UNIVERZITET CRNE GORE

Prirodno-matematički fakultet Podgorica

Jelena Jovanović

Diffie-Hellman protokol i eliptičke krive

SPECIJALISTIČKI RAD

Podgorica, Septembar 2020.

UNIVERZITET CRNE GORE

Prirodno-matematički fakultet Podgorica

Diffie-Hellman protokol i eliptičke krive

SPECIJALISTIČKI RAD

Kriptografija

Mentor: Vladimir Božović

Jelena Jovanović

Matematika i računarske nauke

Podgorica, Septembar 2020.

Apstrakt

Doprinos u razvoju asimetrične kriptografije dali su *Whitfield Diffie* i *Martin Hellman* kada su 1976. godine u svom radu *"New direction in Cryptography"* opisali ideju kriptografije koja se temelji na dva ključa, javnom i tajnom. Potom su napravili konkretan algoritam sigurne razmjene ključeva. Diffie-Hellman protokol, koji nosi ime po svojim tvorcima, zasniva se na kompleksnosti problema diskretnog logaritma. Organizacija IEEE (Institute of Electrical and Electronics Engineers) je predložila standard sa protokolom Diffie-Hellman kao osnovnim algoritmom za razmjenu ključeva, ali postoje još neke poboljšane ideje koje rješavaju probleme kao što je ranjivost na napad sa čovjekom u sredini (eng. man in the middle). Kako bi se spriječio takav napad predlaže se obavljanje autentifikacije prije razmjene ključa. Na Diffie-Hellman protokolu su matematički zasnovani mnogi kriptografski algoritmi. Jedan od poznatih je ElGamal algoritam. S druge strane, postoje algoritmi koji su zasnovani na algebri eliptičkih krivih i konačnih polja. Pomoću njih je određivanje nivoa sigurnosti i postupak razbijanja enkripcije mnogo složeniji u odnosu na odgovarajuće standardne algoritme asimetrične kriptografije. Cilj ovog rada je da se, pored osnovnog značaja Diffie-Hellman protokola, prikaže i njegova primjena u današnjem vremenu.

Abstract

Whitfield Diffie and *Martin Hellman* in 1976. contributed in asymetric cryptography, when they descibed the idea of cryptography based on two keys, public and private, in their paper *"New direction in Cryptography"*. Then they made concrete algorithm for secure key distribution. Diffie-Hellman protocol, which name is by it's creators, is based on the complexity of descrete logarithm problem. The organisation IEEE(Institute of Electrical and Electronics Engineers) suggested a standard with Diffie-Hellman protocol, to be the basic algorithm for key distribution, but there are some more improved ideas that solve problems like it is vulnerability to the man-in-the-middle attack. To prevent the attack, it is suggested to do some authentication before key distribution. There are a lot of cryptographic algorithms that are mathematically based on Diffie-Hellman protocol. One of them is popular ElGamal algorithm. On the other hand, there are algorithms based on algebra of elliptic curves and finite fields. They are very usefull to determine security level and the encryption breaking process which is a lot harder than in some standard algorithms of asymetric cryptography. The aim of this research is to show, not only fundamental importance of Diffie-Hellman protocol, but also it's application nowadays.

Sadržaj

Glava 1

Uvod

Glavni problem koji je pratio komunikaciju kroz cijelu istoriju čovječanstva jeste sigurnost pri razmjeni informacija. Poruke su često putovale nezaštićenim komunikacionim kanalima. Ti kanali su bili fizički putevi, npr. ceste, pruge, telefonske linije, kasnije i računarske mreže itd. Kako bi zaštitili poruke ljudi su ih počeli pretvarati u oblik čitljiv samo osobama kojima su bile namijenjene. To je upravo osnovna ideja nastanka kriptografije kao naučne discipline. Nekada su šifrovane poruke odlučivale o ishodima ratova i bitaka, te u smrt odvele mnoge kraljeve i kraljice. Imale su značajan uticaj na ishod ratova. Tokom vremena mnogo toga se promijenilo, tehnologija je napredovala i potreba za sigurnom komunikacijom postajala je sve veća.

Kriptografija se bavi zaštitom informacija korišćenjem matematičkih metoda. U umreženim računarskim sistemima važno je uspostaviti sigurnost. Milioni ljudi svakodnevno koriste računarske mreže, uključujući Internet, za bankarstvo, kupovinu, slanje poruka i slično. To znači da se svakodnevno Internetom prenose povjerljivi podaci. S obzirom na to da je gotovo nemoguće spriječiti prisluškivanje, pokazalo se korisnim učiniti podatke nerazumljivim neovlašćenim korisnicima. Kao što vidimo kriptografija se primjenjuje u velikoj mjeri i danas, a Diffie-Hellman protokol je jedan od ključnih za njen napredak i prelazak sa simetrične na asimetričnu. Iz tih razloga,

a i zbog interesantnog matematičkog pristupa, sam odabrala ovu temu.

U sledećim poglavljima će biti uvedeni osnovni pojmovi kriptografije, biće riječ o nepraktičnim metodama razmjene ključa u simetričnom kriptosistemu, koji su doveli do nastanka Diffie-Hellman protokola i problemu diskretnog logaritma na kojem se bazira. Analogno tome biće definisan sličan problem ali u skupu tačaka eliptičke krive. Poglavlja o eliptičkim krivama obuhvatiće suštinu i primjenu nekih usavršenih protokola implementiranih na osnovu ECDH (eng. Ellyptic curve Diffie-Hellman).

Glava 2

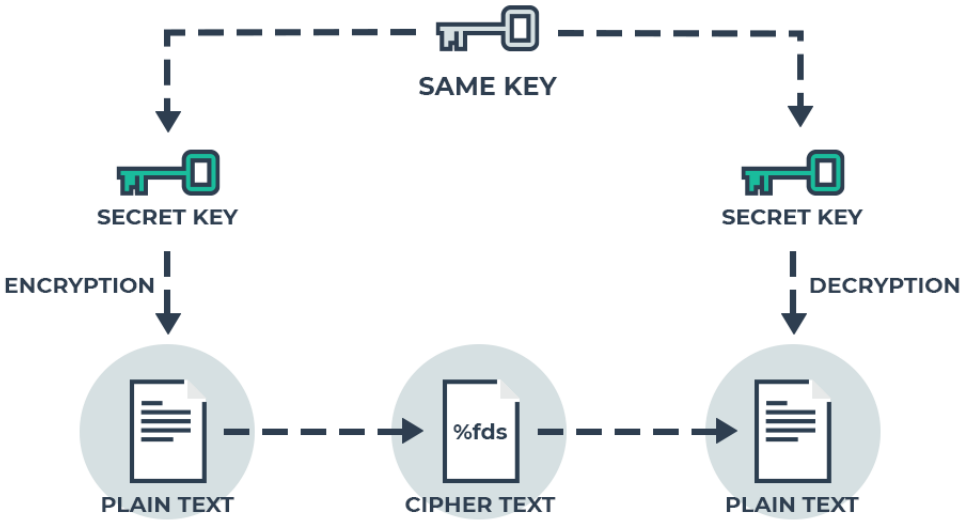
Početne ideje upotrebe ključa u kriptografiji

2.1 Osnovni pojmovi i terminologija

Osnovni zadatak kriptografije je da omogući komunikaciju dvije osobe preko nezaštićenog kanala za komunikaciju tako da treća osoba, kojoj nije namijenjena poruka, ne može razumjeti njihove poruke. Pošiljalac preoblikuje otvoreni ili jasni tekst koristeći unaprijed dogovoreni **ključ**. *Izvorni tekst* se u engleskoj literaturi naziva *plaintext* ili *cleartext*, a postupak transformacije teksta se zove *enkripcija* ili *šifrovanje* (eng. *encryption*). Rezultat je *kriptovan* ili *šifrovan tekst*(eng. *cypher* ili *cyphertext*). Suprotno enkripciji je postupak koji nazivamo *dekripcija* ili *dešifrovanje*. Zbog lakšeg izražavanja uvodimo imena subjekata u komunikaciji i to su: *Alisa, Bob* i *Eva*. Eva je treće lice koje pokušava da ometa komunikaciju između Alise i Boba ili da dođe do sadržaja njihovih poruka iako joj nisu namijenjene, dok su podaci koje razmjenjuju prethodno zaštićeni određenim kriptografskim postupkom. Ovaj komunikativni trougao čini osnovni kriptografski scenario.

Ukoliko Alisa šalje poruku Bobu koristeći **simetrični** kriptosistem, Bob mora

znati ključ kojim je poruka kriptovana, jer će jedino istim tim ključem moći da dekriptuje poruku. Ključ posjeduje samo Alisa, jer je ona kriptovala poruku, tako da ga Bob može jedino od nje dobiti. Prema tome, potrebno je obaviti **razmjenu ključeva**. Ključ u simetričnom kriptosistemu se naziva **tajni** ili **privatni** ključ. Simetričnu kriptografiju često nazivamo *kriptografijom privatnog ključa*. Ovdje je glavni problem način na koji će ga Alisa poslati ili lično predati Bobu. Šema ovog pristupa prikazana je na sledećoj slici.



Slika 2.1: Simetrična kriptografija

2.2 Razmjena ključa

Za nastanak protokola Diffie-Hellman značajnu ulogu igra problem razmjene ključeva. Kriptografe je mučio taj problem jer, kako su šezdesetih godina računari bili sve napredniji i jeftiniji, to su ih kompanije sve više koristile u svrhu komuniciranja kriptovanim porukama. Osnovni problemi kriptografije privatnog ključa su: *razmjena ključa, upravljanje ključevima* i njena *neprimjenljivost u otvorenim sistemima.*

Početna ideja za razmjenu ključa bila je razmjena putem sigurnog kanala koji se može implementirati, npr. koristeći povjerljiv servis za razmjenu poruka. Prosječnoj osobi ova mogućnost nije bila dostupna, dok su vlade, vojska i sigurnosne službe imale način dijeljenja ključa ovom metodom. Bolji način je bio fizički susret prilikom kojeg se može generisati ključ i svakoj strani dati njegova kopija. Problem ovog postupka biće opisan u sledećim primjerima.

