Primjena kriptografije u inteligentnim transportnim sustavima

Zirdum, Jure

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

ZAVRŠNI RAD

Primjena kriptografije u inteligentnim transportnim sustavima

Application of Cryptography in Intelligent Transport Systems

Mentor: izv. prof. dr. sc. Pero Škorput

Student: Jure Zirdum, 0246084611

Zagreb, srpanj 2023.

SVEUČILIŠTE U ZAGREBU FAKULTET PROMETNIH ZNANOSTI

ODBOR ZA ZAVRŠNI RAD

Zagreb, 24. lipnja 2023.

Zavod: **Zavod za inteligentne transportne sustave**
Predmet: **Računalna sigurnost**

ZAVRŠNI ZADATAK

Pristupnik: Jure Zirdum (0246084611)
Studij: Inteligentni transportni sustavi i logistika
Smjer: Inteligentni transportni sustavi

Zadatak: **Primjena kriptografije u inteligentnim transportnim sustavima**

Opis zadatka:

Kriptografija ima važnu primjenu u inteligentnim transportnim sustavima kako bi se osigurala sigurnost i privatnost podataka koji se razmjenjuju u tim sustavima. Kriptografski algoritmi se koriste za šifriranje osjetljivih informacija, poput lokacija vozila, putničkih podataka ili komunikacije između različitih dijelova sustava.

Ovim se osigurava da samo ovlašteni sudionici mogu pristupiti i razumjeti te podatke, dok se neovlaštenima onemogućuje pristup i manipulacija. Rad analizira različite vrste kriptografskih algoritama i protokola koji se koriste za osiguravanje povjerljivosti, integriteta i autentičnosti podataka u prometu unutar sustava.

Zadatak uručen pristupniku: 21. travnja 2023.
Rok za predaju rada: 26. lipnja 2023

Mentor:

izv. prof. dr. sc. Pero Škorput

Predsjednik povjerenstva za završni ispit:

Sažetak:

Ovaj rad bavi se problematikom primjene kriptografskih sustava u inteligentnim transportnim sustavima s ciljem efikasnije i bolje zaštite podataka ili informacija. Korištenjem kriptografskih tehnika poput digitalnih potpisa, simetričnog i asimetričnog šifriranja te hash funkcija postiže se sigurnost i pouzdanost sustava.

Primjena kriptografije u inteligentnim transportnim sustavima omogućava povjerljivost, autentičnost te integritet podataka koristeći se standardiziranim i sigurnim algoritmima za šifriranje i dešifriranje.

KLJUČNE RIJEČI: Kriptografija; Inteligentni transportni sustavi; Sigurnost podataka; Zaštita privatnosti; Šifriranje

Summary:

This paper deals with the issue of the application of cryptographic systems in intelligent transport systems with the aim of more efficient and better protection of data or information during communication. By using cryptographic techniques such as digital signatures, symmetric and asymmetric encryption and the hash functions, it achieves the security and reliability of the system.

The application of cryptography in intelligent transport systems enables the confidentiality, authenticity and integrity of data by using standardized and secure encryption and decryption algorithms.

KEY WORDS: Cryptography; Intelligent transport systems; Data security; Privacy protection; Encryption

SADRŽAJ

1. UVOD

Inteligentni transportni sustavi (Intelligent Transportation Systems - ITS) postaju sve raširenija i kompleksniji sustav koji uz korištenje raznih naprednih tehnologija, moraju osigurati sigurnost i integritet podataka. Ulogu za povjerljivost, integritet, autentičnost podataka preuzima kriptografija stvarajući tako temelje za naprednije i sigurnije sustave koji imaju za cilj poboljšati učinkovitost te iskustvo korisnika u prometu.

Kako bismo shvatili značajnost primjene kriptografije u inteligentnim transportnim sustavima analizirat će se razni primjeri upotrebe kriptografije u prometu. Istaknut će se prednosti i mane te definirati razna pravila i norme kako bi se izbjegli razni propusti u komunikaciji odnosno u pohrani osjetljivih podataka.

Rad se sastoji od osam poglavlja, a to su:

1. Uvod
2. Sigurnosni izazovi u inteligentnim transportnim sustavima
3. Kriptografske sustavi i metode
4. Sustavi autentifikacije i autorizacije u inteligentnim transportnim sustavima
5. Privatnost i zaštita podataka u inteligentnim transportnim sustavima
6. Kriptografski standardi i norme u inteligentnim transportnim sustavima
7. Analiza praktičnih primjera primjene kriptografije u području inteligentnih transportnih sustava
8. Zaključak

Rad se sastoji od 8 poglavlja. Prvo se analiziraju sigurnosni izazovi u inteligentnim transportnim sustavima te mogući napadi i kako ih spriječiti. Zatim se analiziraju kriptografski sustavi i metode koji su najefikasniji te najsigurniji i pravilno zadani za korištenje prilikom prijenosa ili čuvanja podataka. Nakon razmatranja kriptografskih sustava obrađuju se sustavi autentifikacije i autorizacije raznih prometnih entiteta poput korisnika i vozila. Zatim se obrađuju razne strategije privatnosti i zaštite podataka kako bi sustav bio što sigurniji, te se govori o raznim trendovima i regulacijama koje su od velike pomoći u današnjim sustavim zaštite. Kako bi metode funkcionirale za sve sustave visoke sigurnosti, moraju se poštivati kriptografski standardi i norme koje su navedene u radu. Na kraju se analiziraju praktični primjeri primjene kriptografije u području inteligentnih transportnih sustava te se dokazuje funkcionalnost pojedinih sustava.

