CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

# Diffie-Hellman protokol

## NCERT-PUBDOC-2009-12-284

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

## Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

## LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

# Sadržaj

# 1. Uvod

Od davnina pa do današnjih dana, ljudi su imali potrebu za sigurnom komunikacijom. Pritom su bili svjesni da njihove poruke često putuju "nezaštićenim komunikacijskim kanalima". Ti kanali su mogli biti npr. nezaštićeni fizički putovi (kao što su ceste, pruge i sl.), zatim telefonske linije ili računalne mreže. Kako bi zaštitili svoje poruke počeli su ih pretvarati u oblik čitljiv samo osobama kojima su bile namijenjene, odnosno počeli su kriptirati poruke. Ljudska je povijest posijana kriptiranima porukama koje su odlučivale o ishodima bitaka i ratova te u smrt odvele mnoge kraljeve i kraljice. Upravo zbog toga te zbog opasnosti da bi neprijatelj mogao „uhvatiti“ poruku razvila se znanost koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Ta znanost nazvana je kriptografija. Osnovni zadatak kriptografije je omogućavanje dvjema osobama da komuniciraju preko nezaštićenog komunikacijskog kanala na način da treća osoba, kojoj nije namijenjena poruka, ne može razumjeti njihove poruke. Pošiljatelj preoblikuje otvoreni ili jasni tekst koristeći unaprijed dogovoreni ključ K. Taj se postupak zove kriptiranje, a dobiveni je rezultat kriptirani tekst. Ukoliko se koristi simetrični kriptosustav za dekriptiranje, primatelj treba poznavati ključ kojim je poruka kriptirana. Ključ posjeduje samo osoba koja je poruku kriptirala i primatelj jedino od nje može dobiti ključ. Prema tome, potrebno je obaviti razmjenu ključeva, odnosno pošiljatelj treba na neki način poslati ili osobno predati ključ kojim primatelj može dekriptirati poruku. Takav se ključ naziva tajnim ključem i koristi se za kriptiranje i dekriptiranje poruke, što znači da primatelj može poruku dekriptirati samo upotrebom istog ključa kojim je kriptirana. Kako bi došao do tog ključa pošiljatelj mu mora na neki način predati ključ, odnosno primatelj i pošiljatelj moraju obaviti razmjenu tajnog ključa. To je veliki problem koji je riješen tek 1976. godine kada su Diffie i Hellman objavili svoj protokol za razmjenu tajnog ključa.

Diffie-Hellmanov protokol za razmjenu ključeva je prvi takav protokol koji je javno objavljen. On omogućava razmjenu tajnih ključeva na siguran način. Britanska tajna služba GCHQ (Government Cmmunications Headquarters) je već prije 1976. razvila takav protokol, no držala ga je u tajnosti. Postoji mogućnost da je već i prije bio otkriven (s obzirom na svoju jednostavnost) no svakako nije bio javno objavljivan.

Protokol nosi ime po svojim tvorcima: Whitfield Diffie i Martin Hellman. Danas postoji više implementacija ovog protokola, te izvorno nije predviđen za implementaciju pomoću eliptičkih krivulja, no ime je još ostalo povezano uz osnovnu ideju. Organizacija IEEE je predložila standard s protokolom Diffie-Hellman kao osnovnim algoritmom za razmijenu ključeva ali postoje i još neke poboljšane ideje koje rješavaju neke probleme kao što je ranjivost na *napad s čovjekom u sredini* (eng. man in the middle). Kako bi se spriječio takav napad predlaže se obavljanje autentikacije prije početka razmjene ključa.

U sljedećim poglavljima biti će opisana povijest nastanka Diffie-Hellmanovog protokola, sam protokol u svoje dvije inačice, njegova primjena te moguće ranjivosti i primjer napada na protokol.

# 2. Povijest protokola Diffie – Hellman

## 2.1. Osnove kriptografije

Tokom povijesti kraljevi, kraljice i vojskovođe pri upravljanju svojim zemljama i vođenju svojih vojski stoljećima ovise o djelotvornoj komunikaciji. Istodobno su, međutim, svi oni bili svjesni toga što bi se dogodilo kada bi njihove poruke došle u krive ruke. U tom slučaju suparničkim državama bi razotkrile dragocjene tajne, a protivničkim snagama odale ključne informacije. I baš je ta opasnost da bi neprijatelj mogao uhvatiti poruku, napokon i potaknula razvoj kriptografije, odnosno sredstava kojima se postiže da poruku može pročitati samo ona osoba kojoj je namijenjena. Tokom vremena tehnologija se promjenila i napredovala, ali ideja je ostala ista.

U raspodijeljenim računalnim sustavima informacije se prenose raznovrsnim otvorenim i nezaštićenim komunikacijskim putovima u obliku poruka. Pristup do tih putova ne može se fizički zaštititi (to je posebice razumljivo za komunikacijske putove ostvarene radiovezama). Prema tome, svaki neprijateljski nastrojeni napadač ili uljez može vrlo lako narušiti sigurnost raspodijeljenog sustava. Zbog toga u raspodijeljenim sustavima komunikacijski zaštitni mehanizmi postaju najvažniji oblik ostvarenja sigurnosti.

Osnovni problem komunikacijskih zaštitnih mehanizama je zaštita poruka. Pokazuje se da je najdjelotvornija zaštita poruka njihovo kriptiranje. Većina se narušavanja sigurnosti može razmotriti na mehanizmu protoka poruka od izvorišta do odredišta. Prema tome, moguće je razmatrati modele zaštite komunikacijskog kanala od izvorišta do odredišta. Ovakvi se modeli mogu primijeniti i na ostale oblike zaštite jer se međusobno djelovanje subjekata i objekata može positovjetiti s razmjenom poruka.

U umreženim računalnim sustavima važno je uspostaviti sigurnosni mehanizam. Mnoga korisna ostvarenja uporabe računalnih mreža u gotovo svim područjima ljudske djelatnosti dobrim djelom ovise o razvitku pouzdanih zaštitnih mehanizama koji će osigurati primjerenu sigurnost sustava. Milijuni ljudi svakodnevno koriste mreže računala, uključujući i Internet, za bankarstvo, kupovinu, slanje poruka elektroničke pošte i slično. Što znači da se svakodnevno Internetom prenose povjerljivi podaci, kao što su podaci kreditnih kartica, osobni podaci i drugo. Kako bi se podaci zaštitili potrebno je između ostalog ostvariti prikladnu sigurnost komunikacije u mrežama računala. S obzirom da je u komunikacijskom sustavu gotovo nemoguće spriječiti prisluškivanje podataka, pokazalo se razumnim učiniti podatke nerazumljivim neovlaštenim korisnicima. Podaci koji u svom izvornom obliku predstavljaju neku korisnu informaciju mogu se postupkom kriptiranja prevesti u oblik u kojem se ta informacija više ne prepoznaje. S obzirom da su počeci kriptiranja povezani s prenošenjem pisanih informacija u obliku tekstova, u kriptografskoj se terminologiji izvorni oblik podataka naziva razgovjetnim ili jasnim tekstom (eng. plaintext, cleartext). Postupkom kriptiranja jasni se tekst prevodi u kriptirani tekst. Obrnuti postupak prevođenja kriptiranog teksta u jasni tekst naziva se dekriptiranje.

U danjašnje se vrijeme, kada mnogo ljudi ima na raspolaganju vrlo moćna računala, ne mogu primjenjivati neke „naivne“ (stare) metode kriptiranja koje su se zasnivale na zamjeni znakova prema nekim složenim pravilima. Na primjer, Julije Cezar je vrlo često slao tajne poruke. Njegove tajne poruke kriptirane su na jednostavan način. On bi svako slovo u poruci zamijenio drugim, za tri mjesta dalje u abecedi. Sljedeća slika prikazuje takvu zamjenu u abecedi i daje primjer otvorenog teksta i kriptiranog teksta.

```
Abeceda:            a b c č  ć d dž đ e f g h i j  k l lj m n nj o p r s š t u v z ž
Kriptirana abeceda: č ć d dž đ e f  g h i j k l lj m n nj o p r  s š t u v z ž a b c


Otvoreni tekst:     dođoh vidjeh pobjedih
Kriptirani tekst:   esgsk aleljhk šsćljhelk
```

***Slika 1. Primjer Cezarovog pomičnog kriptosustava***

Supstitucija na slici 1 često se naziva Cezarovim pomičnim kriptografskim postupkom. Današnji kriptografski postupci su parametarske matematičke funkcije, odnosno algoritmi kojima se nizovi bitova jednog teksta preračunavaju u nizove bitova kriptiranog teksta i obrnuto.

Funkcija kriptiranja može se zapisati u sljedećem obliku:

$$C = E(P, K_E),$$

gdje je *P* jasni tekst, *C* kriptirani tekst, *E* funkcija kriptiranja i $K_E$ parametar ili ključ kriptiranja.

Funkcija dekriptiranja je u tom slučaju:

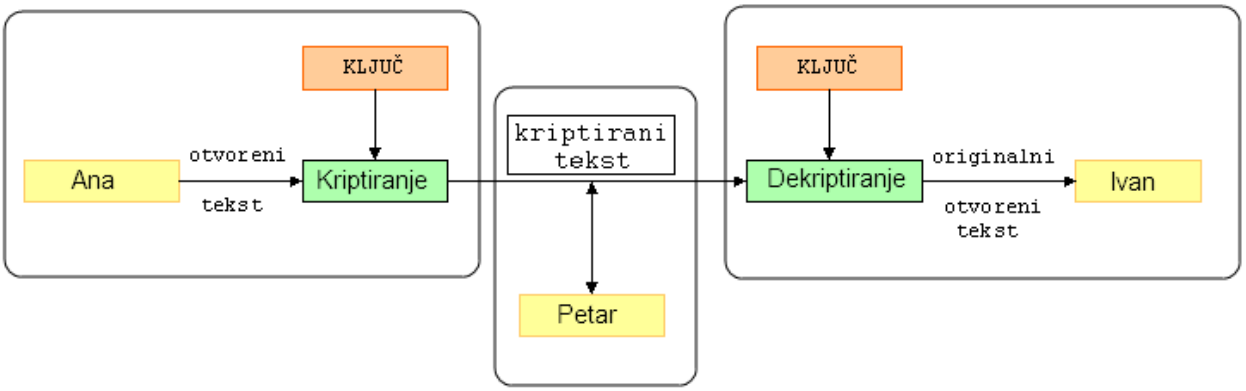
$$P = D(C, K_D),$$

gdje je *D* funkcija dekriptiranja i $K_D$ parametar ili ključ dekriptiranja. Funkcija dekriptiranja je inverzna, tako da vrijedi:

$$P = D(E(P, K_E), K_D),$$

odnosno dekriptiranjem kriptiranog jasnog teksta dobije se ponovno jasni tekst. Ako se kriptiranje obavi u izvorištu i dekriptiranje u odredištu tada se kriptiranjem komunikacijski kanal štiti od prisluškivanja i može se postići povjerljivost informacija.