Primjer 2.1. *Banka želi klijentu poslati povjerljive podatke putem telefona. Jasno je da postoji mogućnost da neko prisluškuje, pa na taj način neovlašćeno otkriva podatke o klijentu ili banci. Kako bi banka zaštitila te podatke, ona bira ključ i radi enkripciju. Za dekriptovanje poruke, klijent mora imati kopiju programa koji je korišćen za enkripciju, ali i upotrijebljeni ključ. Pitanje je kako banka može obavijestiti klijenta o ključu. Nije izvodljivo da to uradi telefonskim putem, jer je to nesiguran kanal. Očigledan i jedini odgovor je da se taj postupak izvrši lično, što je besmisleno (jer bi se na taj način i poruka mogla prenijeti) i oduzima vrijeme. Manje sigurno, ali praktičnije rješenje je slanje pomoću kurira. Za to su se birali najpouzdaniji zaposlenici u banci. Kako je poslovna mreža rasla, rastao je i broj poslatih poruka, tako da je trebalo dostavljati sve više ključeva. Osim toga, troškovi ovog procesa su postali previsoki. Država je raspolagala novcem i resursima pa je, neko vrijeme, mogla da izađe na kraj sa ovim problemima, dok je to za civilni sektor bilo nerješivo.*

Primjer 2.2. *U drugom svjetskom ratu Njemačka vlada je svakog mjeseca morala dostaviti knjigu dnevnih ključeva svim operaterima Enigme, poznate mašine za enkripciju, koja se koristila tokom rata. Ključeve je redovno trebalo dostavljati vojnim jedinicama, pa čak i nuklearnim podmornicama koje su se nalazile skrivene hiljade kilometara daleko od baze.*

Primjer 2.3. *Na nekom radnom mjestu, direktor bi podijelio ključ sa zaposlenim prvog radnog dana. Iako ovo može biti izvodljivo kada bi samo direktor dijelio ključ sa zaposlenim, problem nastaje kada zaposleni moraju međusobno da dijele ključeve. To je značilo da zaposleni moraju dijeliti novi tajni ključ sa svakim novim zaposlenim. To je problem ako je kompanija velika i ako se nalazi na više lokacija. Djelimično rješenje bi bilo angažovanje nekog kontrolora npr. informatičkog stručnjaka, da uspostavi zajedničke ključeve među zaposlenim. Kada se pojavi novi zaposleni, kontrolor bi mogao generisati n različitih ključeva $k_1, k_2, ..., k_n$, dati ih novom zaposlenom i poslati ključ k_i i-tom zaposlenom enkripcijom ključa k_i, koristeći tajni ključ između kontrolora i tog zaposlenog. Ovaj pristup je kompleksan i ne rješava kompletan problem, jer kontrolor zna sve ključeve koje zaposleni međusobno dijele, pa lako može dekriptovati komunikaciju između njih.*

2.2.1 Skladištenje ključa i sigurnost

Nadovezaćemo se na primjer 2.3. Svaki par zaposlenih dijeli neki tajni ključ. To znači da, ako postoji N zaposlenih, ukupan broj tajnih ključeva je $\binom{N}{2}$. Svaki zaposleni, kako bi mogao komunicirati sa ostalim, morao bi biti vlasnik $N-1$ tajnih ključeva. Činjenica koja još više otežava situaciju je da zaposleni nekada moraju imati i ključeve za sigurnu komunikaciju sa određenim izvorima kao što su serveri, baze podataka i sl. Skladištenje tolikog broja ključeva na sigurnom mjestu pravi veliki logistički problem (ometa se cjelokupan proces poslovanja). Osim toga, računarski sistemi mogu imati viruse i druge zlonamjerne softvere, koji za cilj mogu imati krađu tajnih ključeva. Dakle, skladištenje tajnih ključeva u računarima nije dovoljno dobro rješenje.

Ukoliko je broj ključeva, koji se skladište, mali, za to postoje neke dobre metode. Standardni način je korišćenje *pametnih kartica*, što podrazumijeva zaštitu

dijela hardvera u kojem su skladišteni tajni ključevi. Na pametnoj kartici odvijaju se kriptografski proračuni što osigurava da se tajni ključevi nikada ne nađu na nesigurnim računarima. Memorija pametnih kartica je ograničena pa ne može služiti za veliki broj ključeva.

Dakle, kriptografija privatnim ključem se može koristiti u zatvorenim sistemima, gdje postoji mogućnost razmjene ključa fizičkim kontaktom. Iako postoji u nekim kompanijama, ta mogućnost je otežana i iz navedenih razloga postoje određeni rizici. U nekim sistemima nije nikako moguće sprovesti ovakvu kriptografiju, kao što je primjer kada je neophodna enkripcija putem Internet kupovine, slanje mejla osobi koju ne poznajemo u drugu državu itd. Tako u otvorenim sistemima, gdje nisu mogući stalni fizički susreti i kratkotrajne interakcije, potrebna su neka druga rješenja.

2.2.2 Centar za razmjenu ključa

Kako bi se izbjegli fizički kontakti za razmjenu ključeva, može se angažovati neki posrednik između zaposlenih, a to je spomenuti informatički stručnjak. On može postaviti jedinstveni server koji nazivamo **centar za razmjenu ključa** ili **KDC** (eng. Key Distribution Center). Njegova osnovna funkcija bi se sastojala od nekoliko koraka:

- Svaki zaposleni dijeli ključ sa KDC-om.
- Ukoliko Alisa želi komunicirati sa Bobom, ona šalje KDC-u zahtjev za to.
- KDC bira novi proizvoljni, tajni ključ koji nazivamo sesijski (eng. session key). Kriptuje ga Alisinim ključem i dobijeni rezultat šalje Alisi, zatim ga kriptuje Bobovim ključem i dobijeni rezultat šalje Bobu.
- Kada Alisa i Bob prime sesijski ključ, mogu ga koristiti za sigurnu komunikaciju.

Odmah nakon završetka njihove komunikacije oni moraju uništiti taj ključ, jer za novu komunikaciju uvijek mogu opet kontaktirati server.

Funkcionisanje KDC-a podsjeća na ranije opisanu metodu, gdje je kontrolor postavljao zajedničke ključeve između zaposlenih svaki put kada bi novi zaposleni pristupio kompaniji. Možemo reći da je, tada, kontrolor predstavljao *"offline"* KDC. Jedan od najpoznatijih protokola koji koristi KDC je *Needham-Schroeder*. Kod ovog protokola, malo je drugačiji princip dijeljenja sesijskog ključa u odnosu na klasični. Kada Alisa pristupi KDC-u radi komunikacije sa Bobom, KDC kriptuje sesijski ključ Bobovim ključem i šalje ga Alisi. KDC ne šalje kriptovani sesijski ključ na obije strane, već samo Alisi. Alisa prosleđuje Bobu sesijski ključ kriptovan njenim ključem. Ovaj protokol je praktičan čak i u slučaju kada jedna strana u komunikaciji nije osoba. Može se, npr. umjesto Boba posmatrati zaštićeni disk na nekom serveru, odakle Alisa želi pročitati neke podatke. Na Alisin zahtjev za dozvolu od KDC-a, on joj izdaje kartu i to će biti njen dokument koji će služiti kao dozvola za pristup podacima. Komunikacija Alise sa serverom je zaštićena jer karta sadrži sesijski ključ.

Prednosti i nedostaci

Prednost ovog kratkotrajnog rješenja se ogleda u tome što svaki zaposleni treba skladištiti samo jedan tajni ključ. Tako je moguće sprovesti priču o pametnoj kartici. KDC mora skladištiti veliki broj ključeva, ali se on nalazi na sigurnom mjestu sa najvećom mogućom zaštitom od mrežnih napada. Takođe, za svakog novog zaposlenog potrebno je samo dodijeliti tajni ključ između njega i KDC-a. Ostali ne moraju obnavljati svoje ključeve, a isto to važi i kada zaposleni napušta kompaniju. Ovim rješenjem skladištenja je pojednostavljena razmjena ključa i njime kriptografija privatnog ključa postaje praktična u jednostavnim kompanijama, gdje postoji osoba od povjerenja.

Nedostatak ovog pristupa, koji bi mogao izazvati velike posledice za svakoga u kompaniji, je mogućnost uspješnog napada na KDC. Velika je vjerovatnoća da će osoba, koja ima pristup KDC-u, dekriptovati komunikaciju između zaposlenih. Takođe, onesposobljeni dio sistema zaustavlja kompletan njegov rad. U tom slučaju, nemoguće je ostvarivati sigurnu komunikaciju. Ako bi se KDC podijelio na više podsistema, to bi moglo izazvati čak još veći broj napada, što nije dobro. Još jedan nedostatak se ogleda u tome što su ključevi, koji se dijele sa KDC-om, kratke šifre koje se lako pamte, pa to dodatno narušava sigurnost.

Glava 3

Nastanak Diffie-Hellman protokola

Kao što vidimo, bez obzira na to koliko je kriptografski algoritam bio siguran u teoriji, u praksi je to bilo narušeno zbog problema razmjene ključa. Najveću revoluciju u kriptografiji izazvao je razvoj tehnika za njegovo savladavanje. Whitfield Diffie(rođen 1944.) jedan je od najpoznatijih kriptografa svoje generacije i jedan od osnivača asimetrične kriptografije. Zanimao se za problem razmjene ključa i dio motivacije je dobijao iz vizije umreženog svijeta. 1974.godine su mu se pridružili Martin Hellman i Ralph Merkle. Šezdesetih godina je američko Ministarstvo odbrane(eng. U.S. Department of Defense) osnovalo i finansiralo istraživačku organizaciju: "Agencija za napredne istraživačke projekte"(eng. Advanced Research Project Agency - ARPA). Jedan od najistaknutijih projekata svodio se na pronalazak načina povezivanja vojnih računara na velikoj udaljenosti. Računare su povezali mrežom nazvanom ARPANet iz kojeg je 1982.godine proizašao Internet. Vremenom su pristup Internetu dobili i ljudi koji nisu bili povezani sa državom ili akademskim istraživanjem. Diffie je i ranije pretpostavljao da će i obični ljudi imati lične računare koji će biti povezani telefonskim linijama i da će se tako razmjenjivati različite poruke putem računarske mreže. Smatrao je da, samim tim, ljudi imaju pravo na privatnost svojih poruka. Njihovo kriptovanje je zahtijevalo razmjenu ključa pa je tako odlučio i uspio da nađe pravo i

jednostavno rješenje za to 1976. godine uz pomoć spomenutih kriptografa. Tada je zvanično objavljen protokol za razmjenu tajnog ključa prije korišćenja algoritma za enkripciju.

3.1 Komunikacija bez prethodne razmjene ključa

3.1.1 Upotreba kriptografskih zagonetki

Rješenje o sigurnoj razmjeni ključa je djelimično inspirisano i ranijim razvojima koje je napravio *Ralph Merkle*. Ovo je podrazumijevalo uključivanje jedne strane u stvaranje i slanje određenog broja kriptografskih zagonetki drugoj. Za rješavanje ovih zagonetki bila je potrebna umjerena količina računskih resursa. Primalac bi nasumično odabrao jednu zagonetku, a zatim bi potrošio potrebni napor da je riješi. Nakon što je zagonetka riješena, primaocu se otkrivaju identifikator i ključ sesije. Primalac zatim šalje identifikator nazad izvornom pošiljaocu, što mu omogućava da zna koja je zagonetka riješena. Kako je izvorni pošiljalac stvorio zagonetke, identifikator mu daje do znanja koji je ključ sesije otkrio primalac i dvije strane mogu koristiti ovaj ključ za sigurniju komunikaciju. Ako napadač prisluškuje interakciju, imaće pristup svim zagonetkama, kao i identifikatoru koji primalac šalje nazad originalnom pošiljaocu. Identifikator ne govori napadaču koji se ključ sesije koristi, pa je najbolji pristup za dešifrovanje podataka riješiti sve zagonetke za otkrivanje ispravnog ključa sesije. Budući da će napadač u prosjeku morati riješiti dio zagonetki, za njega će biti puno teže otkriti ključ nego za primaoca. Ovaj pristup pruža veću sigurnost, ali još je daleko od savršenog rješenja. Razmjena ključeva Diffie-Hellman uzela je neke od ovih ideja i učinila ih složenijim, kako bi se stvorila sigurna metoda kriptografije javnog ključa.