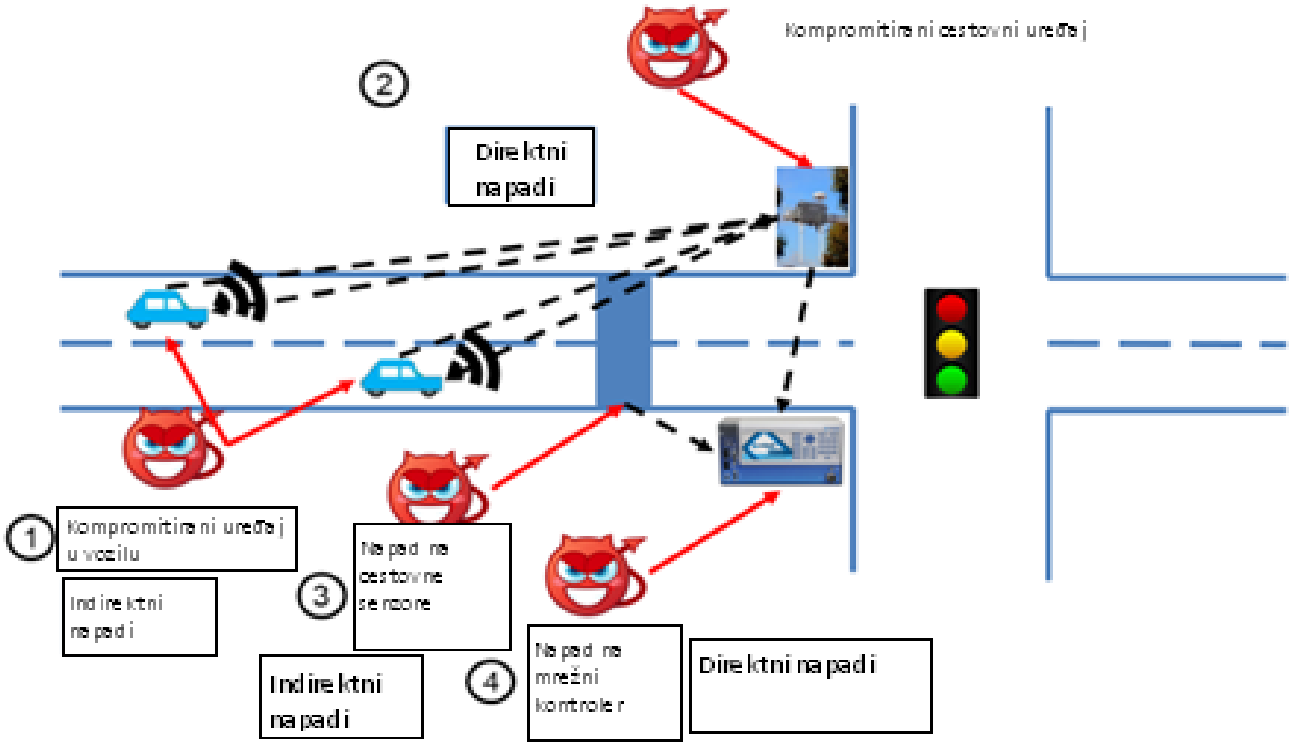
2. SIGURNOSNI IZAZOVI U INTELIGENTNIM TRANSPORTNIM SUSTAVIMA

Inteligentni transportni sustavi koriste razne vještine, senzore i komponente kako bi se na što efikasniji i na što sigurniji način moglo prometovati određenim gradom. Korištenjem senzora i raznih komponenata kojima je prioritet poslati informaciji odnosno primiti istu pojavljuje se veliki sigurnosni rizik od krađe tih istih podataka te manipulacijom istih kako bi se potencijalno narušila sigurnosti u prometu. Kako bi se spriječili takvi pokušaji krađe i narušavanja sigurnosti potrebno je unaprijed definirati određena pravila odnosno protokole kako bi se zaštitili podatci. Određivanje pravila naravno ovisi o vrsti podataka, jesu li to privatni podatci, koji moraju biti šifrirani te ne smiju biti vidljivi ili su to javni podatci, koji smiju biti vidljivi a pretežito se radi o podacima o informiranju putnika, stanju na cesti itd. Još uvijek nije potpuno jasno koje se vrste kibernetičkih napada mogu izvršiti putem komunikacija, infrastruktura – infrastruktura (I2I) i vozilo – infrastruktura (V2I), i mogu li takvi napadi rezultirati kritičnim kvarom sustava. Pošto se sve više senzora i drugih upravljačkih komponenti ugrađuje u prometnice, potrebno je voditi računa i o pohrani tih istih podataka, naravno takvih podataka je iznimno puno i nije ih moguće pohranjivati direktno na mjestu prikupljanja te poseže za novim rješenjem koje naravno donosi određene rizike i mjere odnosno standarde[1]. Trend Cloud Computinga brzo raste i ima tehnološku vezu sa Grid Computingom, Utility Computingom te distribuiranim računalstvom.

Neki od pružatelja usluga oblaka su Amazonove web usluge (Amazon Web Services - AWS), *Microsoft Azure*, *Google Cloud Platform* (GCP) itd. Podatci prikupljeni sa raznih senzora također se mogu pohranjivati u baze podataka, to su jedan od najčešće korištenih načina pohrane, zatim Data Warehouse sustavi, takvi sustavi omogućuju agregaciju različitih podataka sa različitih senzora odnosno sustava, te omogućuju lakšu analizu i prikaz izvještaja, te lokalno pohranjivanje koje se koristi u nekim specifičnim situacijama odnosno slučajevima, podatci se pohranjuju na samom uređaju. Kako bi podatak sa senzora uspješno stigao do oblaka ili baza podataka moramo definirati neke određene korake:

1. Prikupljanje podataka – Mehanizmi za prikupljanje podataka o prometu mogu se kategorizirati u dvije metode, poznate kao nametljiva i nenametljiva metoda. Nametljiva metoda uključuje pneumatske cestovne cijevi, indukcijsku ili magnetsku petlju dok nenametljiva metoda koristi ručno prebrojavanje.
2. Prijenos podataka – Prikupljeni podatci prenose se sa senzora na centralni sustav ili bazu podataka putem bežičnih komunikacijskih tehnologija kao što su bežična lokalna mreža (Wireless Fidelity – Wi – Fi), mobilna mreža (4G ili 5G), Bluetootha ili mreže velikog dometa širokog područja (Long Range Wide Area Network – LoRaWAN).
3. Pohrana podataka – Dolazni podatci se pohranjuju u baze podataka, te se strukturiraju i zapisuju u određene retke i stupce.

4. Obrada i analiza podataka – Pohranjeni podatci se zatim obrađuju primjenom algoritama strojnog učenja i analitičkim metodama kako bi se mogli generirati izvještaji i kako bi dobili uvid u stanje na određenoj prometnici



Slika 1. Primjer upotrebe tehnika za obradu podataka prilikom komunikacije vozila s cestovnim komponentama, [1].

Na slici se mogu vidjeti mogući napadi na prometne entitete i prometnu infrastrukturu. Vrlo bitan aspekt sigurnosti podataka odnosi se na mrežne protokole koje koriste kako bi ti podatci sigurno stigli na odredište. Mrežni protokoli su pravila koja upravljaju komunikacijom između uređaja unutar računalne mreže [1]. Takva pravila uključuju procedure i upute koje omogućuju uređajima da se mogu međusobno povezati i identificirati, te uključuju i pravila oblikovanja koja omogućuju oblikovanja poruke koja zatim omogućuje hoće li se podatak primiti ili odbiti te omogućuje pakiranje i raspakiravanje poruka u cijelosti. Tijekom komunikacije između računala unutar mreže podaci se na izvoru rastavljaju u podatkovne pakete koji se kasnije ponovno sastavljaju na odredištu [1]. Postoje razne tehnike komutacije paketa koje to omogućuju i brojni protokoli koji su razvijeni kako bi omogućili komunikaciju prema različitim kategorijama.