Sljedeća slika prikazuje komunikaciju kriptiranim porukama. Ana i Ivan komuniciraju slanjem kriptiranih poruka, dok Petar pokušava presresti poruke i dekriptirati ih bez poznavanja ključa.




***Slika 2.Komunikacija kriptiranim porukama***

Prije izlaganja kako je nastao protokol Diffie-Hellman potrebno je napomenuti da su danas u uporabi dva osnobna oblika kriptosustava:

- simetrični kriptosustavi i
- asimetrični kriptosustavi.

Danjašnji kriptosustavi zasnivaju se na postupcima koji se mogu učinkovito izvoditi na računalima i to bilo sklopovski ili programski. Ti se postupci zasnivaju na algoritmima koji su u pravilu opće poznati, ali s ključevima koji imaju vrlo velik broj mogućih vrijednosti. To omogućuje stvaranje vrlo velikog broja različitih oblika kriptiranog teksta.

U simetričnim kriptosustavima ključ kriptiranja jednak je ključu dekriptiranja. Zajednički se ključ može označiti simbolom K. Za takav sustav vrijede slljedeći izrazi:

1) $C = E(P, K)$
2) $P = D(C, K)$
3) $P = D(E(P, K), K)$

Asimetrični kriptosustavi imaju različite ključeve kriptiranja i dekriptiranja i mogu se opisati izrazima:

4) $C = E(P, K_E)$
5) $P = D(C, K_D)$
6) $P = D(E(P, K_E), K_D)$

## 2.2. Distribucija ključa

Šezdesetih su godina računala postajala sve naprednija, no istodobno i jeftinija. Tako su postala dostupna i u gospodarstvu pa ih je sve veći broj tvrtki mogao primijeniti i za kriptiranje njima važnih poruka (npr. poruka o prijenosu novca ili o osjetljivim trgovačkim pregovorima). Međutim, kako je sve više tvrtki kupovalo računala i kako su sve više komunicirale kriptiranim porukama, kriptografe je sve više mučio problem distribucije ključa.

Uzmimo na primjer da neka banka želi klijentu telefonskim putem poslati povjerljive podatke. Odmah je jasno kako postoji mogućnost da netko prisluškuje komunikaciju, te na taj način neovlašteno otkriva podatke o klijentu i/ili banci. Kako bi banka poslala povjerljive podatke u porukama klijentu, svakako mora zaštititi svoje poruke od prisluškivanja. Zbog toga banka bira ključ (koji definira točan recept za premetanje poruke) i kriptira poruku. Za dekriptiranje poruke klijent mora imati kopiju programa koji je korišten za kriptiranje, ali i ključ kojim je poruka kriptirana. Kako banka može obavijestiti klijenta o ključu? Ne može mu ga poslati telefonski jer postoji mogućnost da netko prisluškuje. Očito je da se ključ može sigurno prenijeti samo osobno, što ne samo da oduzima vrijeme, nego je i besmisleno – jer se onda umjesto ključa na isti način može prenijeti i čitava poruka. Manje sigurno, no praktičnije rješenje je slanje pomoću kurira. Sedamdesetih su godina banke za distribuciju ključeva zapošljavale posebne tekliće, čija je prošlost temeljito istražena i provjerena. Ti su se ljudi ubrajali u najpouzdanije zaposlenike u banci. Oni bi jurili svijetom sa zaključanim torbama za spise i osobno dijelili ključeve svima koji su trebali dobiti poruku od banke. Kako je poslovna mreža rasla, rastao je i broj poslanih poruka, a kako je trebalo dostavljati sve više ključeva, banke su uskoro otkrile da se taj proces pretvorio u logističku noćnu moru. Uz to, dodatni su troškovi cijelog procesa postali previsoki.

Problem distribucije ključa mučio je kriptografe kroz čitavu povijest. Tako je primjerice u Drugom svjetskom ratu njemačka vlada svakog mjeseca morala distribuirati knjigu dnevnih ključeva i dostaviti je svim operaterima Enigme, poznatog stroja za kriptiranje koji se koristio tokom rata. To je stvaralo velike logističke probleme. Osim toga, ključeve je trebalo redovito dostavljati i podmornicama koje su u pravilu dugo izbivale iz baze. Sve u svemu, ljudi koji su komunicirali kriptiranim porukama morali su pronaći način kako da ključ pošiljatelja sigurno dostave primatelju. Bez obzira koliko je kriptografski algoritam bio siguran u teoriji, u praksi ga može pokopati problem distribucije ključa.

Pitanje distribucije ključa može se činiti trivijalnim, ali on je za poratne kriptografe postao problemom koji je nadišao sve ostale. Ako dvije osobe žele sigurno komunicirati, moraju se pouzdati u trećega koji će dostaviti ključ, i tako taj treći postaje najslabijom karikom u lancu osiguranja.

Usporkos tvrdnjama da je problem distribucije ključa nerješiv, sredinom sedamdesetih godina otkriveno je briljantno rješenje. Unatoč tome što su računala preobrazila primjenu kriptografskih algoritama, ipak je najveću revoluciju u kriptografiji dvadesetog stoljeća izazvao razvoj tehnika za svladavanje problema distribucije ključeva. Zapravo, to se otkriće smatra najvećim kriptografskim ostvarenjem još od izuma monoalfabetske metode [5] kriptiranja (jedne od najranijih metoda kriptiranja poruka) prije dvije tisuće godina.

## 2.3. Preduvjeti za nastanak protokola Diffie-Hellman

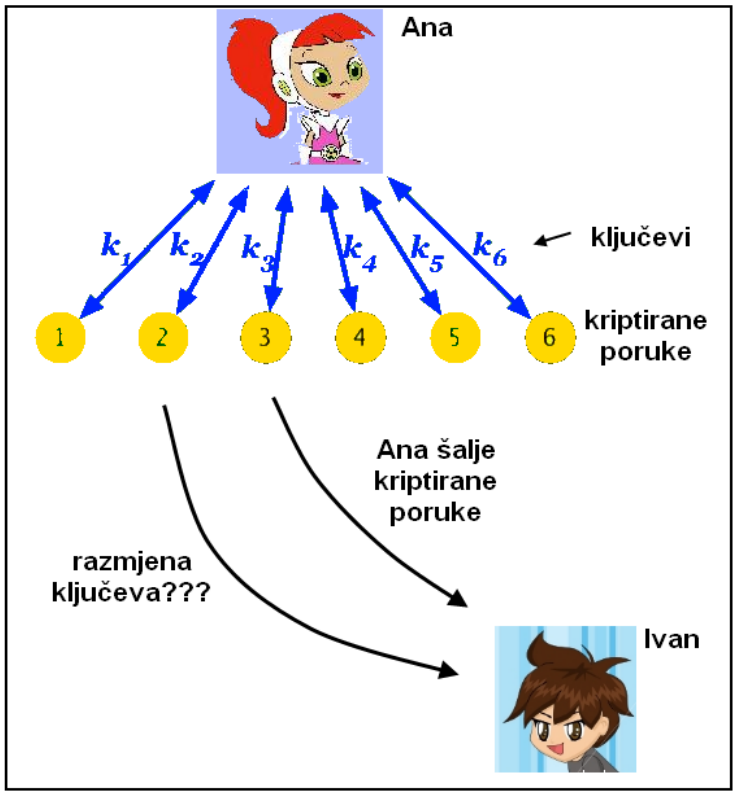
Whitfield Diffie (rođen 1944.) je jedan od najpoznatijih kriptografa svoje generacije i jedan od osnivača asimetrične kriptografije. Diffie se zanimao za problem distribucije ključa i dio motivacije dobivao je iz vizije umreženog svijeta. U rješavanju problema Diffiju su se 1974. godine pridružili Martin Hellman i Ralph Merkle, također kriptografi.

Šezdesetih je godina američko Ministarstvo obrane (eng. U.S. Department of Defense) osnovalo i financiralo istraživačku organizaciju: „Agencija za napredne istraživačke projekte“ (eng. Advanced Research Projects Agency – ARPA). Jedan od najistaknutijih projekata svodio se na pronalazak načina povezivanja vojnih računala na velike udaljenosti. Računala su povezali mrežom nazvanom ARPANet, iz kojeg je konačno 1982. proizašao Internet. Krajem osamdesetih godina pristup Internetu dobili su i ljudi koji nisu bili povezani s državom ili akademskim istraživanjem te je broj korisnika naglo porasao. Danas milijuni ljudi diljem svijeta preko Interneta razmjenjuju najraznovrsnije informacije. Dok je ARPANet bio još u povojima, Diffie je već tada pretpostavio kako će jednoga dana i obični ljudi imati osobna računala koja će biti povezana telefonskim linijama te kako će ljudi razmjenjivati različite poruke putem računalne mreže. Diffie je smatrao da ako ljudi razmjenjuju poruke putem računalne mreže, imaju pravo osigurati privatnost svojih poruka njihovim kriptiranjem. Međutim kriptiranje prije svega zahtjeva sigurnu razmjenu ključa.

Ako razmjena ključa predstavlja veliki problem za državu i velike korporacije, za građane će biti neostvariva (što će ih u konačnici lišiti prava na privatnost).