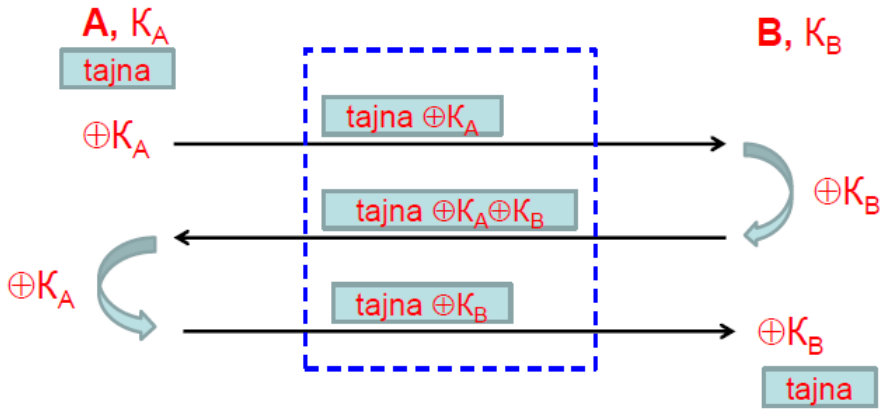
3.1.2 Upotreba metalnih kofera i katanaca

Dvije hiljade godina prije nastanka kriptografije javnog ključa se smatralo da je razmjena ključeva neizbježna. To je bila aksioma kriptografije tj.neporeciva istina. Međutim, uzajamno povjerenje dvije strane i razmjena ključa prije enkripcije bili su ograničavajući kriterijumi za savremene uslove života. Kao što je već rečeno, jedan od nepraktičnih i gotovo nemogućih načina je bila da se učesnici u komunikaciji lično sastaju i tako razmjenjuju ključ. Zbog toga se dolazi i do potpuno suprotnog pristupa koji je podrazumijevao da se ostvari sigurna komunikacija ali **bez prethodne razmjene ključa**. Jedini način za to je bio sledeći:

- Alisa stavlja poruku u metalni kofer koji zaključava katancem A i šalje ga Bobu.
- Nakon prijema, Bob stavlja svoj katanac B i vraća pošiljku(sa dva katanca) Alisi.
- Alisa skida svoj katanac A i vraća pošiljku(na kojoj je sada katanac B) Bobu.
- Bob sada može da otvori pošiljku.

Ipak, ovaj pristup nije mogao funkcionisati ali je Diffie-a i Hellman-a podstakao da krenu u potragu za postupkom koji bi mogao zaobići problem razmjene ključa. Obratili su pažnju na asimetriju u svijetu. Postoje operacije koje je lako izvršiti ali je teško obrnuto. Na primjer, lako je pomnožiti dva broja ali je teško otkriti ih samo iz njihovog proizvoda. Postojanje ovakvih pojava otvorilo je mogućnost konstrukcije sistema u kojem bi enkripcijski i dekripcijski ključevi bili različiti. U tom slučaju bi sigurnost takvog sistema bila očuvana čak i od napadača koji zna enkripcijski ključ. Tako su krenuli sa asimetričnim pristupom kriptografiji 1975.godine, ali su prvi praktični asimetrični kriptosistem, poznat kao RSA, konstruisali tek 1977.godine Rivest, Shamir i Aldeman. Inače se smatra da je koncept asimetrične kriptografije otkriven znatno

ranije, tj. 1969.godine od strane James Ellis-a, dok je radio za britansku vladu. To njegovo otkriće bilo je državna tajna sve do 1997.godine, a pomogli su ga Clifford Cox i Malcolm Williamson.



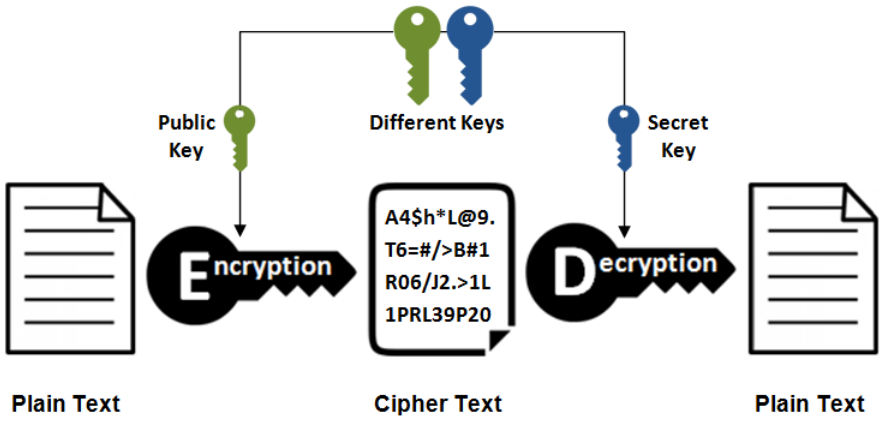
Slika 3.1: Sigurna komunikacija bez razmjene ključa

3.2 Asimetrična kriptografija

U literaturi pojam asimetrične enkripcije se poistovjećuje sa terminom *assymetric-key* ili *public-key* enkripcijom. Često se asimetrična kriptografija naziva *kriptografijom javnog ključa*. Za razliku od simetrične kriptografije, ovdje imamo dva ključa i odatle potiče naziv asimetrična kriptografija. Asimetrija zapravo znači da uloge primaoca i pošiljaoca ne mogu biti zamijenjene kao što je do sada bio slučaj. Ključ koji služi za enkripciju je **javni**, a ključ za dekripciju je **tajni** ili **privatni**. Ako Alisa šalje poruku Bobu, Bob je prethodno formirao javni i tajni ključ. Svako može iskoristiti javni ključ i poslati mu poruku, ali je samo Bob može razumjeti, jer jedini on posjeduje tajni ključ. Važno je da Alisa nikome ne otkriva tajni ključ, pa čak ni Bobu jer se upravo na tom ključu zasniva sigurnost ovog sistema. Jednom javnom ključu odgovara tačno

jedan tajni i obrnuto. Ovdje se zahtijeva tajnost samo jednog od formiranih ključeva.

Posledice ove očigledne razlike između simetrične i asimetrične kriptografije su značajne. Kod simetrične Alisa i Bob moraju dijeliti ključ za enkripciju uz sprječavanje bilo kojoj trećoj strani da ga sazna, dok se kod asimetrične on može slati od jedne do druge strane bez narušavanja sigurnosti.



Slika 3.2: Asimetrična kriptografija

Algoritmi asimetričnog kriptografskog sistema se zasnivaju na određenim svojstvima brojeva. Ključevi za dekripciju i enkripciju su dva različita broja, a izvorni tekst se tretira kao niz prirodnih brojeva.

Diffie i Hellman predstavili su tri posebne asimetrične osnovne funkcije:

- Enkripcija
- Razmjena ključa
- Digitalni potpis

Iako su opisali sve tri funkcije, dali su konstrukciju rješenja samo za razmjenu ključa. Za razliku od razmjene ključa, gdje je potrebno da obije strane budu online,

enkripcija nije interaktivni proces i zbog toga je primjenljivija za neke aplikacije. Na primjer, sigurno slanje mejla zahtijeva enkripciju ali primalac ne mora biti online u istom trenutku kada se mejl šalje.

Upotreba asimetrične kriptografije široko je zastupljena, od HTTPS/SSL protokola koji se koriste na većini web sajtova, do kriptovaluta gdje javni ključevi predstavljaju identitete elektronskih novčanika. Asimetrična kriptografija pomaže razmjeni ključa tako što je moguće objaviti nečiji javni ključ na web stranici ili poslati javni ključ nekome putem mail-a, bez potrebe fizičkog susreta.

3.2.1 Prednosti i nedostaci

Tehnike javnog ključa omogućile su privatnu komunikaciju bez unaprijed dogovorenih informacija. Bitno je primijetiti da sa Alisom može komunicirati više ljudi uz pomoć javnog ključa, koji je ona formirala. Ukoliko Alisa komunicira sa N pošiljaoca, veoma je praktično da ona čuva jedinstveni privatni ključ nego da ga dijeli, skladišti i upravlja sa N različitih ključeva. Svaka strana čuva samo svoj privatni ključ, jer se javni ključevi drugih strana mogu dobiti kad god je to potrebno. Zapravo, koristeći enkripciju javnim ključem, identitet i broj potencijalnih pošiljaoca ne moraju se znati u vrijeme generisanja ključa. Vidimo da se kod asimetričnih kriptosistema par ključeva može koristiti duže vrijeme bez promjene, čak godinama, dok se kod simetričnih ključ mora mijenjati pri svakoj upotrebi.

Broj ključeva u upotrebi je sada mnogo manji. Kod simetričnih kriptosistema je broj neophodnih ključeva u grupi od N ljudi bio $\binom{N}{2} = \frac{N(N-1)}{2}$, jer je svakoj osobi potreban poseban ključ za komunikaciju sa preostalim $N-1$ osobama. Kod asimetričnih kriptosistema taj broj je $2N$, jer je svakoj osobi potreban par ključeva, javni i tajni, za komunikaciju sa preostalim $N-1$ osobama. Evi je dostupan javni ključ, kao i svim ostalim ali ona od njega nema korist.

Takođe, asimetrična kriptografija nam nudi mogućnost potpisa poruke, a samim tim se rješava problem vjerodostojnosti i autentičnosti poruke. Digitalnim potpisom pošiljalac potvrđuje da je on poslao poruku, što ne može kasnije negirati. To su sve prednosti ovog sistema ali najvažnija je ta što nije potrebna prethodna razmjena ključeva. Učesnicima u komunikaciji je obezbijeđena tajna komunikacija čak i ako je pod nečijim nadzorom. Dakle, nije potreban siguran kanal za komunikaciju.

Glavni nedostatak enkripcije javnim ključem je brzina, jer se radi o puno sporijoj metodi enkripcije od principa privatnog ključa. Enkripcija privatnim ključem koristi se u asimetričnoj kriptografiji kako bi se poboljšala efikasnost enkripcije dugačkih poruka. Ključevi asimetričnog kriptosistema znatno su veći od onih kod simetričnih.Iako je moguće, asimetrična kriptografija nije pogodna za enkriptovanje velike količine podataka zbog svoje brzine, za razliku od simetričnih šifara koje su i do 1000 puta brže od asimetričnih. Zbog toga se asimetrična kriptografija koristi u nekim okolnostima kada je količina podataka mala i gdje njene osobine daju najveći doprinos.

Čest scenario je enkripcija podataka simetričnim ključem, a zatim korišćenje algoritama asimetrične kriptografije za enkripciju simetričnog ključa, koji se zajedno sa enkriptovanim podacima šalje primaocu. U stvarnom svijetu kriptografija javnog ključa ne može u potpunosti zamijeniti simetrične kriptosisteme, jer se ona ne koristi za šifrovanje poruka već za šifrovanje ključeva. Zapravo, Alisa i Bob razmjenjuju poruke pomoću simetričnog kriptosistema koristeći ključ koji su razmijenili pomoću asimetričnog kriptosistema. To se naziva **hibridni** kriptosistem.

Glava 4

Problem diskretnog logaritma

4.1 Jednosmjerne (one way) funkcije

Diffie i Hellman su tražili matematičke funkcije za koje redosled dekripcije i enkripcije nije bitan ($f(g(x)) = g(f(x))$). Ovakve funkcije postoje, a većina ih je dvosmjerna, koje je lako izračunati, ali je lako naći i njihovu inverznu vrijednost. Takve funkcije nisu poželjne u kriptografiji. Od interesa su funkcije čiju je inverznu vrijednost teško izračunati. Time se podrazumijeva da je za njeno izračunavanje potrebno ogromno vrijeme uz neograničene resurse, iako su poznati najbolji algoritmi i tehnologija. Njihov značaj se ogleda u tome što poruka enkriptovana jednosmjernom funkcijom ne može da se dekriptuje.

Definicija 4.1. *Za funkciju f kažemo da je jednosmjerna ako je f lako, a f^{-1} teško izračunati. Ako je pritom f^{-1} lako izračunati kada je poznat neki dodatni podatak (tajna vrijednost - zamka), onda f nazivamo jednosmjerna funkcija sa zamkom (prividno jednosmjerna funkcija (eng. trapdoor one way function)).*

Jednosmjerne funkcije ne moraju biti invertibilne. Poznavajući pojam jednosmjerne funkcije sa zamkom, možemo matematički definisati kriptosistem sa javnim ključem.