2.1 PROTOKOLI ZA PRIJENOS PODATAKA

1. Internetski protokol (Internet Protocol – IP) – Internetski protokol standard odnosno skup pravila za funkcionalnosti uređaja koji su povezani na internet. Informacije o IP adresi dostupni su u svakom paketu i uz pomoć njih usmjerivači su u mogućnosti poslati zadani paket na pravo mjesto [2].
   - IP adresiranje: omogućava da svaki uređaj koji je povezan na mrežu ima svoju jedinstvenu IP adresu. To omogućava odrediti izvor i odredište za podatke koje prenosimo.
   - IP usmjeravanje: Usmjeravanje se odnosi na određivanje puteva kojima želimo da se naši podatci kreću do odredišta.

2. Protokol kontrole prijenosa (Transmission Control Protocol – TCP) – Transmission Control Protocol je tehnologija nižeg sloja međusobnog povezivanja otvorenih sustava (Open Systems Interconnection – OSI) modela. TCP protokol radi zajedno sa IP protokolom kako bi se osigurao pravilan prijenos podataka putem internetske mreže. Jedna od glavnih zadaća TCP-a je osigurati da promet bude zaštićen prilikom prijenosa podataka do odredišta [2]. Ovaj protokol naziva se i spojni protokol iz razloga što stvara virtualnu konekciju sa drugim poslužiteljem, te putem ostvarene veze razmjenjuje odnosno prenosi podatke. TCP osigurava sljedeće [3]:
   - Nema izgubljenih paketa podataka
   - Ispravan predviđeni redoslijed paketa se poštuje
   - Prihvatljivo vrijeme kašnjenja
   - Dupliciranje paketa je spriječeno

   TCP obuhvaća paket podataka zaglavljem koje sadrži 10 obaveznih polja koji imaju ukupnu veličinu od 20 bajtova. Svako od tih zaglavlja sadrži informacije o vezi i trenutnim podatcima koji se šalju. U 10 obaveznih polja su uključeni [3]:
   - Izvorni priključak – Priključak uređaja s kojeg se šalje.
   - Odredišni priključak – Priključak uređaja koji prima podatke.
   - Broj sekvence – Uređaj koji inicira TCP vezu mora odabrati nasumični početni broj sekvence, koji se zatim povećava prema broju odaslanih bajtova.
   - Broj potvrde – Uređaj koji prima pakete održava broj potvrde koji počinje s brojem nula. Taj broj se povećava u odnosu s brojem primljenih bajtova
   - Pomak TCP podatka – Određuje veličinu zaglavlja koja je izražena 32 – bitnim riječima
   - Rezervirani podaci – Rezervirano polje uvijek je postavljeno na nulu.
   - Kontrolne oznake – Koristi se devet kontrolnih oznaka koje se koriste za protok podataka u specifičnim situacijama
   - TCP kontrolni zbroj veličine prozora – Prilikom slanja generira se kontrolni broj koji se šalje u zaglavlju svakog paketa, zatim uređaj koji prima pakete može provjeriti točnost pomoću kontrolnog broja.

- Hitni pokazivač – Ova vrijednost označava pomak od rednog broja ako je postavljena URG kontrolna zastavica tako da označava posljednji bajt hitnih podataka
- mTCP izborni podatci – izborna polja koja služe za postavljanje maksimalne veličine segmenta, omogućavanje prilagođavanja prozora za efikasniju upotrebu te selektivne potvrde.

3. Protokol korisničkog datagrama (User Datagram Protocol – UDP) – User Datagram Protocol još jedan je od nižih slojeva OSI modela koji se nalazi u djelu transportne razine [2]. UDP je glavna alternativa TCP – u iako je poprilično nepouzdan. UDP ne može izvršiti provjeru ili ispravljanje pogrešaka u prijenosu podataka [4]. Naravno postoje situacije odnosno određene aplikacije u kojima se preferira UDP umjesto TCP. To su najčešće situacije u kojima nije bitno da su svi paketi podataka na broju, to znači da je moguća komunikacija iako nemamo stalnu vezu. Zaglavlje UDP datagrama čine 4 polja od kojih svako polje sadrži 2 bajta odnosno 16 bitova [4].
   - Broj izvorišnog priključka – Zaslužno je za identifikaciju porta pošiljatelja. Ako se koristi onda bi broj trebao biti 0, a ako je izvorni host klijent onda će broj porta biti jednak prolaznom portu, a ako je izvorni host poslužitelj onda će broj porta biti između 0 i 1023
   - Broj odredišnog priključka - Zaslužno je za identifikaciju porta primatelja te je obavezno. Ako je odredišni host klijent onda će broj porta biti efemerni broj porta, a ako je poslužitelj odredišni host onda će broj porta biti između 0 i 1023.
   - Duljina – U ovom se polju navodi duljina UDP zaglavlja i UDP podataka u bajtovima. Minimalna duljina zaglavlja je 8 bajtova. Ograničenje za duljinu podataka proizlazi iz IPv4 protokola koji nalaže da je maksimalan broj mogućih bajtova 65 507. Korištenjem IPv6 protokola moguće su i veličine veće od 65 535 bajtova
   - Kontrolni zbroj – Može se koristiti za provjeravanje pogrešaka u zaglavlju i u samim podatcima. Ovo polje nije obavezno u IPv4 protokolu dok je obavezno u većini slučajeva kada se radi o IPv6 protokolu. Ako se ne koristi vrijednost polja su sve nule.

4. Protokol prijenosa hiperteksta (Hypertext Transfer Protocol – HTTP) / Protokol sigurnog prijenosa hiperteksta (Secure Hypertext Transfer Protocol – HTTPS) – Protokol koji je zaslužan za pravilnu komunikaciju poslužitelja ili web preglednika. Ovaj protokol se koristi za traženje HTML datoteka putem interneta. HTTP je izgrađen na vrhu TCP – a koji implementira komunikacijski model klijent – poslužitelj [2]. U HTTP protokolu postoje tri glavne poruke:

- HTTP GET: Poslužitelju se šalje poruka koja je u mogućnosti sadržavati URL bez parametara ili URL koji može sadržavati jedan ili više parametara. Zatim poslužitelj odgovara na način da se dodijeli web stranica pregledniku.
- HTTP POST: Poslužitelj šalje poruku koja najčešće sadrži podatke vezane za tijelo zahtjeva.
- HTTP HEAD: U ovoj poruci poslužitelj odgovara na zadane zahtjeve. HTTP HEAD ograničava odgovor poslužitelja tako da odgovori samo s informacijama zaglavlja [2].