Postavlja se pitanje kako dva stranca koja su se upoznala preko Interneta mogu jedan drugome poslati kriptiranu poruku. Ukoliko se zamisli priča o čovjeku koji preko Interneta želi nešto kupiti, postavlja se pitanje kako je moguće poslati kriptirane podatke o kreditnoj kartici, ali na taj način da ih može dekriptirati samo prodavač. U oba slučaja stranke moraju raspolagati ključem, no kako da ga sigurno razmijene?

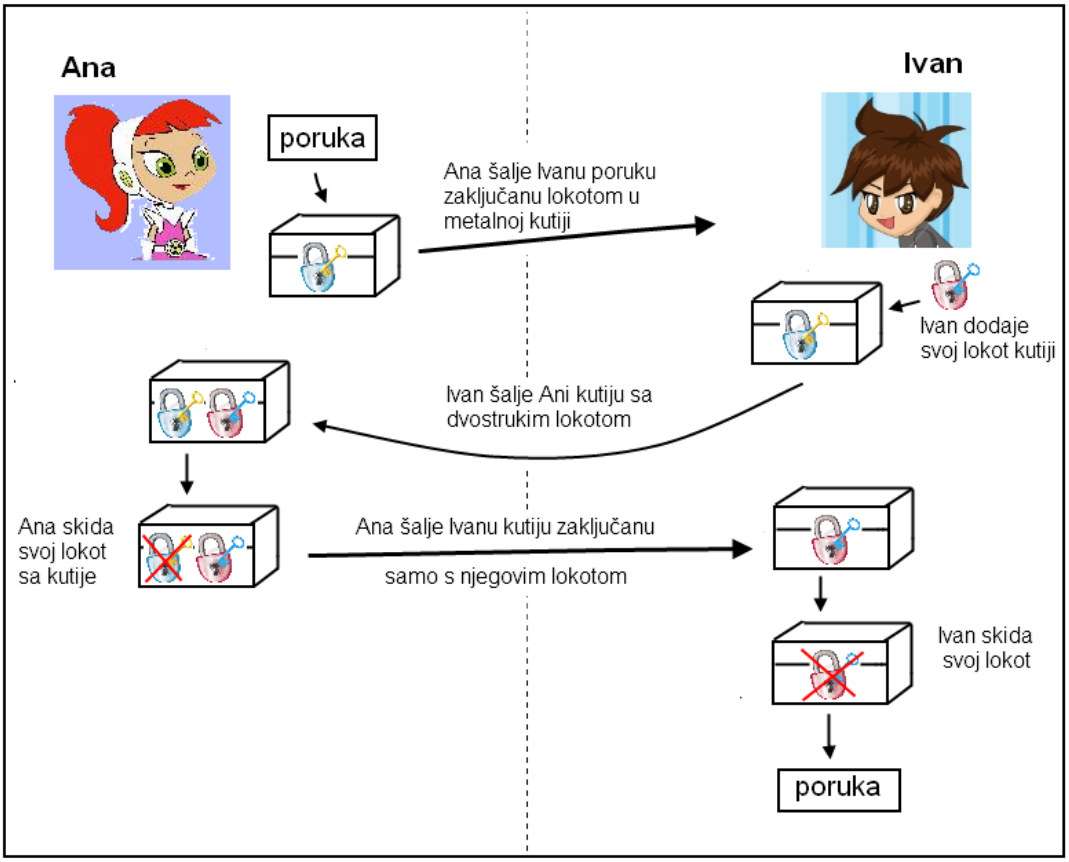
Kako bi se bolje približio problem distribucije ključa, moguće je zamisliti tri osobe. Neka su to Ana, Ivan i Petar, koje sudjeluju u komunikaciji. Ana i Ivan žele komunicirati slanjem poruka, a Petar, koji nije uključen u tu komunikaciju želi (neovlašteno) otkriti sadržaj poruka koje se razmjenjuju. Ako Ana i Ivan ne žele da im bilo tko čita poruke, prije slanja će ih kriptirati. Prema tome kada Ana šalje poruke, svaku poruku koju šalje treba kriptirati upotrebom novog ključa kako bi komunikacija bila što sigurnija i svaka poruka bila kriptirana drugim ključem. Ana se stalno nalazi pred problemom distribucije ključeva jer ih mora sigurnim putem dostaviti Ivanu (kako bi on mogao pročitati njezine poruke). Taj se problem može riješiti tako da se Ana i Ivan nađu jednom tjedno i razmjene dovoljno ključeva za sve poruke koje će poslati u tom tjednu. Osobna razmjena kključeva siguran je postupak, ali i nepraktičan. Što ako se na primjer Ana ili Ivan razbole? Čitav sustav temeljen na ovakvoj komunikaciji se tada ruši. Ana i Ivan, u tom slučaju mogu angažirati kurire, što je skuplje i nepouzdanije. Dvije se tisuće godina smatralo da je distribucija ključeva neizbježna. To se čak smatralo aksiomom kriptografije, tj. neporecivom istinom.




***Slika 3. Slanje kriptiranih poruka i pitanje kako sigurno razmjeniti ključeve***

Slijedeći primjer slikovito opisuje problem distribucije ključeva i nudi jedno rješenje. Neka Ana i Ivan žive u zemlji u kojoj je poštanski sustav nepovjerljiv i svi poštari uvijek čitaju svako pismo koje trebaju predati primatelju. Jednoga dana Ana poželi poslati privatno pismo Ivanu. Ana ga stavlja u čeličnu kutiju, zatvara i osigurava ključem i lokotom. Zaključanu kutiju šalje poštom, a ključ zadrži. Kad paket stigne do Ivana, on ga ne može otvoriti jer ne posjeduje ključ. Ana bi mogla u drugu kutiju staviti ključ, zatvoriti je lokotom i poslati Ivanu, ali bez ključa za taj drugi lokot, on ju ne može otvoriti pa tako ni doći do ključa koji otvara prvi paket. Problem bi se mogao riješiti tako da Ana napravi kopiju svojeg ključa i preda ga Ivanu na osobnom sastanku. No to je samo stari problem prikazan na nov način.

Probajmo zamisliti slijedeću situaciju: kao i ranije Ana želi Ivanu posalti poruku i zato opet stavlja tajnu poruku u željeznu kutiju koju zaključa lokotom te šalje Ivanu. Kada paket stigne do Ivana, on mu dodaje vlastiti lokot i vraća je Ani, koja prima paket osiguran s dva lokota. Ana sada uklanja vlastiti lokot i ostavlja samo Ivanov i paket ponovo šalje Ivanu. Tu se javlja ključna razlika, Ivan sada može otvoriti kutiju zato što je osigurana samo s njegovim lokotom, čiji ključ posjeduje.




***Slika 4. Razmjena poruka upotrebom dvostrukog lokota***

Implikacije ovog primjera su strahovite. On dokazuje da se tajna poruka može pouzdano razmjeniti između dvoje ljudi bez potrebe razmjene ključa. Po prvi put pojavila se nada u to da razmjena ključa u kriptografiji ne mora biti nešto neizbježno. Unatoč tome, javljaju se određene poteškoće u rješenju kojeg nudi primjer. Jedna poteškoća je poredak otključavanja, odnosno kriptiranja i dekriptiranja. Općenito govoreći, redoslijed kriptiranja i dektipritanja vrlo je važan i potrebno je držati se LIFO (eng. Last In First Out) pravila , tj. da se posljednje kriptiranje prvo dekriptira.

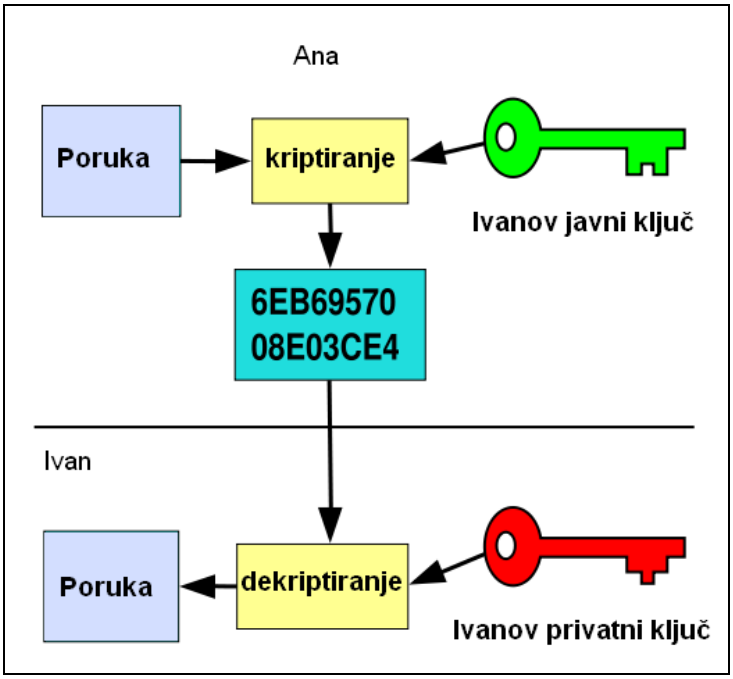
Drugim riječima, posljednji se stupanj enkripcije mora dektiptirati prvi. U opisanom scenariju, Ivan je izveo posljednji stupanj kriptiranja (posljednji je stavio lokot). Prema tome trebalo bi ga se prvog dektiptirati, ali Ana je prva maknula svoju enkripciju, dakle prije Ivana. Nažalost, kad je riječ o poretku, mnogi su kriptografski sustavi osjetljiviji od lokota. Iako taj „dvolokotni“ pristup u stvarnom kriptografskom svijetu ne funkcionira, on je Diffieija i Hellmana potaknuo da krenu u potragu za ostvarivim postupkom koji bi mogao zaobići problem distribucije ključa. 1975. godine otkrili su tada novu vrstu kriptografskog sustava - asimetrični kriptografski sustav.