Definicija 4.2. *Kriptosistem sa javnim ključem sastoji se od familije funkcija za enkripciju e_k i dekripciju d_k sa svojstvima:*

1. *za svaki K važi $d_k = e_k^{-1}$*

2. *za svaki K je e_k javna, ali je d_k poznata samo osobi K*

3. *za svaki K je e_k jednosmjerna funkcija sa zamkom.*

Tada funkciju e_k nazivamo javnim ključem, a d_k tajnim ili privatnim ključem.

Strogo matematički gledano nije dokazano da postoje jednosmjerne funkcije i jednosmjerne funkcije sa zamkom. Uprkos tome, postoje dvije funkcije koje se smatraju kandidatima za funkcije sa pomenutim svojstvima:

- diskretni eksponent, čija je inverzna funkcija diskretni logaritam,
- proizvod cijelih brojeva, čija je inverzna funkcija faktorizacija dobijenog broja.

4.2 Ciklična multiplikativna grupa

Definicija 4.3. *Neka je G neprazan skup i $* : G \times G \to G$ preslikavanje sa svojstvima:*

1. $x * y \in G \quad \forall x, y \in G$ *(zatvorenost)*

2. $(x * y) * z = x * (y * z) \quad \forall x, y, z \in G$ *(asocijativnost)*

3. $\exists e \in G : e * x = x * e = x \quad \forall x \in G$ *(neutralni element)*

4. $\forall x \in G \quad \exists x^{-1} \in G : x * x^{-1} = x^{-1} = e$ *(inverzni element)*

Tada se $(G, *)$ zove grupa.

Ako dodamo svojstvo $x * y = y * x \quad \forall x, y \in G$, onda je $(G, *)$ komutativna grupa ili Abelova grupa.

Definicija 4.4. *Za grupu G kažemo da je ciklična ako je generisana jednim elementom, tj. ako postoji element $g \in G$ tako da za svako $h \in G$ važi $h = \underbrace{g * g * \ldots * g}_{k}$ što kraće zapisujemo kao: $\exists g \in G : G =< g >$. Tada element g nazivamo generatorom grupe G.*

Ciklična grupa koja se često koristi u kriptografiji je multiplikativna grupa $\mathbb{Z}_p^*$ svih ostataka modulo p, različitih od 0, gdje je p dovoljno velik prost broj.
Generator grupe $\mathbb{Z}_p^*$ naziva se *primitivni korijen* modulo p. Broj $g \in \{1, 2, \ldots, p-1\}$ je primitivni korijen modulo p, ako je g^{p-1} najmanji stepen broja g, koji daje ostatak 1, pri dijeljenju sa p.
Za grupu G kažemo da je *konačna* ili *beskonačna* u zavisnosti od toga da li skup G ima konačno ili beskonačno elemenata. Kardinalni broj skupa G nazivamo *red* grupe i označavamo sa $|G|$.

4.2.1 DLOG

Neka je G konačna Abelova grupa. Kako bi bila prikladna za primjenu u kriptografiji javnog ključa, grupa bi trebala imati svojstvo da su operacije množenja i stepenovanja u njoj jednostavne, dok bi logaritmovanje, kao inverzna operacija operacije stepenovanja, bilo vrlo teško. Dakle, glavno pitanje je koliko je težak problem diskretnog logaritma u grupi G.

Definicija 4.5. *Neka je $(G, *)$ konačna grupa i $H = \{g^i : i \geq 0\}$ podgrupa grupe G, generisana elementom $g \in G$ i neka je $h \in H$. **Problem diskretnog logaritma** je traženje broja x, $0 \leq x \leq p-1$ takav da je:*

$$h = g^x = \underbrace{g * g * \ldots * g}_{x}.$$

Broj x se naziva diskretni logaritam i označava sa $log_g h$.

Primjer 4.1. *Posmatrajmo grupu $\mathbb{Z}_p^*$, za $p = 11$ tj. $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Generator te grupe je $g = 7$, što možemo lako provjeriti: $7^1 = 7, 7^2 = 5, 7^3 = 2, 7^4 = 3, 7^5 = 10, 7^6 = 4, 7^7 = 6, 7^8 = 9, 7^9 = 8, 7^{10} = 1$. Tada je diskretni logaritam od, npr. broja 4 jednak 3, tj. $log_7 3 = 4$.*

Ovo direktno traženje diskretnog logaritma nije praktično za velike brojeve p i h.

Napomena: Diskretni logaritam u grupi $\mathbb{Z}_p^*$ nije jedinstven, jer se računa po modulu.

Diskretno stepenovanje u grupi je brzo, obavlja se samo $O(logx)$ operacija nad grupom. Mnogo je teže izračunati diskretni logaritam. Sve metode za to u cikličnim grupama zahtijevaju eksponencijalno vrijeme računanja. Za najbržu metodu potrebno je $O(\sqrt{p})$ operacija. Ovaj problem diskretnog logaritma bio je matematička zagonetka sve dok ga Diffie i Hellman nisu iskoristili kao temelj svog protokola.

Algoritmi za rješavanje

Svi algoritmi za rješavanje problema diskretnog logaritma se mogu klasifikovati u tri grupe:

1. Algoritmi koji rade u proizvoljnim grupama, tj. koji ne koriste nijedno specifično svojstvo grupe. To su metod grube sile (eng. brute force), Šanksov algoritam, Polard-ro..

2. Algoritmi koji rade u grupama glatkog reda, tj. grupama čiji red nema velike proste faktore. Npr. Polig-Helman algoritam.

3. Algoritmi koji koriste metode koji predstavljaju elemente grupe kao proizvod elemenata iz relativno malih skupova, tkzv. faktorskih baza. Predstavnici ove

grupe algoritama su algoritmi koji su varijacije indeks kalkulus (eng. index calculus) metode.

Glava 5

Diffie-Hellman protokol

Postupak razmjene podataka preko nesigurnog komunikacionog kanala sastoji se iz sledećih koraka:

1. Odabere se veliki prost broj p i generator g iz grupe $\mathbb{Z}_p^*$ i objave se kao javni.

2. Alisa izabere proizvoljan broj $a \in \{1, 2, \ldots, p-1\}$, računa vrijednost $A = g^a \pmod p$ i rezultat pošalje Bobu.

3. Bob izabere slučajan broj $b \in \{1, 2, \ldots, p-1\}$, računa vrijednost $B = g^b \pmod p$ i rezultat pošalje Alisi.

4. Oboje računaju $g^{ab} \pmod p$, tj. Alisa računa $B^a = (g^b \pmod p))^a = g^{ab} \pmod p$, a Bob računa $A^b = (g^a \pmod p))^b = g^{ab} \pmod p$. Rezultat koriste kao tajni(privatni) ključ za dalju komunikaciju.

Definicija 5.1. *Neka je p prost broj i g cijeli broj.* ***Diffie-Hellman problem*** *je problem računanja* $g^{ab} \pmod p$*, ukoliko su poznate vrijednosti* $g^a \pmod p$ *i* $g^b \pmod p$*.*

Javni podaci su generator g, prost broj p, $A = g^a \pmod p$, $B = g^b \pmod p$. Evin cilj je da riješi Diffie-Hellman problem (definicija 5.1), ali ona nalazi na problem diskretnog logaritma (definicija 4.5). Vjeruje se da su ova dva problema (DHP i

DLP) u većini grupa, koje se koriste u kriptografiji, ekvivalentni u smislu da postoje polinomijalni algoritmi koji jedan problem svode na drugi.

Ovaj postupak je doveo do odgovarajućih ključeva jer Alisa zna a i g^b, a Bob zna b i g^a i oboje računaju g^{ab}. Suština ovog postupka je da Alisa i Bob završavaju sa istim rezultatom, bez potrebe da cijelu zajedničku tajnu šalju preko komunikacionog kanala. Ovakva struktura razmjene ključeva čini ovaj protokol vrlo efikasnim. Omogućena je komunikacija dvije strane preko potencijalno opasne veze i formiranje zajedničke tajne, koja može služiti za izradu ključeva za buduće komunikacije.

Primjer 5.1. *Neka je* $p = 9967$ *(p je prost broj),* $g = 3$ *(primitivni korijen modulo 9967). Alisa bira broj 34 i računa:*

$$3^{34} \equiv 6366 \pmod{9967}.$$

Bobu šalje 6366. On bira, npr. 37 i dobija:

$$3^{37} \equiv 2443 \pmod{9967},$$

i šalje 2443 Alisi.

Alisa zatim uzima broj, koji joj je poslao Bob i stepenuje ga svojim tajnim brojem. Dobija:

$$k = 2443^{34} = 7782 \pmod{9967}.$$

Analogni postupak sprovodi Bob i dobija:

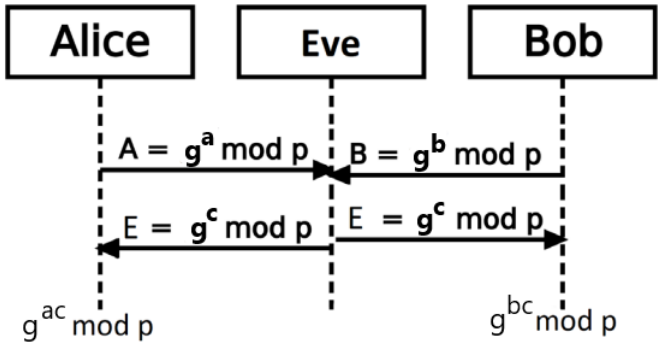
$$6366^{37} \equiv 7782 \pmod{9967}.$$

Napomenimo da je uz date $p = 9967$ *i* $g = 3$ *i uz poznati broj 6366 svejedno teško*

pronaći x, takav da je $3^x \equiv 6366 \pmod{9967}$. Takav x je upravo diskretni logaritam od 6366 po bazi 3 modulo 9967.

5.1 Woman in the middle attack

Bez obzira na veličinu modula p, Diffie-Hellman ima osjetljivost na jedan napad koji ne zavisi od izabranih parametara. To je aktivni napad trećeg lica, poznat kao **woman(man)-in-the-middle** napad. Ovakav napad podrazumijeva da Eva, kao napadač, presrijeće poruke Alise i Boba, mijenja ih i šalje svoje vlastite.



Slika 5.1: Woman-in-the-middle napad

Ovdje je Eva presrela Alisinu i Bobovu poruku, pa je svakome od njih proslijedila generator g stepenovan vlastitim privatnim ključem c. Alisa sada misli da je zajednički tajni ključ $g^{ac} \pmod{p}$, a Bob misli da je zajednički tajni ključ $g^{bc} \pmod{p}$. Kako je Eva presrela njihove poruke i zna vrijednosti A i B, još samo treba izračunati zajedničke tajne ključeve za komunikaciju sa Alisom i Bobom, tj. A^c i B^c respektivno. Eva je sada posrednik u njihovoj komunikaciji i može modifikovati poruke kako ona želi, pa čak i da oni ne znaju da je ona posrednik.

Slaba tačka koju Eva koristi je nemogućnost autentifikacije strana koje razmjenjuju ključeve. Iz tog razloga, u praksi se razmjena ključeva Diffie-Hellman rijetko

koristi sama. Uglavnom se sprovodi zajedno sa nekim sredstvima autentifikacije. To često uključuje korišćenje digitalnih sertifikata i algoritma javnog ključa, poput RSA, za provjeru identiteta obije strane. U rješavanju ovog problema koristi se, već spomenuta, funkcija kriptografije javnog ključa, a to je digitalni potpis. U sklopu ovog rada dovoljno je objasniti osnovnu ideju ove funkcije.

Ideja je sledeća: Alisa i Bob posjeduju svoje parove ključeva (privatni i javni) i sertifikat za javni ključ. Alisa stavlja digitalni potpis na poruke i šalje Bobu neku vrijednost zajedno sa svojim digitalnim potpisom i sertifikatom javnog ključa. Bob učini slično sa svojim vrijednostima. Sada, čak i u slučaju da napadač može presretati poruke između Alise i Boba, on ne može lažirati digitalni potpis bez Alisinog i Bobovog privatnog ključa. Prema tome, ovakav protokol je otporan na woman-in-the-middle napad.