5. Protokol za prijenos podataka (File Transfer Protocol – FTP) / SSH protokol za prijenos datoteka (SSH File Transfer Protocol – SFTP) – Ovaj protokol poznat je kao glavni protokol za prijenos datoteka između dva ili više računala. FTP također kao i HTTP koristi model klijent-poslužitelj za komunikaciju [2]. FTP protokol je prilično pouzdan zbog svojih razvijenih sigurnih metoda za dijeljenje datoteka. SFTP koristi i SSH terminal kako bi se podatci dodatno šifrirali prilikom prenošenja te tako omogućili dodatnu sigurnost prenošenja datoteka.

2.2 MOGUĆI NAPADI NA PROMETNI SUSTAV

Niti jedan sustav nije potpuno zaštićen od vanjskih napada ili unutarnjih napada. Koliko god sustav bio dobro dizajniran i pomno isplaniran uvijek postoji mogućnost propusta bilo da se radi o korisniku ili zaposleniku. Naravno sigurnost sustava ne ovisi samo o ljudskom faktoru već i veliku ulogu igraju sustavi koji nisu pravilno postavljeni ili ne prate najnovije trendove odnosno nadogradnje sustava. Neki od najrasprostranjenijih odnosno najučinkovitijih napada su:

1. Napadi distribuiranim uskraćivanjem usluge (Distributed Denial of Service – DDOS) – Ova vrsta napada radi na način da napadači pokušavaju preplaviti sustav nekim nasumičnim prometnom ili nasumičnim informacijama kako ne bi pravilno funkcionirao. Tijekom DDOS napada niz botova ili mreža botova preplavljuje web-mjesto HTTP zahtjevima i prometom. To u načelu znači da više računala napada jedno računalo, što izbacuje stvarne korisnike usluge. Iz tog razloga usluga može biti nedostupna ili može kasniti tokom određenog perioda napada. Postoje različite vrste DDOS napada a neke od njih su [5]:
    - Volumetrijski napad: Mrežni sloj preplavljuje se ogromnim količinama prometa. Primjer volumetrijskog napada je povećanje poslužitelja naziva domena (Domain Name Server – DNS) u kojem se koriste otvoreni DNS poslužitelji za preplavljivanje mete prometom odgovora na DNS.
    - Napad na protokol: Ova vrsta napada uzrokuje prekid usluge na način da se iskorištava slabost u stogu protokola sloja 3 i sloja 4. Primjer

takvog napada je SYN napad koji iskorištava sve dostupne resurse poslužitelja.

- Napad na sloj resursa: Ova vrsta napada cilja pakete web – aplikacija te ometa prijenos podataka između glavnih računala. Takva vrsta napada obuhvaća kršenje HTTP protokola te SQL injekciju te ciljani sloj napada je sloj 7.

Ovakva vrsta napada može se relativno učinkovito prepoznati na način ako se odjednom bez nekog razloga veliki broj upita odnosno prometa s iste IP adrese ili više IP adresa, zatim ako je mreža odjednom spora i nije u potpunoj funkcionalnosti ili ako je mreža potpuno nedostupna. Kako bi se DDOS napadi spriječili potrebno je definirati određene strategije zaštite poput uskraćivanja usluge, periodičnim ažuriranjem softvera, identifikacijom potencijalnih prijetnji.

2. Nedozvoljen pristup – Nedozvoljen pristup odnosi se na pojedince koji nedozvoljenim radnjama pokušavaju pristupiti važnim podatcima ili uređajima za koje nemaju ovlašten pristup. Postoji nekoliko uobičajenih uzroka odnosno scenarija neovlaštenog pristupa podatcima, neki od njih su najčešće stavljanje slabih zaporki koje su lako provaljive upotrebom raznih algoritama koji se zasnivaju na principu pokušaj - pogreška odnosno čistom silom (engl. Brute Force), zatim upotrebom modernih odnosno sofisticiranih metoda društvenog inženjeringa kako bi se navelo korisnike da bez loših namjera otkriju svoje zaporke odnosno da su prevareni bez njihovog znanja. Kako bi se smanjio rizik od neovlaštenog pristupa moramo obratiti pozornost na sljedećih pet strategija, a to su [6]:

   - Davanje privilegije ne smije se shvatiti olako te se moraju poduzeti mjere kao što su davanje privilegija određenim korisnicima a ne svim zaposlenicima.
   - Stavljanje vrlo jake i kompleksne zaporke sprječava određene algoritme da u prihvatljivom vremenu pogode zaporku.
   - Korištenjem više načine autorizacije istodobno, sprječava napadača da pristupi sustavu iako je možda uspio provaliti prvu razinu autorizacije.
   - Redovito ažuriranje sustava odnosno softvera sprječava napadače da pomoću poznatih ranjivosti uspiju provaliti u sustav.
   - Fizička sigurnost poput korištenja kompromitiranih vjerodajnica za neovlašteni pristup podatcima ili računalnim mrežama može se spriječiti tako da se uređaju nakon korištenja zaključaju ili ugase te da se radno mjesto ograniči samo za ovlaštene osobe

3. Manipulacija i krivotvorenje podataka – Manipulacija i krivotvorenje podataka vrlo je važan sigurnosni problem. Manipulacija podatcima vrsta je prijevare

koja uključuje neznatne tajne, a ponekad i kontinuirane izmjene podataka kako bi se stekla prednost ili kako bi se prevarili drugi [7]. Takva vrsta prevare može rezultirati vrlo visokim sigurnosnim rizikom jer ju napadači mogu iskoristiti za narušavanje reputacije, financijske prevare.