### 2.3.1. Osnove asimetričnog kriptografskog sustava

Asimertični kriptosustavi zasnivaju se na određenim svojstvima brojeva koja se istražuju u teoriji brojeva. Ideju objašnjava sljedeći primjer. Neka Ana i Ivan komuniciraju kao u primjerima iz prethodnog poglavlja, samo u ovom slučaju Ana stvara samo svoj par ključeva: jedan za kriptiranje i jedan za dektipriptiranje. Ako se pretpostavi da je asimetrično kriptiranje oblik računalne enkripcije, tada je Anin ključ za kriptiranje jedan broj, a ključ za dekriptiranje neki drugi broj. Ana svoj dekripcijski ključ drži u tajnosti te se zbog toga obično naziva **privatnim ključem**. Ona međutim svoj ključ za kriptiranje javno objavljuje tako da je on svakome dostupan. Zbog toga se obično naziva **javni ključ**. Ako Ivan želi Ani poslati poruku,

jednostavno će potražiti njezin javni ključ, koji će biti objavljen u nečemu sličnom telefonskom imeniku. Zatim će Ivan njezinim javnim ključem kriptirati poruku i poslati je. Kada poruka stigne, Ana ju može dekriptirati svojim privatnim ključem. Na isti način bilo tko može Ani poslati kriptiranu poruku. Velika prednost sustava je što on uklanja problem distribucije ključa. Znači čak i ako čitav svijet zna Anin javni ključ za kriptiranje, nitko ne može dekriptirati njime pisanu poruku zbog toga što poznavanje javnog ključa ne pomaže u dekriptiranju. Poruku može dekriptirati samo Ana jer samo ona posjeduje privatni ključ.

Situacija je suprotna onoj koja se susreće kod tradicionalne simetrične enkripcije, u kojoj se Ana mora poprilično namučiti da Ivanu sigurno dopremi enkripcijski ključ. U slučaju upotrebe simetričnog kriptosustava ključ kriptiranja je identičan ključu za dekriptiranje pa Ana i Ivan moraju dobro paziti da taj ključ ne padne u krive ruke.




***Slika 5. Komunikacija upotrebom asimetričnog kriptosustava***

Ako se opet upotrijebi analogija čelične kutije i lokota, asimetrični sustav bi ovako izgledao. Svatko može zaključati lokot jednostavnim pritiskom, no otvoriti ga može samo onaj tko ima ključ. Neka je Ana napravila svoj lokot i ključ za taj lokot, kopirala lokot mnogo puta i podijelila ga poštama diljem svijeta. Kada Ivan želi poslati poruku on ju stavi u kutiju, preuzme lokot od pošte i zatvori ga. Ana primi paket i lako ga otvori (svojim ključem za lokot). Ovdje je pritisak na lokot (zaključavanje) ekvivalentan javnom ključu zato što je lokot dostupan svima. Ključ lokota ekvivaelntan je privatnom ključu, zato što ga posjeduje samo Ana te jedino ona može otvoriti paketi i pročitati poruku. Taj sustav objašnjen pomoću lokota čini se vrlo jednostavnim, ali zadaća pronalaženja matematičke funkcije koja obavlja isti posao, a koja bi se mogla ugraditi u upotrebljiv kriptografski sustav, nije trivijalna. Trebalo je otkriti prikladnu matematičku funkciju koja bi obavljala isti posao kao lokot. Funkcija kriptiranja mora biti takva da iz niza brojeva kriptiranog teksta napadač ne može (ili može samo s iznimnim naporima) odrediti izvorni niz brojeva. Međutim, poznavanje ključa dekriptiranja omogućuje lako izračunavanje izvorne poruke. Odgovor je pronađen u modularnoj aritmetici.

Primjer najčešće korištenog asimetričnog kriptosustava je RSA, čiji su autori Ron Rivest, Adi Shamir i Len Adleman. Još neki primjeri takvih algoritama su ElGamal, NTRUEncrypt, LUC i drugi.

# 3. Diffie-Hellmanov postupak za razmjenu tajnog ključa

Diffie-Hellmanov postupak razmjene ključa je kriptografski protokol koji omogućuje osobama koje se ne poznaju da razmjene simetrični tajni ključ preko nezaštićenog komunikacijskog kanala. Razmijenjeni se ključ kasnije može iskoristiti za kriptiranje poruka upotrebom simetričnog kriptosustava. Simetrični se kriptosustav obično koristi zbog uštede vremena kriptiranja i dekriptiranja. Spomenute se operacije obavljaju mnogo brže u simetričnom kriptosustavu nego u asimetričnom u kojem je brzina kriptiranja i dekriptiranja reda veličine od $10^3$ do $10^5$ bitova u sekundi.

Diffie i Hellman objavili su 1976. godine (dvije godine prije nastanka prvog asimetričnog kriptosustava, RSA) svoj postupak za uspostavu simetričnog kriptosustava između dva partnera. Postupak se zasniva na bitnoj različitosti složenosti izračunavanja modularne potencije i izračunavanja diskretnog logaritma. Diffie i Hellman su bili prvi koji su objavili postupak za razmjenu tajnog ključa potrebnog za kriptiranje poruka upotrebom simetričnog kriptosustava. Postupak uklanja probleme razmjene ključa kriptiranja opisane u poglavljima 2.2 i 2.3.

Koraci Diffie-Hellman protokola su:

- Dva se sudionika na bilo koji način (npr. objava na Internetu) unaprijed dogovore o dva velika broja, $n$ i $g$. Broj $g$ je relativno prost u odnosu na $n$, a najveći zajednički djelitelj im je broj 1: $nzd(g,n)=1$. Najpraktičnije je za $n$ odabrati veliki prosti broj $p$. Brojevi $p$ i $g$ ne moraju biti tajni. Oni se mogu javno objaviti.
- Zatim, korisnik 1, neka je to Ana, odabere veliki nasumični prirodni privatni broj x. Korisnik 2, neka je to Ivan, odabere na isti način svoj privatni tajni broj y.
- Ana, koja želi uspostaviti komunikaciju s Ivanom, šalje rezultat izračunavanja operacije modulo:

$$X = g^x \pmod p.$$

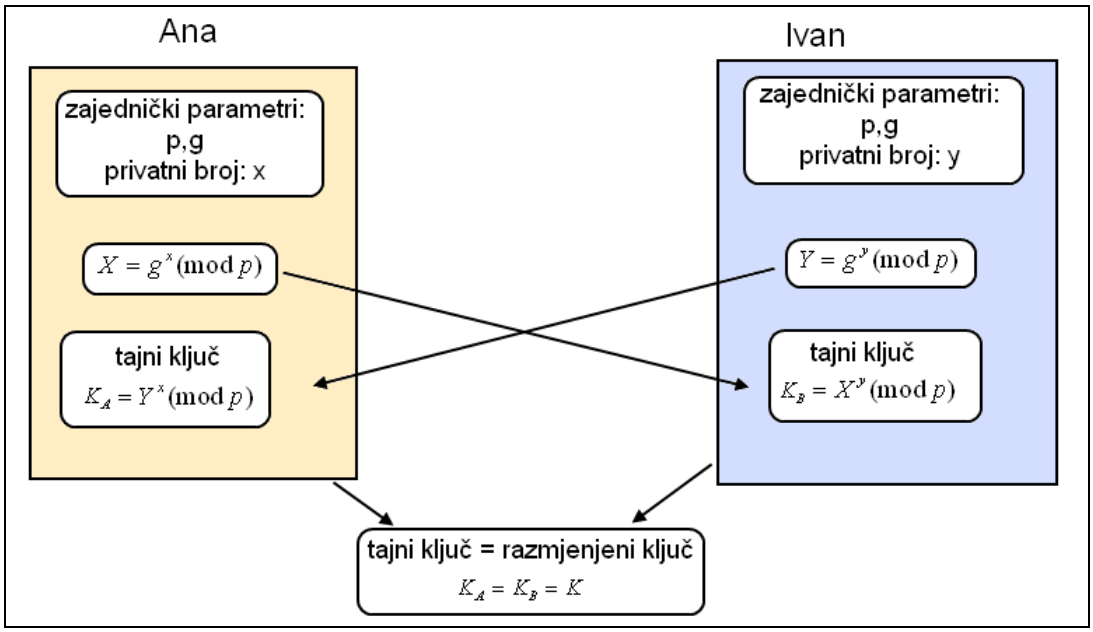
- Pero šalje Ani rezultat izračunavanja operacije modulo te u jednadžbi koristi svoj privatni broj y:

$$Y = g^y \pmod p.$$

- Ana zatim izračunava: $K = Y^x \pmod p = (g^y)^x \pmod p = g^{xy} \pmod p$. Ana je izračunala ključ koji se može koristiti za kriptiranje poruka.
- Slično, Ivan izračunava: $K = X^y \pmod p = (g^x)^y \pmod p = g^{xy} \pmod p$. Pero je također izračunao ključ kriptiranja koji je jednak onom kojeg je i Ana izračunala.
- Kako su ključevi koje su Ana i Pero izračunali jednaki, oni su upravo razmjenili simetrični ključ kriptiranja.

Iz koraka Diffie-Hellmanovog protokola moguće je vidjeti kako za razmjenu ključa kriptiranja uopće nisu potrebni osobni sastanci ili kuriri. Izračunata vrijednost $K$ je tajni ključ koji Ana i Ivan mogu koristiti za simetrično kriptiranje. Čak i ako neki napadač prisluškuje komunikaciju između Ane i Ivana te dozna vrijednosti $g$, $p$, $X$, $Y$, on ne može izračunati ključ $K$, osim ako ne uspije izračunati diskretni logaritam od $X$ ili $Y$. S obzirom da je to vrlo teško, ključ $K$ ostaje tajnim. Dakle, Ana je primjenila svoj privatni ključ x na Ivanovu poruku i izračunala ključ K. Ivan je također primjenio svoj privatni ključ y na Aninu poruku i izračunao ključ K, koji je jednak onom kojeg je izračunala Ana. Na jednostavan način Ana i Ivan sada posjeduju broj koji je poznat samo njima.

Sljedeća slika opisuje razmjenu tajnog ključa upotrebom Diffie-Hellmanovog postupka.




***Slika 6. Razmjena ključa Diffie-Hellmanovim protoko om***

Proučavanjem postupka moguće je uočiti da se Diffie-Hellmanov protokol temelji na asimetričnom kriptosustavu za razmjenu poruka (u ovom slučaju poruka je tajni ključ za kriptiranje).

