham. https://doi.org/10.1007/978-3-030-03332-3_12

[9] D. Pasaila, V. Alexa, S. Iftene, *Cheating Detection And Cheater Identification in CRT-Based Secret Sharing Schemes*, Computing, **9 (2)** (2010), 107-117. Preuzeto s: http://computingonline.net/computing/article/view/702/664 (listopad, 2020.)

[10] M. Quisquater, B. Preneel, J. Vandewalle, *On the Security of the Threshold Scheme Based on the Chinese Remainder Theorem*, Public Key Cryptography, Lecture Notes in Computer Science, **2274** (2002), 199-210, Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45664-3_14

[11] M. Rosulek, *The Joy of Cryptography, Chapter 3. Secret Sharing*, skripta preddiplomskog kolegija. Preuzeto s: https://web.engr.oregonstate.edu/~rosulekm/crypto/chap3.pdf (listopad, 2020.)

[12] K. N. Sandhya Sarma, Hemraj S. Lamkuche and S. Umamaheswari, Secret Sharing Schemes, Research Journal of Information Technology, **5** (2013), 67-72. Dostupno na: `https://scialert.net/fulltext/?doi=rjit.2013.67.72`

[13] A. Shamir. *How to share a secret*, Communications of the ACM **22** (1979), 612-613.

[14] A. Shamsoshoara. *Overview Of Blakleys Secret Sharing Scheme,* ArXiv abs/1901.02802 (2019): n. pag. Preuzeto s: `https://www.researchgate.net/publication/330225718_OVERVIEW_OF_BLAKLEYS_SECRET_SHARING_SCHEME` (listopad, 2020.)

[15] D. R. Stinson, Cryptography Theory and Practice. 3rd edition. Chapman and Hall/CRC, Taylor and Francis Group, 2006. *Secret Sharing Schemes*: 481-514

[16] Secret sharing. Wikipedija: `https://en.wikipedia.org/wiki/Secret_sharing` (listopad, 2020.)

[17] Shamir's Secret Sharing. Wikipedija: `https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing` (listopad, 2020.)

[18] Secret sharing using the Chinese remainder theorem. Wikipedija: `https://en.wikipedia.org/wiki/Secret_sharing_using_the_Chinese_remainder_theorem` (listopad, 2020.)

[19] M. Djukanović, *Interpolacijski polinomi*. Preuzeto s: `https://markosite.files.wordpress.com/2013/12/npm7.pdf` (listopad, 2020.)

[20] Python skripta, *Shamirova_shema_za_lozinke_Josipa_Despotovic.py*.
`https://github.com/JosipaD/Shamirova_shema_praga`

TEMELJNA DOKUMENTACIJSKA KARTICA

PRIRODOSLOVNO–MATEMATIČKI FAKULTET
SVEUČILIŠTA U SPLITU
ODJEL ZA MATEMATIKU

DIPLOMSKI RAD

METODE ZA PODJELU TAJNE

Josipa Despotović

Sažetak:

Metode ili sheme za podjelu tajne su metode za raspodjelu tajne među skupinom sudionika na način da se svakome sudionika dodijeli dio tajne. Izvorna tajna može se rekonstruirati samo kada se kombinira dovoljan broj dijelova tajne. U prvom poglavlju ovog rada dana su osnovna svojstva i navedene različite vrste metoda za podjelu tajne te su dani primjeri njihove primjene u raznim područjima. U drugom dijelu rada su obrađene osnovne metode za podjelu tajne: Shamirova i Blakleyeva shema praga te metode koje koriste Kineski teorem o ostacima, Mignotteova i Ashmut-Bloomova shema praga. Pokazano je da su Shamirova i Asmuth-Bloomova shema savršene, dok druge dvije to nisu. Na samom kraju rada, opisana je implementacija Shamirove sheme praga u svrhu podjele i rekonstrukcije lozinke.

Ključne riječi: *metode za podjelu tajne, (t,n)-shema praga, Shamirova shema praga, Lagrangeov interpolacijski polinom, Blakleyeva shema praga, Kineski teorem o ostacima, savršena metoda*

Podatci o radu: *61 stranica, 9 slika, 3 tablice, 20 literaturnih navoda. Izvornik je na hrvatskom jeziku. Rad je pohranjen u knjižnici Prirodoslovno-matematičkog fakulteta Sveučilišta u Splitu.*

Voditeljica rada: *Prof. dr. sc. Borka Jadrijević*

Članovi povjerenstva:

Prof. dr. sc. Borka Jadrijević

Prof. dr. sc. Anka Golemac

Doc. dr. sc. Marija Bliznac Trebješanin

Povjerenstvo za diplomski rad je prihvatilo ovaj rad u *22. veljače 2021.godine.*

BASIC DOCUMENTATION CARD

FACULTY OF SCIENCE, UNIVERSITY OF SPLIT

DEPARTMENT OF MATHEMATICS

MASTER'S THESIS

SECRET SHARING SCHEMES

Josipa Despotović

Abstract:

Secret sharing schemes are methods of distributing a secret among a group of participants, each of whom is assigned a share of the secret. The secret can only be reconstructed if a sufficient number of shares are combined. In the first chapter of this thesis, we deal with the basic properties of secret sharing schemes. Moreover, we analyzed various secret sharing schemes and classified them based on their characteristics. We also give examples of their application in numerous fields. The second chapter of the thesis deals with the basic secret sharing schemes: Shamir's and Blakley's threshold schemes and the methods that use the Chinese remainder theorem, Mignotte's and Asmuth-Bloom's threshold schemes. It has been shown that Shamir's and Asmuth-Bloom's schemes are perfect, while the other two methods are not. At the very end of the paper, we describe an implementation of Shamir's threshold scheme for sharing and reconstructing the password.

Key words: *secret sharing methods, (t, n)-threshold scheme, Shamir's threshold scheme, Lagrange interpolating polynomial, Blakley's threshold scheme, Chinese remainder theorem, perfect method*

Specifications: *61 pages, 9 images, 3 tables, 20 literature citations. Original language: Croatian. The work is stored in the library of the Faculty of Science, University of Split.*

Mentor: *Professor Borka Jadrijević*

Committee:

Professor Borka Jadrijević

Professor Anka Golemac

Assistant professor Marija Bliznac Trebješanin

This thesis was approved by a Thesis commettee on *February 22, 2021*