5.2 Tipovi ključa i odabir parametara

Diffie-Hellman protokol se može postaviti tako da se poboljša otpornost na napade grubom silom(eng. brute force), odnosno izračunavanje diskretnog logaritma. Postoje 2 načina upotrebe Diffie-Hellman protokola, u zavisnosti od toga koriste li se odabrane vrijednosti p i g samo jednom u komunikaciji ili više puta. Ključ koji se koristi više puta sa istim p i g naziva se *statični* ključ. Upotreba statičnog ključa je brza i ne pomaže napadaču u statističkoj analizi odabira ključa, odnosno pogađanju bitova ključa. Ukoliko se za svaku poruku koja se šalje koristi drugi ključ, takav se ključ naziva *privremeni*. Prednost privremenog ključa jeste da se može odbaciti ili trajno obrisati, tako da čak i u slučaju da napadač neovlašćeno preuzme nadzor nad računarem na kojem misli da se nalazi ključ, on neće uspjeti otkriti razmijenjeni

ključ. Osim toga, pošiljalac i primalac mogu kombinovati upotrebu statičnog i privremenog ključa tokom razmjene tajnog ključa Diffie-Hellman protokolom. Na primjer, pošiljalac može koristiti privremeni, a primalac statični.

Osim odabira statičnog i privremenog ključa, korisnici moraju paziti pri odabiru veličine broja p i veličine privatnog ključa. Zavisno od potrebnog stepena zaštite komunikacije, potrebno je odabrati broj p i privatni ključ veće dužine (za broj p se smatra da treba da bude dužine minimum 1024 bita). Broj g može biti relativno mali kao npr. 2, ali mora biti iz grupe $\mathbb{Z}_p^*$.

Glava 6

Eliptičke krive

Algebarske krive predstavljaju skup tačaka u ravni koje se mogu definisati algebarskim izrazom: $f(x, y) = 0$. Eliptičke krive predstavljaju familiju *glatkih* algebarskih krivih, pa je njihov prvi izvod definisan u svakoj tački domena krive. Potrebno je naglasiti da eliptičke krive nemaju nikakve veze sa elipsama ili drugim konusnim presjecima. Konusni presjeci su algebarske krive drugog reda, a eliptičke krive su algebarske krive trećeg reda. Red krive je najveći stepen agebarskog izraza koji je definiše. Algebarske krive trećeg reda se mogu javiti u različitim oblicima i definišu se nad algebarskom strukturom koju nazivamo *polje*.

6.1 Konačna polja

Konačna polja su polja sa konačnim brojem elemenata i nazivaju se još i Galoisovim poljima (Evariste Galois,1811-1832).

Eliptičke krive koje se koriste u kriptografiji definisane su sa 2 tipa konačnih polja: $\mathbb{F}_p$ i $\mathbb{F}_{2^m}$. Za opšti slučaj koristimo oznaku $\mathbb{F}_q$, gdje je $q = p$ ili $q = 2^m$. Za definiciju polja biće neophodno poznavanje svojstva distributivnosti.

Definicija 6.1. *Neka je K skup na kojem su definisane operacije "+" i "*" na*

određeni način. Ako važi $\forall a, b, c \in K : a * (b + c) = (a * b) + (a * c) \in K$*, onda ove operacije zadovoljavaju svojstvo distributivnosti.*

6.1.1 Konačno polje $\mathbb{F}_p$

Konačno polje $\mathbb{F}_p$ sadrži p elemenata. Iako postoji jedinstveno konačno polje $\mathbb{F}_p$ za svako p, na više načina se mogu predstaviti njegovi elementi. Predstavljamo ih kao skup cijelih brojeva:

$$\{0, 1 \ldots, q-1\},$$

sa sabiranjem i množenjem definisanim na sledeći način:

- Sabiranje po modulu p: Ako su $a, b \in \mathbb{F}_p$, onda $a + b = r \in \mathbb{F}_p$, gdje je $r \in \{0, 1, \ldots, p-1\}$ ostatak pri dijeljenju $a+b$ sa p. Neutralni element za sabiranje je $0 \in \mathbb{F}_p$. Suprotni element elementa $a \in \mathbb{F}_p$ je $-a \in \mathbb{F}_p$ i on predstavlja jedinstveno rješenje jednačine $a + x \equiv 0 \pmod{p}$.

- Množenje po modulu p: Ako su $a, b \in \mathbb{F}_p$, tada je $ab = s \in \mathbb{F}_p$, gdje je $s \in \{0, 1, \ldots, p-1\}$ ostatak pri dijeljenju ab sa p. Neutralni element za množenje je $1 \in \mathbb{F}_p$. Suprotni element elementa $a, a \neq 0$ je $a^{-1} \in \mathbb{F}_p$ i on predstavlja jedinstveno rješenje jednačine $ax \equiv 1 \pmod{p}$.

Ako ove dvije operacije, uz navedeno, zadovoljavaju i svojstvo zatvorenosti, asocijativnosti, komutativnosti (definicija 4.3) i distributivnosti (definicija 6.1) za $K = \mathbb{F}_p$, onda je $\mathbb{F}_p$ sa opisanim operacijama polje i to sa konačnim brojem elemenata.

6.1.2 Konačno polje $\mathbb{F}_{2^m}$

Posmatrali smo polja $K = \mathbb{F}_q$, gdje je $q = p$ prost broj ili $q = p^m$, za neki prirodan broj m. Ukoliko je $q = p^m$, onda postoji (do na izomorfizam) jedinstveno polje $\mathbb{F}_q$

čija je jedna od realizacija $\mathbb{Z}_p[x]/(f(x))$, gdje je $f(x)$ nerazloživ polinom (ne može se zapisati kao proizvod polinoma stepena bar 1). Elementi ovog polja su polinomi nad $\mathbb{Z}_p$ stepena manjeg ili jednakog od $m-1$, dok se sabiranje i množenje nasleđuju iz $\mathbb{Z}_p[x]$, s tim što se, nakon množenja računa ostatak pri dijeljenju dobijenog polinoma sa polinomom $f(x)$. Da bi operacije u polju $\mathbb{F}_q$, neophodne za računanje sa tačkama na eliptičkoj krivoj nad ovim poljem, bile što jednostavnije, treba odabrati pogodan nerazloživ polinom $f(x)$. Pokazuje se da najbolje mogućnosti pružaju polinomi sa manje nenultih koeficijenata.

Konačno polje $\mathbb{F}_{2^m}$ je polje koje sadrži 2^m elemenata. Iako postoji jedinstveno konačno polje $\mathbb{F}_{2^m}$, za svaki 2^m, $m \geq 1$, na više načina se mogu predstaviti njegovi elementi. Predstavljamo ih kao skup binarnih polinoma stepena $m-1$ ili manje:

$$\{a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots + a_1x + a_0 : a_i \in \{0,1\}\},$$

sa sabiranjem i množenjem definisanim u odnosu na nerazloživ binarni polinom $f(x)$ stepena m na sledeći način:

- Sabiranje: Ako je $a = a_{m-1}x^{m-1} + \ldots + a_0$,$b = b_{m-1}x^{m-1} + \ldots + b_0 \in \mathbb{F}_{2^m}$, onda je $a + b = r$, gdje je $r = r_{m-1}x^{m-1} + \ldots + r_0$ i $r_i \equiv a_i + b_i \pmod 2$. Neutralni element za sabiranje je polinom $0 \in \mathbb{F}_{2^m}$. Suprotni element elementa $a \in \mathbb{F}_{2^m}$ je $-a \in \mathbb{F}_{2^m}$ i on predstavlja jedinstveno rješenje jednačine $a + x = 0 \in \mathbb{F}_{2^m}$. Primijetimo da je $-a = a$, za sve $a \in \mathbb{F}_{2^m}$.

- Množenje: Ako je $a = a_{m-1}x^{m-1} + \ldots + a_0$,$b = b_{m-1}x^{m-1} + \ldots + b_0 \in \mathbb{F}_{2^m}$, onda je $ab = s \in \mathbb{F}_{2^m}$, gdje je $s = s_{m-1}x^{m-1} + \ldots + s_0$ ostatak pri dijeljenju polinoma ab sa $f(x)$, za sve koeficijente redom po modulu 2. Neutralni element za množenje je polinom $1 \in \mathbb{F}_{2^m}$. Suprotni element elementa $a \in \mathbb{F}_{2^m}, a \neq 0$ je $a^{-1} \in \mathbb{F}_{2^m}$ i on predstavlja jedinstveno rješenje jednačine $ax = 1$ u $\mathbb{F}_{2^m}$.

Ako ove dvije operacije, uz navedeno, zadovoljavaju i svojstvo zatvorenosti, asocijativnosti, komutativnosti (definicija 4.3) i distributivnosti(definicija 6.1) za $K = \mathbb{F}_{2^m}$, onda je $\mathbb{F}_{2^m}$ sa opisanim operacijama polje i to sa konačnim brojem elemenata.

6.2 Opšti slučaj eliptičke krive nad poljem K

Definicija 6.2. *Neka je E eliptička kriva nad poljem $K = \mathbb{F}_q$, $q = p^m$. Definišemo njen oblik na sledeći način: ako je $p > 3$, tada je E oblika $y^2 = x^3 + ax + b$. Ako je $p = 3$, tada E ima oblik $y^2 = x^3 + ax^2 + bx + c$. U ova dva slučaja polinomi sa desne strane nemaju višestrukih korijena. Za $p = 2$, može imati jedan od 2 oblika: $y^2 + cy = x^3 + ax + b$ ili $y^2 + xy = x^3 + ax^2 + b$. Ovdje polinomi sa desne strane mogu imati višestruke korijene.*

Eliptičkoj krivoj se može dodati tačka koja se nalazi u beskonačnosti, odnosno čije su koordinate (∞, ∞) i tada se može formirati skup $E(K)$, koji pored tačaka eliptičke krive, sadrži i tačku u beskonačnosti.

Uslov da polinomi sa desne strane jednakosti nemaju višestrukih korijena ekvivalentan je uslovu da je diskriminanta

$$\Delta = -4a^3 - 27b^2 \neq 0.$$

Nije teško primijetiti da, ako su x_1, x_2, x_3 nule polinoma $f(x)$, onda je

$$D = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2.$$

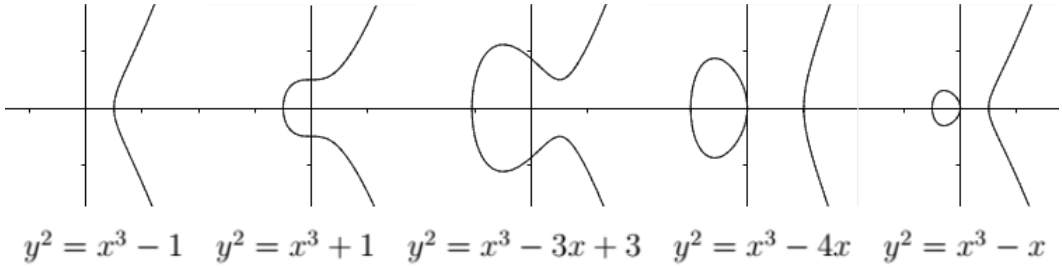
Algebarske krive trećeg stepena se mogu javiti u različitim oblicima, a opšti oblik

jednačine eliptičke krive nad bilo kojim poljem definiše se kao

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$$

i nazivamo ga *Wierstrassova forma*. Za koeficijente važi $a_1, a_2, a_3, a_4, a_5 \in K$. U slučaju ove opšte jednačine, umjesto uslova o različitim korijenima, imamo uslov da su sve tačke na krivoj nesingularne. To znači da je u svakoj tački barem jedan od parcijalnih izvoda različit od 0.