## 3.1. Primjer razmjene ključeva upotrebom protokola Diffie-Hellman

Zbog jednostavnosti računanja u primjeru će se koristiti mali brojevi. U stvarnosti ti brojevi trebaju biti mnogo veći (barem 1024 okteta) kako napadač ne bi mogao otkriti tajni ključ.

Neka se Ana i Ivan dogovore oko brojeva $p$ = 53 i $g$ = 48. Ana odabire svoj privatni broj x = 36 i pošalje Ivanu:

$$\mathrm{X}=48^{36} \pmod{53} = 49$$

Ivan odabire privatni broj y=40 i šalje Ani:

$$Y = 48^{40} \pmod{53} = 44$$

Nakon toga Ana i Ivan mogu izračunati zajednički ključ. Ana ga računa ovako:

$$K = Y^x \pmod p = 44^{36} \pmod{53} = 49,$$

a Ivan na sljedeći način:

$$K = X^y \pmod p = 49^{40} \pmod{53} = 49.$$

Ana i Ivan su se izračunavanjem ključa K složili da je tajni ključ jednak broju 49.

# 4. Diffie-Hellmanov problem

Objašnjenje zašto Diffie-Hellmanov protokol funkcionira leži u matematičkom problemu kojeg su Diffie i Hellman postavili u kontekstu kriptografije. Taj se problem naziva Diffie-Hellmanov problem. Motivacija za spomenuti problem dolazi iz činjenice da mnogi sigurnosni sustavi koriste matematičke funkcije kojima je vro teško pronaći inverznu funkciju. Kao u primjeru asimetričnog kriptiranja iz poglavlja 2.3.1, kriptiranje poruke je lagano, ali dekriptiranje bez posjedovanja pravog ključa vrlo teško. U slučaju da postoji jednostavno rješenje Diffie-Hellmanovog problema, sigurnosne bi sustave bilo jednostavno ugroziti.

Diffie-Hellmanov problem formalno se postavlja ovako:

*Neka je dan element* $g$ *i vrijednosti* $g^x$ *i* $g^y$*, koja je vrijednost od* $g^{xy}$*?*

Formalno, $g$ je generator neke grupe [6] (obično multiplikative grupe konačnog polja ili grupe eliptične krivulje). Pojam grupe u metematici omogućuje „mjerenje“ simetričnosti nekog skupa u ravnini ili prostoru. x i y su slučajno odabrani prirodni brojevi.

Ako Ana i Ivan koriste Diffie-Hellmanov protokol za razmjenu tajnog ključa i njihovu komunikaciju prisluškuje neka treća osoba, neka je to Petar, on može prisluškivanjem preuzeti vrijednosti $g^x$ i $g^y$ koje razmjenjuju Ana i Ivan kao dio postupka. Ana i Ivan mogu izračunati tajni ključ $g^{xy}$, ali ga Petar može vrlo teško izračunati. Pod izrazom „računarski težak“ smatra se da nije moguće u razumnom vremenu izračunati rezultat.

U kriptografiji se za određene grupe pretpostavlja da je Diffie-Hellmanov problem računarski težak. To se često naziva Diffie-Hellmanovom pretpostavkom. Tokom proteklih nekoliko desetljeća mnogo je ljudi pokušalo rještiti problem, no još uvijek nije objavljeno jednostavno rješenje. Složenost izračuna je velika i zbog toga je sa današnjim računalima gotovo nemoguće u razumnom vremenu izračunati rješenje.

Od 2006. godine najefikasnija metoda za rješavanje problema je rješavanje problema disktetnog logaritma, odnosno pronalaska broja x, ako je poznat $g^x$. Diskretni je logaritam inverzna operacija od diskretnog potenciranja na konačnoj cikličkoj grupi [6]. Ako je dana ciklička grupa G uz definiranu operaciju označenu oznakom $\square$ nad grupom i generator g, potenciranje u G se definira na sljedeći način:

$$g^x = \overbrace{g \square g \square .. \square g}^{x \ puta}$$

Element g se naziva generatorom gupe ako se može koristiti za stvaranje svih elemenata grupe G.

Neka je $d = g^x$, tada je diskretni logaritam od $d$ jednak x:

$$\log_g d = x.$$

Zapravo, diskretni logaritam od $d$ nije jedinstven jer ga se može jedino izračunati upotrebom funkcije modulo reda od g u grupi G. Ako je g generator, kao što je već pretpostavljeno, tada se logaritam pronalazi kao modulo reda grupe. Ako je $n = |g|$, gdje je n red grupe, odnosno broj elemenata grupe, tada je:

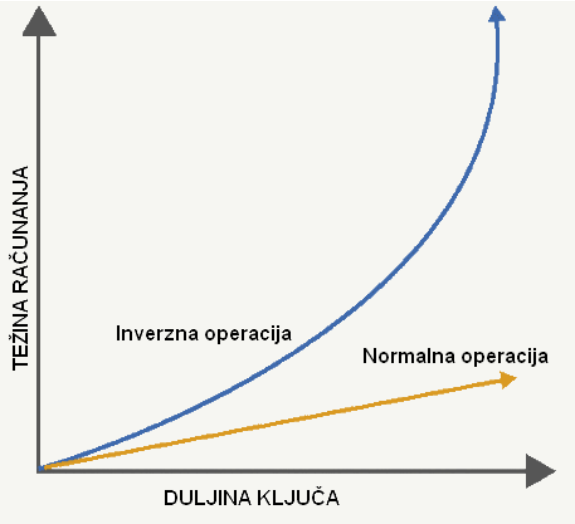
$$\log_g d \equiv x (\mathrm{mod}\, n)$$

Diskretno potenciranje unutar grupe je brzo, obavlja se samo $O(\log x)$ operacija nad grupom, uz upotrebu metode brzog potenciranja [18]. Međutim, mnogo je teže izračunati diskretni logaritam. Sve metode za računanje diskretnih logaritama u svim cikličkim grupama zahtjevaju eksponencijalno vrijeme računanja. Za najbržu metodu potrebno je $O(\sqrt{n})$ operacija. Dokazano je da ako je nad grupom moguće obaviti samo definirane operacije za tu grupu te izračunati inverz, tada su tzv. metode drugog korijena najbolje za pronalazak diskretnog logaritma. Problem diskretnog logaritma važan je zbog raširene primjene u kriptografiji. Prvi koji su upotrijebili taj problem u kriptografiji bili su Diffie i Hellman za svoj protokol razmjene tajnog ključa. Problem računanja diskretnog logaritma bio je samo još jedna matematička zagonetka, dok ga nisu upotrijebili Diffie i Hellman 1976. godine kao temelj

svojeg protokola. U postupku razmjene ključa Diffie-Hellman protokolom, vrijednosti $g^x$ i $g^y$ se javno objavljuju. Diffie-Hellmanov problem kaže da je računarski teško izračunati $g^{xy}$ uz poznavanje vrijednosti $g^x$ i $g^y$. Očigledno, da je jednostavno izračunati diskretne logaritme, tada bi bilo tko mogao lagano izračunati $y = \log_g(g^y)$ i tada $g^{xy} = (g^x)^y$. Nije poznat jednostavan način računanja $g^{xy}$ isključivo iz poznavanja $g^x$ i $g^y$ bez potrebe računanja diskretnih logaritama od x i y.

Otkad je uveden u upotrebu Diffie-Hellmanov protokol, otkriveno je mnogo novih protokola za razmjenu ključeva, asimetrično kriptiranje i digitalno potpisivanje [9] koji svoju sigurnost temelje na težini računanja diskretnog logaritma. Također, u slučaju da postoji jednostavno računanje diskretnih logaritama, to bi značilo da je lagano faktorizirati velike brojeve. Sigurnost asimetričnih kriptosustava ovisi o težini faktoriziranja velikih cijelih brojeva (npr. RSA kod kojeg je uobičajeno da je ključ duljine između 1024 i 2048 bitova). Svi takvi sustavi također ovise i o težini problema diskretnog logaritma.

Postoji nekoliko algoritama za računanje diskretnog logaritma u proizvoljnoj cikličkoj grupi koji rješavaju problem u eksponencijalnom vremenu. Najboljem algoritmu potrebno je $O(\sqrt{n_g})$ operacija nad grupom, gdje je $n_g$ red baze logaritma, g, u grupi. Ako je g generator od G, red grupe je $n = n_g$.




***Slika 7.Usporedba težine računanja normalne operacije i inverzne operacije***

# 5. Diffie-Hellmanov protokol s eliptičnom krivuljom

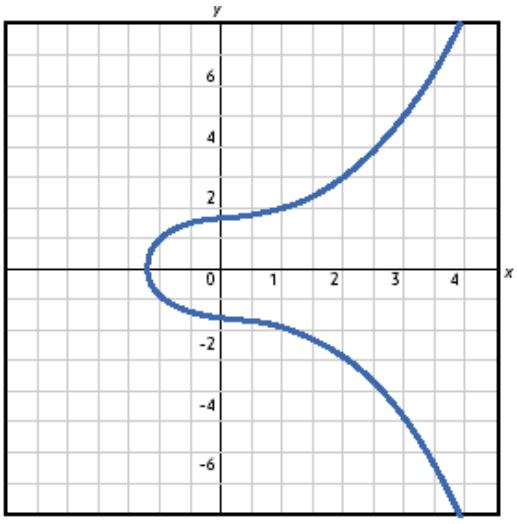
Diffie-Hellman postupak razmjene tajnog ključa s eliptičnom krivuljom je inačica Diffie-Hellmanovog protokola kojim se dvije osobe mogu dogovoriti oko tajnog ključa koji će se upotrebljavati u daljnjoj komunikaciji upotrebom simetričnog kriptosustava putem nezaštićenog komunikacijskog kanala.

## *5.1. Osnove kriptografije eliptičnom krivuljom*

Kriptografija eliptičnom krivuljom je pristup asimetričnoj kriptografiji koji se temelji na algebarskoj strukturi eliptične krivulje nad konačnim poljima. Spomenuti pojmovi su matematička područja koja se istražuju u teoriji brojeva.