4. Neovlašten pristup vozilima – Hakiranje automobila je manipulacija kodovima u elektroničkoj upravljačkoj jedinici automobila kako bi se iskoristila ranjivost ili stekla kontrola nad drugim komponentama u vozilu [8]. Moderni automobili sadrže jako puno ugrađenih sustava koje koriste računala kako bi se što bolje kontroliralo vozilo. Elektroničke upravljačke jedinice međusobno komuniciraju putem komunikacijskih protokola te višestrukih mreža uključujući i mrežu kontrolera koja služi za komunikaciju komponenti unutar vozila. Takve veze uključuju upravljanje motorom i kočnicama te upravljanje svjetlima i bravama. U 2010. godini sigurnosni istraživači pokazali su kako mogu stvoriti fizičke učinke i potkopati kontrole sustava hakiranjem elektroničke upravljačke jedinice. Istraživačima je bio potreban fizički pristup upravljačkoj jedinici te su bili u mogućnosti steći potpunu kontrolu nad bilo kojim sigurnosnim odnosno automobilskim sustavom, uključujući onesposobljavanje kočnica i zaustavljanje motora. U naknadnom istraživačkom radu objavljenom 2011. godine, istraživači su pokazali da fizički pristup nije čak ni potreban [8]. Istraživači su pokazali da je iskorištavanje na daljinu izvedivo putem mehaničkih alata, CD playera, Bluetootha, mobilnog radija i bežičnih komunikacijskih kanala koji omogućuju kontrolu vozila na velikim udaljenostima, praćene lokacije, audio eksfiltraciju u kabini i krađu [9]. Kako bi se sprječili napadi na vozilo trebaju se poduzeti mjere kao što su redovito ažuriranje softvera, isključivanjem komponenti koje ne koristimo poput bluetooth – a, postavljanje jakih zaporki na WIFI mreže, itd.

5. Ometanje i blokiranje signala – Ometač signala radi na način da emitira „šum“ na određenim radio frekvencijama. Za vrijeme emitiranja „šuma“ korisniku su onemogućene funkcije koje koriste takve frekvencije odnosno napadnute frekvencije. Ometače signala vrlo je lagano kupiti putem interneta te radi tako da se uključi u određeno napajanje u vozilu, najčešće je to adapter za upaljač. Upotreba ometača signala može se na neki način usporediti sa DDOS napadima zato jer sprječava. Važno je napomenuti da ometač signala ne prekida prijem obližnjim uređajima već samo ometa njihovu sposobnost slanja i primanja poziva [10].

3. KRIPTOGRAFSKI SUSTAVI I METODE

Kriptografske metode i sustavi služe nam za sigurno prenošenje informacija među korisnicima iako je sadržaj poruke vidljiv on je kriptiran i nerazuman je svima onima kojima nije dopušteno vidjeti pravi sadržaj poruke. Kriptografija je razumijevanje i proučavanje raznih tehnika za sigurnu komunikaciju u kojoj sudjeluju i treće strane. Glavna grana kriptografije je matematika odnosno aritmetika te računalne znanosti. Upotrebom matematike i računalnih znanosti osigurava se autentičnost, cjelovitost te povjerljivost poruke u određenim okolnostima.

Povjerljivost je vrlo bitna stavka zato je uključuje sigurnost odnosno da se sadržaj informacija nije u mogućnosti mijenjati i naravno čitati tokom prijenosa bez neovlaštenog pristupa odnosno kako treće strane nebi mogle presresti i pročitati sadržaj poruke. U kriptografiji ne postoji jedinstvena odnosno univerzalna metoda za sakrivanje sadržaja poruke. Definirani su mnogi načini koji svojim tehnikama imaju prednosti i mane. U današnje vrijeme najrasprostranjenije metode šifriranja koriste javni i simetrični ključ. Uz legitimno korištenje kriptografije postoje i kriminalci koji koriste razne načine šifriranja kako bi izbjegli otkrivanje i omogućili lakše prenošenje nedopuštenih poruka. Dizajn kriptografskih protokola vrlo je složen i težak proces. Sve donedavno istraživači su bili orijentirani na korištenje formalnih metoda za analizu i verifikaciju postojećih protokola. Te su se metode pokazale uspješnima u otkrivanju nedostataka s postojećim protokolima, ponekad prethodno neprepoznatih [11]. U prošlosti kriptografije se gotovo uvijek odnosila na pretvaranje običnih informacija odnosno teksta u nerazumljiv oblik zamjenom određenih znakova nekim drugim znakovima pritom pazeći da pravila odnosno „ključevi“ potrebni za dešifriranje poruke budu sakrivena od neželjenih korisnika. Ključ je tajna koja je u idealnom slučaju poznata samo sugovornicima. Sadržaj ključa najčešće uključuje niz kratkih znakova koji su ključni kako bi se šifrirana poruka mogla dešifrirati.

U matematičkom smislu, sustav kriptografije uređeni je popis elemenata konačnih mogućih otvorenih tekstova, konačnih mogućih šifriranih tekstova, konačnih mogućih ključeva te algoritama za šifriranje i dešifriranje koji moraju odgovarati određenom ključu i mora se poštivati format ključa [11]. Ključevi su vrlo važna stavka za šifriranje i dešifriranje iz razloga što se bez ključeva tekstovi mogu trivijalno te u prihvatljivom vremenu dešifrirati. Gledajući kroz povijest šifre su se koristile izravno bez potrebnih provjera autentičnosti ili provjere integriteta.

3.1 SIMETRIČNA KRIPTOGRAFIJA

Simetrična kriptografija poznata je po tome što se koristi tajnim ključem te time omogućava razmjenu šifriranih podataka dokle god sugovornici znaju sadržaj tajnog ključa. Simetrična kriptografija dobila je naziv po tome što koristi isti ključ i za šifriranje i za dešifriranje podataka [12]. Takva vrsta enkripcije predstavlja dvosmjerni proces. S blokom otvorenog teksta i dobivenim ključem, simetričan način šifriranja uvijek će proizvesti šifrirani

tekst istog sadržaja, te sukladno tomu korištenjem istog tog ključa na istom tom bloku uvijek će se generirati izvorno šifrirani tekst. Simetrična enkripcija vrlo je korisna za zaštitu i sigurnost podataka između dviju strana koje koriste jednaki uspostavljeni zajednički ključ. Ovakva vrsta enkripcije vrlo često se koristi i za druge primjene poput pohrane povjerljivih podataka. Na primjer, ASP.NET koristi *3DES* (Data Encryption Standard) za šifriranje podataka kolačića za ulaznicu za provjeru autentičnosti obrazaca.

Slika 2. Princip rada simetričnog kriptografskog sustava, [13].