Sada uzmimo da je $K = \mathbb{R}$ polje realnih brojeva. Eliptičku krivu $E(\mathbb{R})$ (bez tačke u beskonačnosti) možemo prikazati kao podskup u ravni. U zavisnosti od parametara a i b, grafik eliptičkih krivih može imati različite oblike, kao npr. na sledećoj slici.



Slika 6.1: Karakteristični oblici eliptičkih krivih, $K = \mathbb{R}$

Neal Kobiltz i *Victor Saul Miller* opisuju matematičke osnove kriptografije eliptičkih krivih (eng. Ellyptic curve cryptography - ECC) kao skup pravila za operacije u konačnim poljima nad kojima se definišu eliptičke krive kao geometrijska mjesta tačaka sa određenim algebarskim svojstvima. Uzima se prost broj $q > 3$ i skup eliptičkih krivih E nad poljem F_q. Ovako definisanom skupu $E(F_q)$ treba pridružiti posebno definisanu operaciju sabiranja kako bi se formirala grupa $E(F_q)$, pogodna za primjenu u kriptografiji eliptičkih krivih.

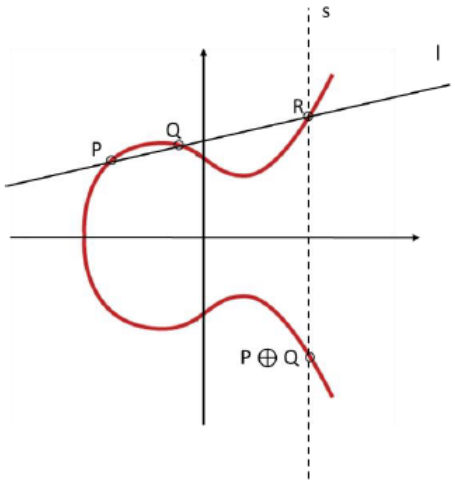
6.2.1 Operacije nad skupom E(K)

Sabiranje dvije različite tačke eliptičke krive

Posmatrajmo dvije različite tačke $P(x_1, y_1)$ i $Q(x_2, y_2)$ iz skupa $E(K)$ (definicija 6.2). Poznato je da se kroz dvije tačke u ravni može povući tačno jedna prava. Postavimo pravu l tako da sadrži te dvije tačke. Očigledno je da je prava l sječica grafika eliptičke krive. Koeficijent prave l može se računati kao

$$k = \operatorname{tg} \alpha = \frac{y_2 - y_1}{x_2 - x_1}$$

. U opštem slučaju, prava l će presijecati grafik eliptičke krive u još jednoj tački. Označimo tu tačku sa R. Sada, postavljamo pravu s, tako da ona sadrži tačku R i da je paralelna y osi, pri čemu je istovremeno normalna na x osu. Presjek prave s i grafika eliptičke krive označimo sa $-R$. Očigledno je ova tačka simetrična sa tačkom R u odnosu na x osu. Na ovaj način definisano je sabiranje tačaka eliptičke krive, odnosno elemenata skupa $E(K)$. Tačka $-R$ predstavlja zbir tačaka P i Q i takođe se nalazi na grafiku eliptičke krive ($R \in E(K)$). Iz navedenog se može zaključiti da je skup $E(K)$ zatvoren u odnosu na sabiranje. Zbir dva elementa $P, Q \in E(K)$ zapisuje se kao $P \oplus Q$ ili $P + Q$.



Slika 6.2: Grafička interpretacija sabiranja dvije različite tačke eliptičke krive

Sabiranje tačke eliptičke krive sa samom sobom

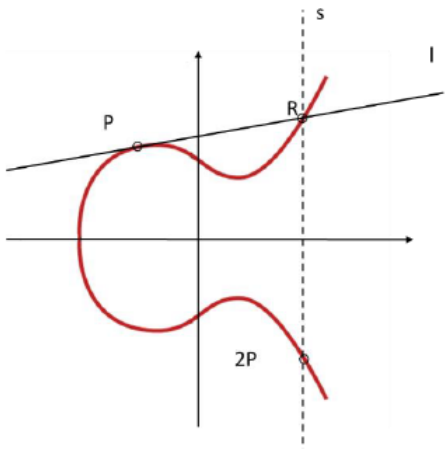
Sabiranje tačke eliptičke krive sa samom sobom sprovodi se malo drugačije, jer kroz jednu tačku u ravni prolazi beskonačno mnogo pravih. U ovom slučaju postavljamo tangentu l u tački P na eliptičku krivu. U izrazu

$$k = \operatorname{tg} \alpha = \frac{y_2 - y_1}{x_2 - x_1}$$

pustimo da x_2 teži x_1. Tada tačka Q teži tački P duž grafike eliptičke krive. Dobijamo da je koeficijent pravca tangente eliptičke krive u tački P

$$k_t = \lim_{x_2 \to x_1} \frac{y_2 - y_1}{x_2 - x_1}.$$

Sada, uočimo tačku presjeka tangente l sa eliptičkom krivom i označimo je sa R. Za tačke P i R sprovodimo isti postupak kao kod sabiranja dvije različite tačke i dobijamo tačku sa grafika eliptičke krive.



Slika 6.3: Grafička interpretacija sabiranja tačke eliptičke krive sa samom sobom

Višestruko sabiranje tačke eliptičke krive

Za tačke eliptičke krive moguće je višestruko sabiranje, tj. n-tostruko sabiranje tačke P sa samom sobom i označava se sa nP. Iako je moguće računati n-tostruku vrijednost tačke kao uzastopno sabiranje tačke:

$$nP = \underbrace{P + P + P + \ldots + P}_{n} = 2P + \underbrace{P + P + \ldots + P}_{n-2},$$

što zahtijeva n sabiranja, efikasniji pristup je korišćenje što više izračunatih dupliranih sabiraka.

Npr, za trostruko sabiranje imamo $3P = P + P + P = 2P + P$, pri čemu je prvo sabiranje dupliranje tačke P, a drugo je regularno sabiranje dvije različite tačke ($2P$ i P). Za četvorostruko sabiranje imamo $4P = P + P + P + P = 2P + 2P = 2(2P)$, pri čemu je jedno sabiranje upotrijebljeno za dupliranje tačke P i jedno sabiranje za $2P$ i $2P$.

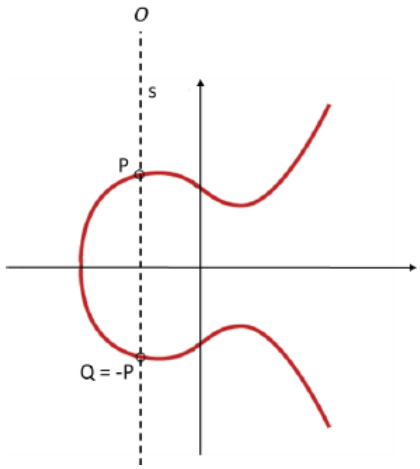
U opštem slučaju:

$$nP = \begin{cases} 2P + \ldots + 2P = 2(\frac{n}{2}P) & \text{ako je } n \text{ paran broj} \\ 2P + \ldots + 2P + P = 2(n-1)P + P & \text{ako je } n \text{ neparan broj} \end{cases}$$

pri čemu je potrebno $O(\log n)$ množenja.

Određivanje suprotnog elementa

Ako je tačka P tačka sa grafika eliptičke krive i s prava koja je paralelna sa y osom i prolazi kroz tačku P. Presjek prave s i eliptičke krive je tačka $-P$, koja je simetrična tački P u odnosu na x osu. Kako bismo izvršili sabiranje $P \oplus -P$ potrebna nam je i treća tačka presjeka sa grafikom eliptičke krive, koja u ovom slučaju ne postoji. Koristimo tačku $O \in E(K)$, koja se nalazi u beskonačnosti. Definiše se pravilo da se tačka O može smatrati tačkom bilo koje prave paralelne sa y osom.



Slika 6.4: Grafička interpretacija određivanja suprotnog elementa u skupu E(K)

6.2.2 Algebra eliptičkih krivih

Pored grafičke interpretacije potrebno je definisati i algebarsku interpretaciju operacija nad skupom E. Operacija sabiranja elemenata skupa E ima sledeća svojstva:

1. $P + Q \in E, \quad \forall P, Q \in E$ (zatvorenost)

2. $P + O = O + P = P, \quad \forall P \in E$ (postojanje neutralnog elementa O)

3. $P + (-P) = O, \quad \forall P \in E$ (postojanje inverznog elementa)

4. $P + (Q + R) = (P + Q) + R, \quad \forall P, Q, R \in E$ (asocijativnost)

5. $P + Q = Q + P, \quad \forall P, Q \in E$ (komutativnost)

Pokazali smo da je skup $E(K)$ u odnosu na operaciju sabiranja Abelova grupa.

Pretpostavimo da želimo da saberemo dvije tačke iz skupa E i to $P(x_1, y_1)$ i $Q(x_2, y_2)$. Neka je prava l prava koja prolazi kroz te dvije tačke. Jednačina koja je opisuje je:

$$l = \lambda x + v,$$

gdje je λ koeficijent pravca, dok je v odsječak te prave na y osi. U opštem slučaju, λ je predstavlja nagib prave l prema x osi, odnosno tangens ugla α, koji prava l zaklapa sa pozitivnim dijelom x ose, tj.

$$\lambda = \operatorname{tg} \alpha.$$

U slučaju eliptičke krive važi sledeće:

$$\lambda = \begin{cases} \frac{y_2 - x_2}{y_1 - x_1} & \text{ako je } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{ako je } P = Q \end{cases}$$

dok je $v = y_1 - \lambda x_1$.

Koordinate presječne tačke prave l i eliptičke krive E, koju smo prethodno označavali sa R, dobijamo rješavanjem sledeće jednačine:

$$(\lambda x + v)^2 = x_3 + ax + b.$$

Pošto je u pitanju jednačina trećeg stepena jasno je da je, u opštem slučaju, moguće dobiti 3 različita, realna rješenja. Imajući u vidu da su nam već poznata 2 rješenja, odnosno x koordinate tačaka P i Q : x_1 i x_2, potrebno je da prikažemo x koordinatu tačke R, tj. x_3.