Kriptografiju eliptičnom krivuljom otkrili su Victor Miller i Neal Koblitz sredinom osamdesetih. Eliptična krivulja je skup rješenja (x,y) jednadžbe oblika $y^2 = x^3 + ax + b$ te dodatna točka O koja se zove točka u beskonačnosti. Za primjenu u kriptografiji razmatra se konačno polje q elemenata. Ako je q prost broj, polje elemenata su prirodni brojevi dobiveni operacijom modulo q. Pojam polja predstavlja generalizaciju pojma skupa realnih brojeva zajedno s operacijama zbrajanja i množenja realnih brojeva. Primjer konačnog polja je skup $\square_n$ koji je polje onda i samo onda ako je n prost broj: $\square_2 = \{0,1\}, \square_3, \square_5, \square_7, \square_{11}, \square_{13}, \ldots$ Polje $\square_2$ je u ovom slučaju najmanje polje, jer svako polje mora sadržavati barem dva elementa, 0 i 1.

Skup točaka na eliptičnoj krivulji čine grupu s određenim pravilom dodavanja, koje se označava simbolom **+**. Točka O je neutralni element grupe (element koji ne utječe na promjenu rezultata kada se kombinira s ostalim elementima grupe). Kada se uzme u obzir grupa nad konačnim poljem, nužno je da je i grupa konačna (jer ima konačno mnogo točaka).




***Slika 8. Primjer eliptične krivulje***

U kriptografiji s eliptičnom krivuljom, eliptična se krivulja koristi za definiranje elemenata skupa nad kojim se računa grupa, kao i za definiranje operacija među elementima grupe. Neka postoji graf na čijim se osima nalaze brojevi polja $\square_p$, gdje je p prost broj. Prosti brojevi koji se koriste u kriptografiji obično su vrlo veliki pa je teško zamisliti graf takve funkcije. Ako se definira eliptična krivulja takva da se točke P=(x,y) nalaze na krivulji i zadovoljavaju uvjet da su x i y elementi polja $\square_p$, moguće je definirati grupu iz skupa točaka na krivulji. Uz danu točku P i pozitivni prirodni broj n, definira se:

$$[n]P = \overbrace{P + P + \ldots + P}^{n\ puta}.$$

Red točke P jednak je najmanjem pozitivnom prirodnom broju n takvom da je [n]P = O. Grupa stvorena nad točkama P označava se sa < P >, odnosno vrijedi

$$< P > = \{O, P, P+P, P+P+P, \ldots\}$$

Za razliku od grupa nad kojima se definira Diffie-Hellman protokol, elementi skupa nisu brojevi već točke. Rezultirajući će sustav ipak biti sličan aritmetičkom sustavu korištenom za asimetrične kriptosustave bez eliptičnih krivulja. Postoji skup elemenata (u ovom slučaju točaka) i kada se obavljaju aritmetičke operacije nad njima, postoje pravila po kojima se dobiva rezultat operacija (slično kao operacije u modularnoj aritmetici koja se koristi za Diffie-Hellmanov protokol). Spomenuta pravila još uvijek slijede mnoga opće poznata pravila aritmetike, kao što su zbrajanje i množenje.

Sigurnost kriptografije eliptičnom krivuljom oslanja se na problem diskretnog logaritma eliptične krivulje. Neka je E eliptična krivulja nad konačnim poljem $\square_p$. Neka je P jedna točka na krivulji E i neka je Q točka u grupi < P >. Potrebno je pronaći broj t takav da vrijedi Q = [t] P. Vrijedi opće uvjerenje da je problem diskretnog logaritma eliptične krivulje računarski teško rješiv kada točku P čine veliki prosti brojevi. Postoji nekoliko metoda za rješavanje navedenog problema i to su:

- Pohling-Hellmanov algoritam
- Shanksova metoda mali-korak-veliki-korak (baby-step-giant-step)
- Frey-Rueckov napad upotrebom Teteovog uparivanja
- Napadi na eliptične krivulje s anomalijama
- Pollardove metode, rho metoda i kangaroo metoda
- Weilov spust (za neka posebna konačna polja) [12][13]

Zbog postojanja Pohling-Hellmanovog algoritma, uvijek se ograničava na slučaj kada su elementi točke P veliki prosti brojevi. Tada su jedini primjenjivi algoritmi Shanksova i Pollardova metoda, ali te metode imaju eksponencijalnu složenost, što znači da ne rješavaju problem u razumnom vremenu. Asimetrični kriptosustavi koji koriste eliptične krivulje analogni su sustavima koji se temelje na problemu diskretnog logaritma (kao što je upravo i Diffie-Hellmanov protokol). Sigurnost kriptosustava s eliptičnom krivuljom temelji se na srodnim problemima, kao što je Diffie-Hellmanov problem i problem rješavanja diskretnog logaritma.

## *5.2. Diffie-Hellmanov protokol s eliptičnom krivuljom*

Kada se koristi kriptografija temeljena na eliptičnim krivuljama, sve se osobe koje žele komunicirati kriptiranim porukama moraju dogovoriti oko parametara koji definiraju eliptičnu krivulju, odnosno o domenskim parametrima postupka. Neka je konačno polje definirano oznakom $\square_p$ u slučaju da se koriste prosti brojevi. Eliptičnu krivulju definiraju konstante *a* i *b* koje se koriste u jednadžbi eliptične krivulje. U postupku je potrebno definirati i cikličnu grupu čiji je generator (npr. bazna točka) označen sa P. Za primjenu u kriptografiji red generatora P, odnosno najmanjeg nenegativnog broja n takvog da je nP=O, mora biti prost. U slučaju kada se koriste prosti brojevi, domenski parametri su (p,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. Osim ako postoji uvjerenje da je domenske parametre generirala stranka od povjerenja u smislu njezine upotrebe, domenski se parametri moraju validirati prije upotrebe, što znači potvrditi da su ih generirale osobe koje žele komunicirati.

Uobičajeno je da odabir domenskih parametara ne obavljaju osobe koje žele komunicirati jer proces uključuje prebrojavanje točaka koje se nalaze na eliptičnoj krivulji (što je posao koji uzima mnogo vremena i nije ga lako implementirati). Zbog toga postoje organizacije koje objavljuju domenske parametre eliptičnih krivulja za polja poznatih veličina. Neke od njih su:

- NIST, Recommended Elliptic Curves for Government Use i
- SECG, SEC 2: Recommended Elliptic Curve Domain Parameters

Ukoliko netko ipak želi sam odabrati domenske parametre potrebno je odabrati konačno polje te zatim koristiti neku od strategija za odabir krivulje s primjerenim brojem točaka upotrebom jedne od sljedećih metoda:

- odabir slučajne krivulje i upotreba algoritma općenitog brojanja točaka, na primjer Schoofov algoritam[10] ili Schoof-Elkies-Atkinov algoritam [11],

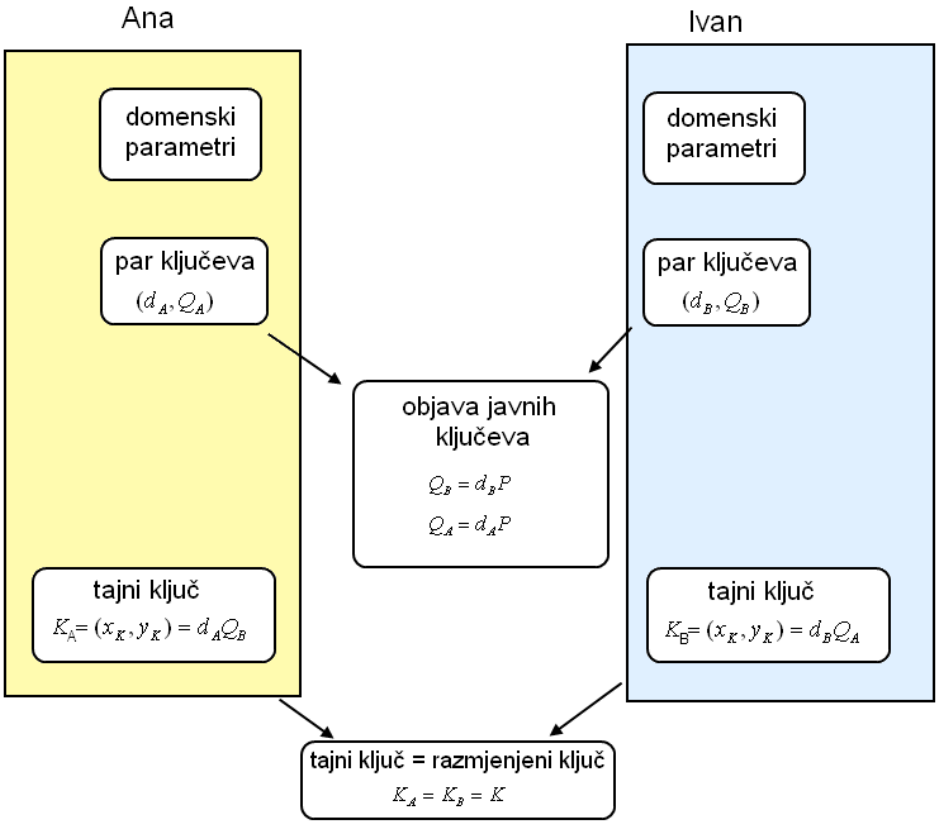
- odabir slučajne krivulje iz skupa nad kojimje lagano izračunati broj točaka, na primjer Koblitzove krivulje
- odabir broja točaka i generiranje krivulje s tim brojem točaka upotrebom tehnike kompleksnog množenja [14]

Pri odabiru domenskih parametara treba izbjegavati neke krivulje i polja [12][13][14][15][16][17].