Slika iznad prikazuje jednostavan princip rada simetričnog kriptografskog sustava koji sadrži tri ključna elementa kako bi se uspješno šifrirali ili dešifrirali pojedini dokumenti. Primjer sa slike sadrži ulazne podatke, ključ te vrstu algoritma za šifriranje. Ulazni podatci najčešće su u obliku teksta te njih namjeravamo šifrirati, zatim kako bi uspješno šifrirali ulazni tekst potreban nam je ključ koji je tajna te nam je obavezan za šifriranje i dešifriranje podataka te na neki način on određuje vrstu algoritma koji će se koristit prilikom šifriranja i dešifriranja. Simetrični sustavi kriptiranja koriste dva načina šifriranja teksta, a to su [12]:

- Šifriranje toka (engl. Stream Ciphers) – Šifriranje toka radi na način da se šifriraju znamenke ili slova teksta jedno po jedno. Prednosti ovakvog načina je brzina, otpornost na mijenjanje teksta odnosno dodavanje simbola koji nisu inače prisutni. Nedostatak je niska razina difuzije odnosno svaki znak običnog teksta sadržan je u samo jednom simbolu šifriranog teksta.

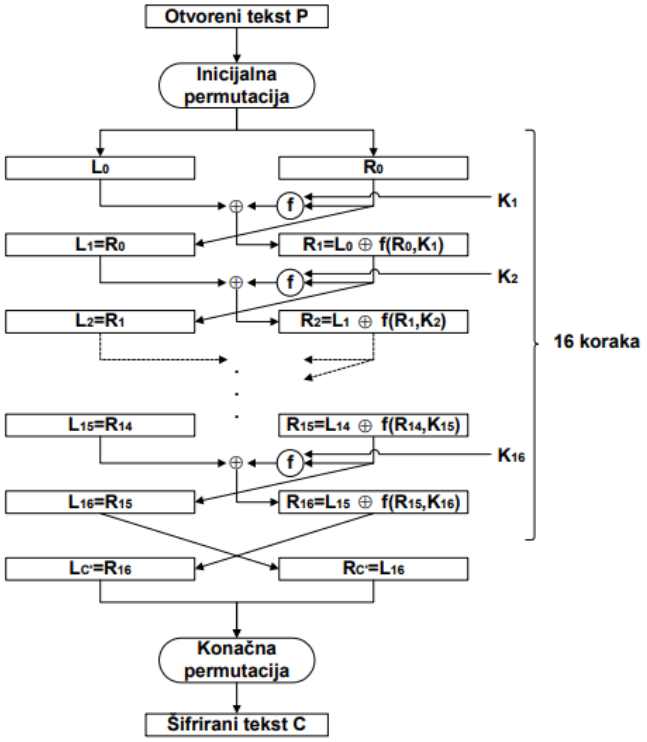
- Blokovsko šifriranje (engl. Block Ciphers) – Blokovsko šifriranje radi na način da se uzima više bitova teksta te se oni šifriraju. Prednost je visoka razina difuzije i vrlo jaku otpornost na napade otkrivanja. Nedostatak ovog načina je sporija brzina kriptiranja iz razloga što se cijeli blok uključuje u šifriranje odnosno dešifriranje.

Napadi koji pogađaju simetrični kriptografski sustav su napadi poznatog otvorenog teksta, diferencijalna kriptoanaliza te linearna kriptoanaliza [13]. Kako bi se spriječili takvi napadi poduzimaju se mjere poput pažljive konstrukcije funkcija za svaki blok, zatim povećanje duljine ključa ili bloka u procesu enkripcije sprječava lako otkrivanje ključa.

Problem s kojim se suočava kriptografija je također i izum kvantnih računala koja bi eksponencijalno smanjila vrijeme potrebno za dekodiranje. Jedan takav primjer je Groverov algoritam koji bi smanjio inače potrebno vrijeme za razbijanje ključa, na korijen toga vremena. Iako se takve ranjivosti mogu kompenzirati udvostručenjem duljine ključa opet sustavi nisu sto posto sigurni.

3.1.1 DES algoritam

Standard šifriranja podataka (Data Encryption Standard – DES) je simetrična vrsta algoritma koja je proizvedena tijekom sedamdesetih godina u IBM – u. 1977. godine američka vlada prihvatila je DES algoritam kao standard za zaštitu podataka. Glavna mana je, što je javno poznato, da je tijekom razvoja mnoge „sugestije“ davala i *NSA* (National Security Agency), pa mnogi smatraju da u algoritmu postoji sigurnosna „rupa“ (engl. backdoor), koja omogućava američkoj vladi dešifriranje podataka [14]. *DES* (Data Encryption Standard) se više ne smatra potpuno sigurnim iz razloga što se njegov 56 – bitni ključ može vrlo jednostavno probiti s današnje raspoloživim računalnim resursima korištenjem čiste sile (engl. brute force) u prihvatljivom vremenu.



Slika 3. Blokovni dijagram šifriranja otvorenog teksta DES algoritmom, [14].

DES algoritam radi način da zadani tekst ili poruku šifrira po 64 – bitnim blokovima te se pri tom na izlazu dobiva 64 – bitni šifrirani tekst odnosno poruka. Ključ potreban za šifriranje i dešifriranje dugačak je 56 – bita, no često se pojavljuje i u 64 – bitnom prikazu ali se svaki osmi bit zanemaruje, odnosno služi za provjeru pariteta [14]. Prva stvar koju

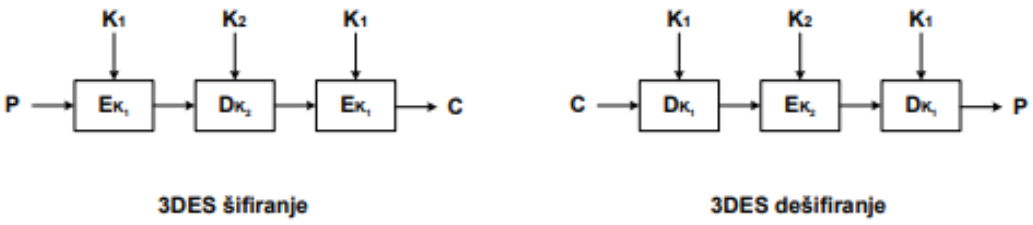
algoritam radi jest inicijalna permutacija sve dok posljednji korak predstavlja inverziju inicijalne permutacije [14]. Prije posljednjeg koraka, desna i lijeva polovica odnosno 32 – bitna polovica se zamjenjuju [14]. Kod preostalih 16 koraka, niz znakova se dijeli na lijevu i desnu 32 – bitnu polovicu, gdje desna polovica postaje lijeva polovica idućeg koraka, dok se nad lijevom polovicom provode operacije koje su u svakom koraku parametrizirane drugim 48 – bitnim potključem [14]. Potključevi se izvode iz osnovnog ključa te ih ukupno ima 16 različitih duljine od 48 bitova. Algoritam izgleda ovako:

```
početak
  permutiraj P
  P^T=L_0R_0
  za i=1 do i=16 radi
        L_i = R_i-1
        R_i = L_i-1 ⊕ f(R_i-1,S_i)
  kraj
  zamijeni(L_16,R_16)
  C' = L_16R_16
  C = permutiraj^-1C'
kraj
```

Slika 4. Vizualni prikaz koda DES algoritma, [14].