Ukoliko izvršimo transformaciju polinoma na sledeći način:

$$\begin{aligned} x^3 + ax + b - (\lambda x + v)^2 = \\ &= (x - x_1)(x - x_2)(x - x_3) = \\ &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3 \end{aligned}$$

Izjednačavanjem koeficijenata po x^2 dobijamo:

$$-\lambda = -x_1 - x_2 - x_3,$$

odakle slijedi da je:

$$x_3 = \lambda^2 - x_1 - x_2.$$

Sada, izračunavamo z_3 na sledeći način:

$$y_3 = \lambda x_3 + v.$$

Na taj način smo izračunali koordinate tačke R, tj.:

$$P + Q = (x_3, -y_3).$$

Na osnovu ovoga mogu se definisati pravila za sabiranje tačaka eliptičkih krivih,tj.sabiranja u skupu E:

1. Ako je $P \neq Q$ i pri tome je $x_1 = x_2$, tada je $P + Q = O$.

2. Ako je $P = Q$ i pri tome je $y_1 = 0$, tada je $P + Q = 2P = O$.

3. Ako je $P \neq Q$ i pri tome je $x_1 \neq x_2$, tada je:

$$\lambda = \frac{y_2 - y_2}{x_2 - x_1} \quad \text{i} \quad v = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

4. Ako je $P = Q$ i pri tome je $y_1 \neq 0$, tada je:

$$\lambda = \frac{3x_1^2 + a}{2y_1} \quad \text{i} \quad v = \frac{-x^3 + ax + 2b}{2y}.$$

I konačno:

$$P + Q = (\lambda^2 - x_1 - x_2, \lambda^3 + \lambda(x_1 + x_2) - v)$$

Glava 7

Savremena primjena Diffie-Hellman protokola

Od 2016.godine preporučena vrijednost za broj p u standardnom Diffie-Hellman protokolu je 2048 bita. Još jedan od načina, koji poboljšava sigurnost, je prelazak sa grupe $\mathbb{Z}_p^*$ na skup tačaka eliptičkih krivih nad konačnim poljem. U tom skupu rješavanje problema diskretnog logaritma je gotovo neizvodljivo. Osim toga, ovim se omogućava korišćenje manjeg broja p tj. q, a da se pritom održava prihvatljiv nivo sigurnosti. Iz tog razloga Diffie-Hellman protokol u svojim implementacijama koristi algebarsku strukturu eliptičkih krivih. Ovo može učiniti razmjenu efikasnijom i smanjiti zahtjeve za skladištenjem. Npr. 224-bitni ključ eliptičke krive pruža isti nivo sigurnosti kao 2048-bitni RSA ključ. Za eliptičke krive nad $\mathbb{F}_q$ dužina prostog broja q bi trebala da bude barem 160 bita, dok je do sada taj broj bio 2048. Time je Alisi i Bobu jeftinije i jednostavnije računanje.

U sledećoj tabeli biće predstavljen odnos složenosti operacija Diffie-Hellman algoritma(DH) i eliptičkih krivih(ECDH) prema različitim nivoima sigurnosti.

Nivo sigurnosti (bitovi)	Odnos složenosti operacija DH i ECDH
80	3:1
112	6:1
128	10:1
192	32:1
256	64:1

Kada se koristi kriptografija eliptičkih krivih, sve osobe koje žele komunicirati kriptovanim porukama moraju se dogovoriti oko parametara koje definišu eliptičku krivu, odnosno o domenskim parametrima postupka. Neka je $E(\mathbb{F}_q)$ ciklična grupa sa generatorom P. Za primjenu u kriptografiji red generatora P, odnosno najmanjeg nenegativnog broja n takvog da je $nP = \underbrace{P + P + \ldots + P}_{n} = 0$, mora biti prost. Domenski parametri su $(q, FR, S, a, b, P, n, h)$, gdje se h naziva kofaktor i to je mali prirodni broj ($h < 4$) koji se u većini slučajeva postavlja na vrijednost 1, FR je indikator koji se koristi za prikazivanje elemenata, a S slučajni element ukoliko je eliptička kriva slučajno definisana korišćenjem određenih algoritama. Osim ako postoji uvjerenje da je domenske parametre generisala osoba od povjerenja, mora se potvrditi, prije upotrebe, da su ih generisale osobe koje žele komunicirati. Obično odabir domenskih parametara ne obavljaju osobe koje žele komunicirati, jer proces uključuje prebrojavanje tačaka koje se nalaze na eliptičkoj krivoj (što je posao koji oduzima puno vremena i nije ga lako implementirati). Zbog toga postoje organizacije koje obavljaju odabir domenskih parametara eliptičkih krivih za polja poznatih veličina. Neke od njih su *NIST (National Institute of Standards and Technology)* i *SECG(Standards for Efficient Cryptography Group)*. Ukoliko neko ipak želi sam odabrati domenske parametre, potrebno je odabrati konačno polje, a zatim iskoristiti neku od strategija za odabir krive sa prihvatljivim brojem tačaka, kao npr. *Koblitzove krive*. To su

eliptičke krive definisane nad $\mathbb{F}_2$ kao: $E : y^2 + xy = x^3 + a_2x^2 + 1$.

7.1 Određivanje grupe $E(\mathbb{F}_p)$

Bitan parametar, pri odabiru eliptičke krive, je broj tačaka koji će ona imati nad izabranim poljem. Kako bismo došli do tog broja, iskoristićemo polje $\mathbb{F}_p$ sa manjim brojem p i u primjeru odrediti grupu $E(\mathbb{F}_p)$.
U polju $\mathbb{F}_p$, pri čemu je $p \neq 2$ prost broj, pola elemenata su kvadrati.

Primjer 7.1. *U polju* $\mathbb{F}_{13}$ *je* $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 3$, $5^2 = 12$, $6^2 = 10$, $7^2 = 10$, $8^2 = 12$, $9^2 = 3$, $10^2 = 9$, $11^2 = 4$, $12^2 = 1$. *Jednačina* $y^2 = 12$ *ima dva rješenja* $y = \pm 5$ *tj.* $y = 5$ *i* $y = 8$. *Ako je* g *generator, onda su* g^{2k} *kvadrati, a* g^{2k-1} *nisu.*

Postoje efikasni elementi za utvrđivanje da li je neki element polja $\mathbb{F}_p$ kvadrat, odnosno ako jeste - za računanje njegovog korijena.

Primjer 7.2. *Neka je* E *kriva* $y^2 = x^3 + 1$. *Odrediti* $E(\mathbb{F}_5)$*(tačke sa koordinatama u* $\mathbb{F}_5$ *i broj tih elemenata).*

Rješenje:

Korisno je prethodno izračunati kvadrate: $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 4$, $4^2 = 1$.

x	x^3+1	$y=\pm\sqrt{x^3+1}$	*tačke*
0	*1*	$\pm 1 = 1, 4$	*(0,1),(0,4)*
1	*2*		
2	*4*	$\pm 2 = 2, 3$	*(2,2),(2,3)*
3	*3*		
4	*0*	*0*	*(4,0)*
			O

Dakle, skup $E(\mathbb{F}_5)$ *ima 6 tačaka. Tačke nad konačnim poljem se mogu sabirati korišćenjem jednačina pravih ili primjenom izraza za sabiranje. Ako je* $G = (2, 3)$*, onda je* $2G = (0, 1)$ *,* $3G = (4, 0)$*,* $4G = (0, 4)$ *(primijetimo da ova tačka ima istu* x*-koordinatu kao tačka* $2G$*, pa je* $4G + -2G$ *i* $6G = O$*),* $5G = (2, 2)$*,* $6G = O$*. Vidimo da je* $G = (2, 3)$ *generator grupe* $E(\mathbb{F}_5)$*.*

Primjer 7.3. *Neka je* E *kriva* $y^2 = x^3 + x + 1$ *nad* $\mathbb{F}_{109}$*. Postupkom analognim kao u prethodnom primjeru ispostavlja se da skup* $E(\mathbb{F}_{109})$ *ima 123 tačaka i da je generisan tačkom* $G = (0, 1)$*. Tačka* $(39, 45)$ *je u* $E(\mathbb{F}_{109})$*, jer je* $39^2 + 39 + 1 \equiv 63 \pmod{109}$ *i* $45^2 \equiv 63 \pmod{109}$*. Dakle,* $(39, 45) = (0, 1) + (0, 1) + \ldots + (0, 1) = n(0, 1)$*, za neki prirodan broj* n*. Postavlja se pitanje, koliko je to* n*?*

Određivanje broja n *je* ***problem diskretnog logaritma*** *sa eliptičkim krivama nad konačnim poljem. Problem se može rješavati grubom silom, ali ne i ako se broj* 109 *zamijeni sa prostim brojem* $\approx 10^{50}$*.*

Ovaj problem je trenutno teže riješiti nego DLP, pa se mogu koristiti kraći ključevi. Druga prednost je ta što se za fiksirano konačno polje može posmatrati više eliptičkih krivih.

Primjer 7.4. *Neka je* E *kriva* $y^2 = x^3 + 1$*. Odrediti* $E(\mathbb{F}_7)$*.*

Rješenje:

Imamo: $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 2$.

x	$x^3 + 1$	$y = \pm\sqrt{x^3 + 1}$	*tačke*
0	*1*	$\pm 1 = 1, 6$	*(0,1),(0,6)*
1	*2*	$\pm 3 = 3, 4$	*(1,3),(1,4)*
2	*2*	$\pm 3 = 3, 4$	*(2,3),(2,4)*
3	*0*	*0*	*(3,0)*
4	*2*	$\pm 3 = 3, 4$	*(4,3),(4,4)*
5	*0*	*0*	*(5,0)*
6	*0*	*0*	*(6,0)*
			O

Prema tome $E(\mathbb{F}_7)$ *ima 12 tačaka.*

$$R = (5, 0) \quad 2R = O$$

$$Q = (1, 3) \quad Q + R = (2, 3)$$

$$2Q = (0, 1) \quad 2Q + R = (4, 4)$$

$$3Q = (3, 0) \quad 2Q + R = (6, 0)$$

$$4Q = (0, 6) \quad 4Q + R = (4, 3)$$

$$5Q = (1, 4) \quad 5Q + R = (2, 4)$$

$$6Q = O$$

Sve tačke su oblika $nQ + mR$*, pri čemu je* $n \in \mathbb{Z}_6$ *i* $m \in \mathbb{Z}_2$*. Primijetimo da su koeficijenti krive* $y^2 = x^3 + 1$ *i koordinate tačaka definisane po modulu 7, a da se*

tačke sabiraju po modulu 6. U ovom slučaju dvije tačke generišu krivu. I dalje se može raditi sa diskretnim logaritmom koristeći npr. tačku $G = (1, 3)$ kao pseudogenerator. Ova tačka generiše samo polovinu skupa $E(\mathbb{F}_7)$.

U prosjeku skup $E(\mathbb{F}_p)$ ima $p + 1$ tačku.

U ovoj oblasti važna varijanta problema diskretnog logaritma naziva se problem diskretnog logaritma za eliptičke krive (eng. Ellyptic curve descrete logarithm problem-ECDLP). Ovaj problem kao i postupak Diffie-Hellman (eng. Ellyptic curve Diffie-Hellman-ECDH) definisaćemo analogno problemu unutar ciklične grupe $\mathbb{Z}_p^*$.

7.2 ECDH

Alisa i Bob žele komunicirati porukama preko nesigurnog komunikacionog kanala. Zajedno se dogovaraju o eliptičkoj krivoj E koju će koristiti i o tački $P \in E(\mathbb{F}_q)$. Diffie-Hellman protokol za razmjenu ključeva primijenjen na eliptičke krive sastoji se iz sledećih koraka:

1. Alisa generiše slučajan prirodan broj $k_A \in \{1, 2, \ldots, n-1\}$. Zatim, računa element $P_A = k_A P$.

2. Bob generiše slučajan prirodan broj $k_B \in \{1, 2, \ldots, n-1\}$. Zatim, računa element $P_B = k_B P$.

3. Alisa i Bob razmjenjuju P_A i P_B.

4. Alisa računa $P_{AB} = k_A P_B = (k_A k_B \pmod n)P$.

5. Bob računa $P_{AB} = k_B P_A = (k_B k_A \pmod n)P$.

Kao i u standardnom Diffie-Hellman protokolu, Alisa i Bob su izabrali svoje privatne ključeve k_A i k_B, koje nisu direktno razmijenili, već u sklopu poruka P_A i P_B.

Na taj način njihovi privatni ključevi ostali su sigurni. Ukoliko prisluškuje njihov protivnik, Eva, može saznati jedino elemente E,P,P_A i P_B. Međutim, ono što Evi treba za napad je broj P_{AB} tj. treba joj ili k_A ili k_B. U svakom slučaju, ona treba riješiti problem diskretnog logaritma, kako bi iz P_A došla do k_A ili iz P_B došla do k_B. Primijetimo da je ključ broj, a ono što koriste i biraju Alisa i Bob je tačka P sa krive. Na kraju dobijaju opet tačku sa krive. Nju transformišu u string bitova tako da im može koristiti kao njihov zajednički ključ.