Protokol će biti objašnjen na primjeru komunikacije dvije osobe, Ane i Ivana. Neka Ana želi razmjeniti tajni ključ s Ivanom, ali jedini komunikacijski kanal koji im je dostupan je javan i postoji mogućnost prisluškivanja. Koraci postupka su sljedeći:

- prvo je potreban dogovor oko domenskih parametara između Ane i Ivana.
- Ana i Ivan moraju odabrati par ključeva prikladnih za kriptografiju eliptičnom krivuljom. Par ključeva koji svaki treba odabrati su privatni ključ d, slučajno odabran broj iz intervala [1,n-1], i javni ključ Q, gdje je Q=dP. Neka par ključeva koje odabire Ana bude $(d_A, Q_A)$ i par ključeva koje odabire Ivan $(d_B, Q_B)$. Ana i Ivan objavljuju svoje javne ključeve.
- Ana računa $K = (x_K, y_K) = d_A Q_B$ i Ivan računa $K = (x_K, y_K) = d_B Q_A$, iz čega slijedi da je razmjenjeni ključ K

Točku K koju Ana i Ivan računaju jednaka je zbog toga što je $d_A Q_B = d_A d_B P = d_B d_A P = d_B Q_A$.




***Slika 9. Razmjena ključa Diffie-Hellmanovim protokolom s eliptičnom krivuljom***

Protokol je siguran jer su jedini podaci koji su objavljeni javni ključevi i osoba koja prisluškuje promet ne može otkriti privatni ključ (osim ako ne uspije riješiti problem diskretnog logaritma eliptične krivulje, što nije moguće u realnom vremenu).

# 6. Primjena Diffie-Hellmanovog protokola

Diffie-Hellmanov protokol je postupak koji osigurava razmjenu tajnog ključa kriptiranja putem nezaštićenog komunikacijskog kanala. Kao takav, ima raširenu upotrebu u mrežnim protokolima koji omogućuju zaštićenu komunikaciju. Koristi se:

- kod autentikacije u mrežama računala,
- u IPsec (eng. IP security) protokolu,
- unutar IKE (eng. Internet Key Exchange) strukture,
- SSH i TLS protokolima te
- u postupku stvaranja digitalnih potpisa i digitalnih certifikata.

Autentikacija je postupak provjere osobe ili računala s kojim se komunicira u smislu da se ne predstavlja lažno. Provjera identiteta udaljenog procesa je postupak za koji su potrebni kompleksni protokoli temeljeni na kriptografiji. Postoji mnogo autentikacijskih protokola koji se koriste na nezaštićenom kanalu. Općeniti model koji svi autentikacijski protokoli koriste dan je sljedećim primjerom. Ana počne slati poruku Ivanu ili provjerenom KDC-u (eng. Key Distribution Center). Slijedi izmjena nekoliko poruka. Tokom slanja poruka Petar može presresti poruke, izmjeniti ih ili odgovoriti na njih kako bi prekinuo ili ometao komunikaciju Ane i Ivana. Međutim, kada postupak protokola završi Ana i Ivan su sigurni da im se u komunikaciju nije ubacio uljez. U većini protokola za autentikaciju uspostavlja se tajni sjednički ključ za upotrebu u razgovoru. U praksi, zbog zahtjeva na karakteristike izvedbe, sav podatkovni promet je kriptiran upotrebom simetričnog kriptosustava. Razmjena simetričnog tajnog ključa obično se obavlja prema Diffie-Hallmanovom protokolu.

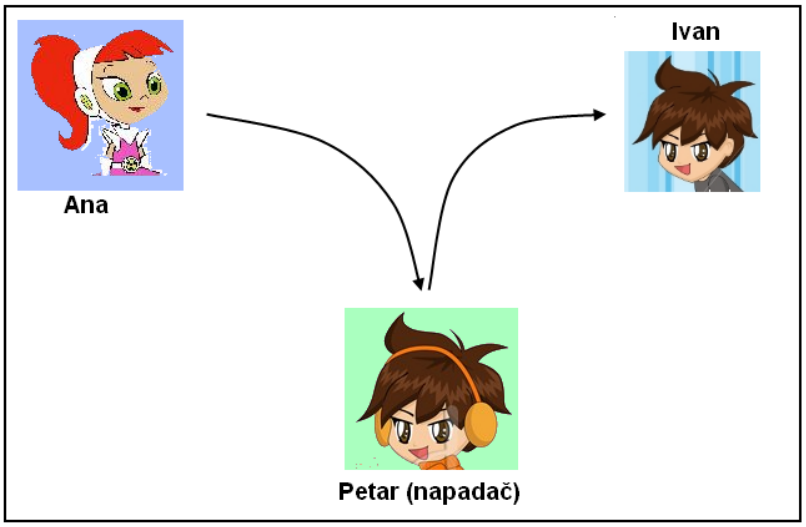
IPsec je standard i skup protokola koji obuhvaća mehanizme za zaštitu mrežnog prometa na razini trećeg sloja OSI modela, kriptiranjem i/ili autentikacijom IP paketa. IPsec uključuje protokole za uspostavu međusobne autentikacije računala ili procesa na početku sjednice i za dogovor kriptografskog sjedničkog ključa koji će se koristiti tokom sjednice. Sjednički ključ je tajni ključ kojim se kriptiraju poruke koje se razmjenjuju tokom trajanja sjednice. IPsec se može koristiti za zaštitu toka podataka između korisnika i poslužitelja, usmjerivača (eng. router) i vatrozida (enf. firewall). Zaštitni mehanizmi IPsec protokola se između ostalog zasnivaju na protokolima za razmjenu ključeva, kao što je IKE protokol. Ti protokoli obično koriste Diffie-Hellmanov postupak za razmjenu tajnog ključa koji se dalje koristi kao sjednički ključ.

SSH (eng. Secure Shell) protokol ili skup pravila za sigurnu prijavu na udaljeno računalo se uglavnom koristi na računalima s operacijskim sustavima Unix/Linux za udaljeni konzolni pristup (eng. shell account access). Osmišljen je kao zamjena za Telnet i druge nezaštićene protokole za ostvarivanje udaljene ljuske koje šalju informacije (poput lozinke) u jasnom tekstu. Kriptiranje koje koristi SSH osigurava povjerljivost i integritet podataka koji se šalju putem nezaštićene mreže, kao što je Internet. SSH protokol koristi Diffie-Hellmanov postupak za razmjenu ključeva.

Digitalni potpisi obično koriste asimetričnu kriptografiju, odnosno algoritme kao što je RSA, ali postoje i potpisi koji se temelje na Diffie-Hellmanovom protokolu. Digitalnim potpisom (eng. digital signature - DS) se utvrđuje autentičnost elektroničkih dokumenata, kao što su elektroničko pismo, web stranica ili slika. Dokument je autentičan ako je poznat njegov autor i ako je moguće dokazati da nije neovlašteno izmijenjen. Vjerodostojnost (eng. authentication) potpisanih dokumenata provjerava se upotrebom kriptografskih metoda. Osim u digitalnom potpisu, Diffie-Hellmanov postupak moguće je koristiti i u postupku stvaranja digitalnih certifikata. Digitalni certifikat je elektronički dokument koji utvrđuje identitet i autenticira korisnika kada obavlja određene transakcije na Internetu. Certifikati koriste digitalne potpise za povezivanje javnih ključeva s podacima o identitetu vlasnika, kao što su ime osobe ili organizacije, adresa i sl., i time sprečavaju neovlaštenu izmjenu podataka.

# 7. Napadi na protokol Diffie-Hellman

U poglavljima 3 i 5.2 opisane su dvije inačice Diffie-Hellmanovog protokola. Obje se inačice temelje na pretpostavci da je vrlo teško u razumnom vremenu rješiti problem računanja diskretnog logaritma te problem diskretnog logaritma eliptične krivulje. Iako se na temelju spomenutih problema pretpostavlja da je Diffie-Hellmanov protokol siguran, postoji jedna ranjivost. Postupak je osjetljiv na napade kada uljez može presresti poruke koje šalju korisnici (u primjeru Ana i Ivan) i nadomjestiti ih svojim porukama. Takav se napad naziva *napad s čovjekom u sredini* (eng. man in the middle).




***Slika 10. Napad s čovjekom u sredini***

## *7.1. Primjer napada s čovjekom u sredini*

Neka napadač odabere nasumični broj z i poznavajući objavljene brojeve p i g izračuna:

$$Z = g^z \pmod p$$

Kada Ana pošalje vrijednost X, napadač pohrani tu vrijednost i pošalje Ivanu vrijednost Z. Jednako tako uljez presretne Ivanovu poruku Y, zadrži ju za sebe i Ani pošalje poruku Z. Ana i Ivan misle da su dobili informacije jedan od drugoga, ali u stvarnosti dobili su poruke od napadača.

Napadač izračunava ključeve $K_A$ i $K_B$:

$$K_A = X^z \pmod p = (g^x)^z \pmod p = g^{xz} \pmod p$$
$$K_B = Y^z \pmod p = (g^y)^z \pmod p = g^{yz} \pmod p$$

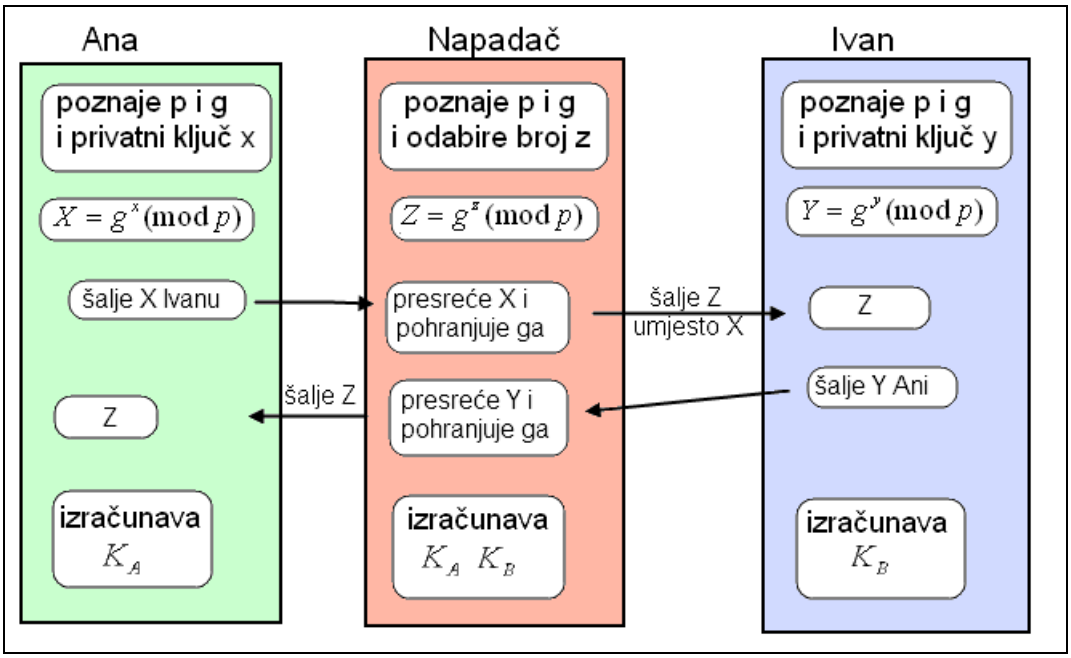
Ana izračunava ključ

$$K_A = Z^x \pmod p = (g^z)^x \pmod p = g^{xz} \pmod p$$

i Ivan izračunava ključ

$$K_B = Z^y \pmod p = (g^z)^y \pmod p = g^{yz} \pmod p .$$

Ako nakon razmjene ključeva Ana i Ivan nastave komunicirati koristeći izračunate tajne ključeve, napadač može naruštiti tajnost i besprijekornost komuniciranja.