Pošto se ovaj algoritam koristi i danas unatoč tome što znamo da je 56 – bitna duljina ključa podložna napadima izvedene su razne modifikacije te se njima i unaprijedila sigurnost.

Neke takve modifikacije odnosno unaprjeđenja su korištenje višestrukog DES algoritma, odnosno upotreba trostrukog DES algoritam (3DES) u takozvanom EDE načinu rada [14]. Takav način rada prikazan je na slici ispod:



Slika 5. Blokovski dijagrami šifriranja i dešifriranja putem 3DES inačice, [14].

3DES je prvi put predstavljen 1998. godine, gdje je i primarno usvojen u financijskim pa tako i u drugim privatnim sektorima za šifriranje prijenosnih poruka odnosno podataka te za šifriranje pohranjenih podataka. Uz 3DES inačicu DES algoritam postoji i DESX inačica koja je

izrađena od strane RSA Data Security. DESX koristi tehniku „izbjeljivanja“ (engl. whitening), koja radi na način uvođenja dodatnih XOR operacija nad ulaznim i izlaznim podatcima u algoritmu [14]. Ut 56 – bitni ključ, DESX koristi i dodatni 64 – bitni ključ koji se koristi za „izbjeljivanje“ [14]. 64 – bitni ključevi koriste se također za izvođenje XOR operacija prije prvog koraka algoritma. Također, dodatna 64 – bita izvedena korištenjem jednosmjerne funkcije nad ukupnim 120 – bitnim DESX ključem koriste se za izvođenje još jedne XOR operacije u posljednjem koraku [14]. Također imamo i inačicu s modificiranim S – blokovima, to je ujedno i jedan od prijedloga da se alterniranjem odnosno promjenom S – blokova poboljša rad algoritma te ga učini još sigurnijim. Pokazalo se da je redoslijed te dizajn S – blokova dizajniran odnosno optimiziran za napade koje koriste diferencijalne kriptoanalize. Dizajn s druge strane se pokazao kao neoptimizirano svojstvo s obzirom na razne napade korištenjem linearne kriptoanalize. Grupa istraživača imala je niz pokušaja promjena S – blokova kroz s^n DES algoritma, od kojih su neki bili uspješniji, dok su drugi pokazivali i lošije performanse prilikom linearne i diferencijalne kriptoanalize [14].

- Diferencijalna kriptoanaliza – U širem smislu to je skup strategija za praćenje razlika u mreži transformacija odnosno pronalaženje gdje šifra pokazuje periodično ponašanje te se korištenjem takvih saznanja pokušava otkriti tajni ključ.
- Linearna kriptoanaliza – Temelji se na pokušaju otkrivanja afinih aproksimacija djelovanja šifre u kriptografiji

Kako bi se poboljšala sigurnost DES algoritma potrebno je uzeti u obzir da ako se blokovi naprave tako da budu ovisni o ključu i da se odabiru korištenjem neke jake kriptografske metode, primjena linearne i diferencijalne kriptoanalize bila bi znatno teža [14].

3.1.2 AES algoritam

Napredni standard šifriranja (Advanced Encryption Standard – AES) je simetrična vrsta šifriranja koja koristi šifriranje po blokovima. Izabrana je od strane SAD – a kao standard za obranu odnosno zaštitu povjerljivih podataka. Ova vrsta algoritma poznata je također kao i Rijndaelov algoritam koji radi na principu simetričnog blokovskog šifriranja s veličinom bloka od 128 bita [15].

U današnje vrijeme što se tiče rasprostranjenosti upotrebe, DES i drugi simetrični algoritmi još uvijek se koriste u većoj mjeri. Ubrzo će i AES pronaći svoje mjesto pogotovo zato što je sigurniji od DES algoritma i pruža veću razinu zaštite što naravno sustavi sa najvišom razinom sigurnosti zahtijevaju. S obzirom na korištenje ključeva različitih dimenzija, AES algoritam možemo nazivati i kao AES – 128, AES – 192 i AES – 256.

Unutarnje operacije AES algoritma provode se na matrici stanja odnosno dvodimenzionalnom nizu okteta. Dvodimenzionalni niz okteta sastoji se od četiri retka koji sadrže zadani broj okteta. Zadani broj okteta predstavlja ukupnu duljinu bloka u bitovima

podijeljenu sa 32 [16]. Kod AES algoritma to znači 4 okteta iako Rijndael – ov algoritam dopušta i druge vrijednosti. Šifriranje odnosno dešifriranje provodi se na način da se ulazni blok podataka kopira u matricu stanja nad kojom se zatim provode razne operacije, te se završna vrijednost matrice stanja kopira u izlazni šifrirani blok podataka.

Slika 6. Blokovski dijagram prikazuje način rada AES algoritma, [15].

Blokovi se kreiraju pomoću ključeva veličine 128, 192 i 256 bita. Nakon uspješnog šifriranja blokovi se zatim spajaju u cjeloviti šifrirani tekst. AES je napravljen kako bi uspješno zamijenio DES algoritam koji je podložan napadima čistom silom (engl. Brute Force). Istraživanja su pokazala da unatoč broju zahtjeva, korisničkim opterećenjima te vremenu odziva u različitim situacijama opterećenja korisnika, AES nadmašuje DES algoritam. Na slici ispod možemo vidjeti kako radi AES u obliku algoritma.

```
početak
  oktet stanje[4,Nw]

  stanje = ulaz
  dodaj_podključ (stanje, w[0,Nw-1])

  za korak=1 do korak=Nr-1 radi
        zamjena_okteta(stanje)
        posmak_redaka(stanje)
        mijesanje_stupaca(stanje)
        dodaj_podključ(stanje,w[korak*Nw,(korak+1)*Nw-1])
  kraj
  zamjena_okteta(stanje)
  posmak_redaka(stanje)
  mijesanje_stupaca(stanje)
  dodaj_podključ(stanje,w[Nr*Nw,(Nr+1)*Nw-1]

  izlaz = stanje
kraj
```

Slika 7. Prikaz koda AES algoritma, [16].