7.2.1 ECDLP

Definicija 7.1. *Neka je E eliptička kriva nad konačnim poljem K. Neka su tačke $P, Q \in K$ takve da je tačka G element podgrupe od $E(K)$ generisane tačkom P, reda n. Treba odrediti $k \in \{2, 3, \ldots, n\}$, za koje važi $G = kP$, odnosno $G = \underbrace{P + P + \ldots + P}_{k puta}$.*

Vidimo da je množenje tačke P brojem k veoma lako, ali inverzna operacija (traženje broja k znajući kP) je neizvodljiva, ako je polje $\mathbb{F}_q$ dovoljno veliko. Ovaj problem je razlog zbog kojeg su eliptičke krive toliko proučavane u kriptografiji i zbog čega se koriste i danas. Naime, zbog posebnog načina računanja broja k i svojstva da sve tačke čine cikličnu grupu, za dovoljno veliko k protivniku je gotovo nemoguće riješiti problem ECDLP u razumnom vremenu. Treba napomenuti da je ECDLP u grupi $E(\mathbb{F}_q)$ čak još teži od DLP u $\mathbb{F}_p^*$.

Primjer 7.5. *Neka je $p = 211$, $E : y^2 = x^3 - 4$, $P = (2, 2)$. Ispostavlja se da je $241P = O$. Alisin privatni ključ je $k_A = 121$, pa je njen javni ključ $k_A P = 121(2, 2) = (115, 48)$. Bobov privatni ključ je $k_B = 223$, pa je njegov javni ključ $k_B P = 223(2, 2) = (198, 72)$. Njihov zajednički (dogovoreni) ključ je $k_A k_B P$. Prema tome, Alisa izračunava $k_A(k_B P) = 121(198, 72) = (111, 66)$, a Bob izračunava $k_B(k_A P) = 223(115, 48) = (111, 66)$. Dobili su istu vrijednost i to je njihv zajednički ključ.*

Primijetimo da, broj k_A koji množenjem sa tačkom $P = (2, 2)$ daje Alisin javni ključ $(115, 48)$ je u stvari instanca problema ECDLP. Alisa može množenje $121P$ izvršiti ponovljenim udvostručavanjem $64P + 32P + 16P + 8P + 1P$. Analogno za broj k_B.

7.3 Napadi na ECDH

Kao što je već rečeno, sigurnost protokola ECDH temelji se na težini ECDLP. Domenski parametri u kriptografiji eliptičkih krivih moraju biti pažljivo odabrani, kako bi se izbjegli eventualni napadi na ECDLP. Najobičniji napad je napad grubom silom koji predstavlja iscrpljujuće istraživanje i može se sprovesti birajući dovoljno veliko $n (n \geq 2^{80})$. Pored toga, postoji napad kombinacijom Pohlig-Hellman i Pollard's rho algoritama sa predviđenim vremenom izvršavanja $O(\sqrt{p})$, gdje je p najveći prost djelilac broja n. Kako bi se izbjegao ovaj napad, trebalo bi birati parametre eliptičke krive tako da je n djeljiv sa dovoljno velikim brojem p. Veličina broja p trebala bi biti takva da se računanje mora svesti na minimum $\sqrt{p}$ koraka tj. da je $p \leq 2^{160}$. Vodeći računa o tome, rješavanje ECDLP je neizvodljivo u okviru današnje tehnologije. S druge strane, ne postoji matematički dokaz za to. To je jedno od fundamentalnih otvorenih pitanja u računarskim naukama. ECDLP se pojavio 1985.godine, pa i nije dovoljno proučavan, kao što je DLP za koji je pronadjeno subeksponencijalno rješenje. Iz tih razloga, i danas postoji određena doza skepticizma pri korišćenju ECDH-a.

Napad woman-in-the-middle je popularan i kod korišćenja eliptičkih krivih. Ako se koristi neki način autentifikacije uz ECDH, a Alisa i Bob koriste iste ključeve pri svakoj novoj komunikaciji, onda ovaj algoritam nazivamo *statički* ECDH. Postoji i drugi način, da se ne koriste sertifikati, ali da se generišu novi ključevi svaki put kada se koristi protokol. Ova varijanta se naziva *anonimni* ECDH. Ova varijanta ne

obezbjeđuje autentifikaciju učesnika u komunikaciji, već se koristi u kombinaciji sa odvojenim metodama autentifikacije, kao što su one bazirane na digitalnom potpisu i sertifikatu. Ova kombinacija se naziva *efemeralni* ECDH ili skraćeno ECDHE. Ovako korišćen, ECDHE može obezbijediti potpunu sigurnost u smislu da otkrivanje ključa jedne poruke ne može dovesti do otkrivanja ključeva preostalih poruka i da ne postoji neka tajna vrijednost čije kompromitovanje može dovesti do kompromitovanja još nekih.

7.4 Sigurni Internet protokoli

Diffie-Hellman protokol ima široku upotrebu u mrežnim protokolima kao što su IPsec, IKE, SSH, SSL, TLS i mnogim drugim.

IPsec (Internet protocol security) je skup protokola koji obuhvata mehanizme za zaštitu mrežnog prometa na nivou trećeg sloja OSI modela (mrežni sloj) kriptovanjem i autentifikacijom IP paketa. IPsec standard obično se koristi za spajanje servera sa korisnikom, kako bi oni mogli komunicirati putem nesigurnog kanala. Prije uspostavljanja veze, koristi se **IKE** (Internet key exchange) protokol za razmjenu simetričnog ključa. IKE protokol zapravo u pozadini koristi Diffie-Hellman algoritam za razmjenu ključeva.

SSH (Secure Shell) protokol koristi se za sigurni pristup i prijavu na konzoli udaljenog računara, uglavnom na operativnim sistemima Unix/Linux. Često se koristi za sigurno prijavljivanje na Internet. Ovaj protokol može automatski da enkriptuje, autentifikuje prenos podataka. SSL funkcioniše u tri faze. U prvoj radi identifikaciju, a u drugoj se obavlja razmjena ključa u kojoj se može iskoristiti i standardni Diffie-Hellman protokol. U trećoj fazi se razmijenjeni tajni ključ koristi za generisanje novih ključeva. Osmišljen je kao zamjena za nezaštićeni protokol Telnet koji je imao istu

svrhu. Sve naredbe i odgovori koji se prenose između servera i klijenta kriptovane su simetričnim ključem koji se dobija upravo Diffie-Hellman algoritmom.

TLS (Transport layer security) i njegov prethodnik **SSL** (Security Sockets Layer) danas su najčešće korišćeni protokoli koji omogućavaju sigurnu komunikaciju jer se koriste na Webu (HTTP protokol), za e-mail, Internet fax, instant messaging itd. Njihova osnovna funkcija je da uspostave enkriptovanu vezu izmedju web servera i pretraživača(browser-a). TLS omogućava aplikacijskom sloju autentičnost i privatnost komunikacije pomoću enkripcije dogovorenim simetričnim ključem. TLS i SSL se često zajedno nazivaju SSL. Prije nego klijent i server počnu da razmjenjuju informacije zaštićene protokolom SSL, moraju se dogovoriti oko ključa koji će koristiti za enkripciju podataka. ECDH je jedan od najsigurnijih načina za to. SSL se sastoji od 2 sloja. Donji sloj koristi simetričnu kriptografiju, a gornji sloj se naziva *handshake* protokol. Diffie-Hellman se koristi u gornjem sloju. Može se koristiti u više oblika, ali je preporučljiv ECDH. Handshake protokol omogućava serveru da autentifikuje sebe klijentu, koristeći tehnike javnog ključa, tj. asimetričnu kriptografiju. Time je riješen problem autentifikacije i utvrđivanja identiteta učesnika u komunikaciji.

Glava 8

Zaključak

U ovom radu opisani su protokoli za obavljanje sigurne komunikacije putem otvorenih komunikacionih kanala, kao što je Internet. Znajući koliko je Internet značajan, primjećujemo da su ovi protokoli neophodni za funkcionisanje u današnjem vremenu.

Jasno je da iza toga stoji kriptografija eliptičkih krivih, koja ima sve veću primjenu u različitim oblastima gdje je neophodna kriptografska zaštita, a pri čemu se raspolaže ograničenim memorijskim i procesorskim resursima. Mogućnost korišćenja minimalne dužine ključa i brže računanje zajedničkog ključa su neke od brojnih prednosti. Kao familija algebarskih krivih eliptičke krive su detaljno obrađene u matematici, ali zbog obimnosti u ovom radu su objašnjeni samo pojmovi suštinski za Diffie-Hellman protokol. Problem rješavanja diskretnog logaritma se koristi kao temelj sigurne razmjene ključa, ali nije dobro što i dalje ne postoje matematički dokazi za njegovu težinu. U poređenju standardnog Diffie-Hellman protokola (DH) i Diffie-Hellman protokola sa eliptičkim krivama(ECDH) zaključujemo da je ECDH u velikoj mjeri efikasniji. Iako je u grupi $E(\mathbb{F}_q)$(ECDH) sabiranje mnogo sporija operacija od množenja u $\mathbb{F}_q$ (DH), taj nedostatak nadoknađuje činjenica da broj q u $E(\mathbb{F}_q)$ može biti mnogo manji od broja q u $\mathbb{F}_q$, a da se time ne umanjuje sigurnost sistema. Osim toga, u pogledu rješavanja ECDLP nije bilo napretka u poslednjih 20 godina, dok

se rješavanje DLP stalno usavršava. Kada su u pitanju napadi na DH i ECDH sisteme, osnovni i zajednički cilj je da se izbjegne otkrivanje tajnog ključa. Uz pravilan odabir parametara oba sistema otporna su na napade grubom silom, a ranjivost na napade woman-in-the-middle rješavaju u kombinaciji sa metodama za autentifikaciju učesnika u komunikaciji.

Diffie-Hellman protokol ušao je u istoriju kao najznačajniji jer je jedini koji je omogućio sigurnu razmjenu tajnog ključa simetričnih kriptosistema. Time je riješio problem star preko dvije hiljade godina i dao osnove asimetrične kriptografije.

Bibliografija

[1] A.J. McCurley: The discrete logarithm problem, Proceedings in applied Cryptography, Providence, 1990.

[2] www.sinergija.edu.ba : Asimetrični šifarski sistemi, Difi Helman

[3] Miodrag Živković: Kriptografija, 2020.

[4] CARNet CERT, LS & S: Korištenje eliptičnih krivulja u kriptografiji

[5] CARNet CERT, LS & S: Diffie-Hellman protokol

[6] Kristina Kunjadić-Ćulibrk, master rad : Kriptografija eliptičnih krivih, Beograd, 2016.

[7] Ivan Škorić: Kriptografija javnog ključa, Osijek, 2015.

[8] Visoka škola elektrotehnike i računarstva strukovnih studija, Beograd: Šifarski sistemi sa javnim ključem

[9] https://web.entrust.com/resource/zero-ecdh-elliptic-curve-diffie-hellman-30-minutes/ : Zero to ECDH in 30 minutes

[10] Rakel Haakegaard, Joanna Lang: The Elliptic Curve Diffie-Hellman, Decembar, 2015.

[11] Daniel L.R. Brown: Elliptic Curve Criptography, Maj, 2009.

[12] Tomislav Milković: Diffie-Hellman protokol za razmjenu ključeva, Zagreb, 2019.

[13] Marija Sabljić: Koblitzove eliptičke krive, Zagreb, 2018.

[14] Dino Sejdinović: Eliptičke krivulje u kriptografiji, 2006.

[15] https://heritage-offshore.com/sigurnost-informacija/to-je-razmjena-kljueva-diffie-hellman-i-kako-to/