***Slika 11.Napad s čovjekom u sredini***

Nakon ovakve razmjene ključeva, kada Ana šalje kriptiranu poruku $M_1 = E(T, K_A)$, gdje je T jasni tekst, napadač ju presretne i dekriptira te saznaje sadržaj poruke $T = D(M_1, K_A) = D(E(T, K_A), K_A)$. Napadač sada može tekst T ili neki izmišljeni tekst T' kriptirati i poslati Ivanu poruku $M_2 = E(T', K_B)$. Ivan misli da je dobio poruku od Ane i svojim ključem $K_B$ dekriptira poruku te dobiva $T' = D(M_2, K_B) = D(E(T', K_B), K_B)$.

Na isti je način moguće ostvariti tok informacija u suprotnom smjeru. Ana i Ivan neće otkriti da se u njihovu komunikaciju umiješao napadač - čovjek u sredini. Dakle, ovakve i slične razmjene ključeva potrebno je dodatno zaštititi postupkom autentikacije sudionika u komunikaciji.

## 7.2. Dobre navike prilikom upotrebe kriptirane komunikacije

Diffie-Hellmanov protokol se može postaviti tako da se poboljša otpornost na napade grubom silom (eng. brute force), odnosno izračunavanje diskretnog logaritma. Vrijednosti p i g se javno objavljuju. Postoje dva načina upotrebe Diffie-Hellmanovog protokola, u ovisnosti o tome koriste li se odabrane vrijednosti p i g samo jednom u komunikaciji ili više puta. Ključevi koji se koriste više puta sa istim p i g vrijednostima nazivaju se statičnim ključevima. 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 ključ. Prednost privremenog ključa jest da se može odbaciti i trajno obrisati, tako da čak i u slučaju da napadač neovlašteno preuzme nadzor nad računalom na kojem misli da se nalazi ključ, on neće uspjeti otkriti razmijenjeni ključ. Osim toga, pošiljatelj i primatelj mogu kombinirati upotrebu statičnog i privremenog ključa tokom razmjene tajnog ključa Diffie-Hellmanovim protokolom. Na primjer pošiljatelj može koristiti privremeni ključ, a primatelj statični.

Osim odabira statičnog i privremenog ključa, korisnici trebaju paziti pri odabiru veličine broja p i privatnog ključa. Općenito, napadaču je jednostavnije izvesti napad na broj p nego na privatni ključ. To znači da je potrebno odabrati broj p koji sadrži mnogo više bitova od privatnog ključa. Uz to, privatni ključ bi trebao biti dva puta „bitovno duži“ (sadržavati najmanje dvostruko više bitova) od ključa koji se razmjenjuje. Treba imati na umu da 1024 bitni prosti broj p ima efektivnu dužinu od 160 bitova u privatnom ključu. To znači da, ako privatni ključ treba biti 2 puta duži od tajnog ključa, moguće je sigurno razmijeniti ključ duljine 80 bitova. Napad grubom silom na takav ključ zahtjeva računanje $2^{80}$ mogućnosti. Uz dovoljno velik budžet, takav ključ se može izračunati za sat vremena. Prema tome ovisno o potrebnoj razini zaštite komunikacije potrebno je odabrati broj p i privatni ključ veće dužine (na primjer broj p dužine 2048 bitova).

Općenito protokoli koji koriste Diffie-Hellmanov protokol obično imaju dodatnu zaštitu za sprečavanje napada s čovjekom u sredini. Na primjer SSL protokol na početku razgovora, odnosno razmjene poruka zahtjeva autentikaciju pošiljatelja i primatelja.

Kako bi se spriječio napad s čovjekom u sredini na Diffie-Hallmanov protokol, Diffie, van Oorschot i Wiener su 1992. [19] razvili autenticirani Diffie-Hallmanov protokol, ili STS (eng. Station-to-Station) protokol. Otpornost na napad se postiže autenticiranjem pošiljatelja i primatelja upotrebom digitalnih potpisa i certifikata. Ideja je sljedeća, dvije osobe, Ana i Ivan, posjeduju svoje parove ključeva (privatni i javni ključ) i certifikat za javni ključ. U tijeku protokola, Ana stavlja digitalni potpis na poruke i šalje Ivanu vrijednost X zajedno sa njezinim digitalnim potpisom i certifikatom javnog ključa. Ivan učini slično sa svojim vrijednostima. Sada, čak i u slučaju da napadač može presretati poruke između Ane i Ivana, on ne može lažirati digitalni potpis bez Aninog privatnog ključa i Ivanovog privatnog ključa. Prema tome, autenticirani protokol je siguran od napada s čovjekom u sredini.

# 8. Zaključak

Objava protokola za razmjenu tajnog ključa kojeg su smislili Diffie i Hellman označila je prekretnicu u komunikaciji kriptiranim porukama. Riješili su stoljećima stari problem i dali osnove asimetrične kriptografije. Postoji nekoliko inačica protokola, od kojih su najpoznatije osnovna i inačica u kojoj se koristi eliptična krivulja. Sigurnost protokola se temelji na eksponencijalnoj složenosti izračunavanja diskretnog logaritma za velike brojeve. Temelj sigurnosti protokola dakle leži u teoriji brojeva. Zbog težine računanja diskretnog logaritma ukoliko se koristi dovoljno veliki prosti brojevi nije moguće, uz postojeću tehnologiju, u razumnom vremenu grubom silom (eng. brute force) izvesti uspješan napad na Diffie-Hellmanov protokol. Diffie-Hellmanov protokol ima jednu ranjivost, a to je nedostatak autentikacije sudionika. Zbog toga je moguće izvesti napad s čovjekom u sredini. Ukoliko se žele spriječiti takvi napadi potrebno je prvo provesti autentikaciju osoba ili računala koji razmjenjuju ključeve. Protokol ima raširenu upotrebu i čini temelj zaštite komunikacije putem otvorenih komunikacjiskih kanala, kao što je Internet. Koristi se za uspostavu sigurne komunikacije i razmjenu ključeva u mrežama računala.

Dakle, Diffie-Hellmanov protokol ušao je u povijest kao jedan od najznačajnijih jer je omogućio sigurnu razmjenu tajnog ključa simetričnih kriptosustava te riješio problem star preko dvije tisuće godina. Iako se provode stalna istraživanja u području razmjene ključeva, Diffie-Hellmanov protokol još uvijek ostaje u upotrebi kao jedino rješenje za razmjenu tajnih ključeva u kriptografskim sustavima.

# 9. Reference

[1] W.Diffie, M.E. Hellman, „New Directions in Cryptography“, IEEE Transactions on Information Theory, IT-22,n.6,studeni 1976, pp 644-654

[2] C. Studholme, The discrete logarithm problem, lipanj 2002, http://www.cs.toronto.edu/~cvs/dlog

[3] A.J. Menezes, P.C. van Oorschot,S.A. Vanstone , Handbook of applied cryptography, listopad 1996, http://www.cacr.math.uwaterloo.ca/hac/

[4] D.Hankerson, A.J.Menezes, S.A.Vanstone, Guide to eliptic curve cryptography, Springer, 2004.

[5] S.Singh, TheC ode Book, Doubleday of New York, 1999.

[6] D.Žubrinić, Diskretna matematika, ELEMENT, 2001.

[7] Diffie-Hellman key exchange, http://www.netip.com/articles/keith/diffie-helman.htm, kolovoz 2006.

[8] A.S. Tannenbaum, Computer networks, Prentice Hall, ožujak 2003.

[9] Digitalni potpis, http://www.cert.hr/documents.php?id=275, CERT veljača 2007.

[10] Schoofov algoritam, http://en.wikipedia.org/wiki/Schoof%27s_algorithm

[11] Schoof–Elkies–Atkinov algoritam, http://en.wikipedia.org/wiki/Schoof%E2%80%93Elkies%E2%80%93Atkin_algorithm

[12] S.D. Galbraith, N.P. Smart, A cryptographic application of the Weil descent, Cryptography and Coding, 1999.

[13] P. Gaudry, F. Hess, N.P. Smart, Constructive and destructive facets of Weil descent on elliptic curves, Hewlett Packard Laboratories Technical Report, 2000.

[14] G. Lay, H. Zimmer, Constructing elliptic curves with given group order over large finite fields, Algorithmic Number Theory Symposium, 1994.

[15] I. Semaev, Evaluation of discrete logarithm in a group of P-torsion points of an elliptic curve in characteristic P, Mathematics of Computation, number 67, 1998.

[16] N. Smart, The discrete logarithm problem on elliptic curves of trace one, Journal of Cryptology, Volume 12, 1999.

[17] T. Satoh and K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, Commentarii Mathematici Universitatis Sancti Pauli, Volume 47, 1998.

[18] D.M. Gordon, A Survey of Fast Exponentiation Methods,Journal of Algorithms ,1997.

[19] Diffie, W.; van Oorschot, P. C.; Wiener, M. J. (1992), "Authentication and Authenticated Key Exchanges", *Designs, Codes and Cryptography* (Kluwer Academic Publishers) **2**: 107–125