Šifriranje se provodi na način da se ulazni blok kopira u matricu stanja, te se nakon kopiranja provodi inicijalno dodavanje potključa u matricu. Matrica stanja zatim se transformira ovisno o duljini ključa, a to je najčešće 10, 12 ili 14 puta. Zadnji korak obuhvaća kopiranje matrice stanja u izlazni blok. Postupak šifriranja prikazan je slikom iznad, dok ako želimo dešifrirati tekst onda koristimo inverzije funkcija zamjena_okteta(), posmak_redaka(), i mijesanje_stupaca(). Svaki korak algoritma predstavlja funkciju koja sadrži četiri transformacije koje se izvršavaju nad oktetama, a to su [16]:

- Zamjena okteta na temelju supstitucijske tablice (S - blok).
- Posmak redaka u matrici stanja.
- Miješanje podataka unutar svakog stupca matrice stanja.
- Dodavanje potključa u matricu stanja.

Sigurnost algoritma ovisi o duljini ključa koji se koristi, ako koristimo AES – 128 odnosno ključ veličine 128 bitova za šifriranje i dešifriranje, to može predstavljati problem iz razloga što se kriptiranje putem 128 bitnog ključa pomoću kvantnog računala može otkriti sa svega 6 mjeseci dok bi običnim računalima trebalo preko 10 kvintilijuna godina. Međutim AES algoritam još uvijek je siguran za korištenje jer postoje i veće veličine ključeva poput 192 – bitnih i 256 – bitnih ključeva koji se još uvijek nebi mogli otkriti pomoću kvantnih računala u prihvatljivom vremenu. Zbog veličine ključeva AES se još uvijek smatra „kvantno otpornim“.

3.2 ASIMETRIČNA KRIPTOGRAFIJA

Asimetrična kriptografija ili bolje poznata kao kriptografija s javnim ključem je sustav koji koristi javni ključ i privatni ključ. Javni ključ može biti poznat drugima dok privatni ključ treba ostati tajna svima osim vlasniku. Sustav radi na način da svaka osoba koja posjeduje javni ključ može uspješno šifrirati tekst, no taj šifrirati tekst može se dešifrirati samo privatnim ključem primatelja. Ovakva vrsta kriptografija pogodna je u poslužiteljskim programima koji mogu generirati kriptografski ključ namijenjen odgovarajućoj metodi kriptografija sa simetričnim ključem, te zatim koristimo klijentov javni ključ za šifriranje novogeneriranog simetričnog ključa. Poslužitelj je tada u mogućnosti poslati šifrirani simetrični ključ preko nesigurnih kanala komunikacije pošto ga samo klijent može dešifrirati koristeći vlastiti privatni ključ. Naravno i klijent i poslužitelj imaju isti simetrični ključ te mogu sigurno koristiti šifriranje simetričnog ključa.

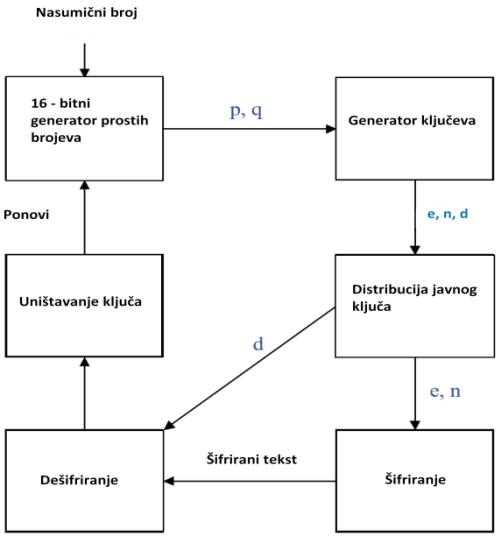
Prednost ovakvog postupka je ta što se ne mora unaprijed ručno dijeliti simetrične ključeve dok se u isto vrijeme postiže veća propusnost podataka kriptografije kriptiranjem simetričnim ključem. Kriptografija javnim ključem omogućava i robusniju autentifikaciju. Pošiljatelj može kombinirati poruku s privatnim ključem kako bi stvorio digitalni potpis na poruci. Svatko s odgovarajućim javnim ključem pošiljatelja može kombinirati tu poruku s traženim digitalnim potpisom, ako potpis odgovara poruci, potvrđuje se podrijetlo poruke. Šifriranje korištenjem javnog ključa temelj su sigurnosti u modernoj kriptografiji, uključujući protokole i aplikacije koje garantiraju autentičnost, povjerljivost, pohranu podataka te

elektroničku komunikaciju. Asimetrična kriptografija temelj je mnogih internetskih standarda, kao što su sigurnost transportnog sloja (Transport Layer Security – TLS), S/MIME, Prilično dobra privatnost (engl Pretty Good Privacy – PGP) i GNU čuvar privatnosti (GNU Privacy Guard – GPG) [17]. Određene metode kriptografije javnog ključa omogućuju i prenošenje odnosno distribuciju i tajnog ključa (npr. Diffie – Hellman razmjena ključeva). Asimetrična kriptografija u odnosu na simetričnu kriptografiju je dosta sporija od prihvatljive simetrične kriptografije te je tako prespora da bi se koristima u neke druge svrhe. Početkom 1970 – ih godina gotovo svi sustavi šifriranja koristili su algoritme simetrične kriptografije i kojim koristim isti ključ za šifriranje i dešifriranje. Najpoznatije metode asimetrične kripotgrafije koje se koriste danas su [17]:

- Šifriranje javnog ključa – Ovo se pretežito koristi za osiguranje povjerljivosti poruke. Koristi se na način da se poruka šifrira javnim ključem željenog primatelja.
- Digitalni potpis – Kada je poruka potpisana privatnim ključem pošiljatelja, svatko tko posjeduje javni ključ pošiljatelja može provjeriti valjanost potpisa za tu poruku.

3.2.1 RSA ALGORITAM

RSA (Rivest – Shamir – Adleman) je asimetrična vrsta kriptografije koja je najpoznatija i najviše se koristi, kako u prometu tako i u ostalim znanstvenim granama. To je kriptosustav koji se koristi javnim ključem i ujedno je i jedan od najstarijih široko korištenih algoritama za siguran prijenos podataka [18]. Sustav radi na način da se koristi javni ključ za šifriranje koji je javan i razlikuje se od ključa za dešifriranje koji se drži u tajnosti. RSA korisnik stvara o objavljuje javni ključ na temelju dva velika prosta broja, zajedno s pomoćnom vrijednošću. Primarni brojevi se čuvaju u tajnosti. Poruke može šifrirati bilo tko koristeći javni ključ ali ih može dekodirati samo netko tko zna proste brojeve.



Slika 8. Blokovski prikaz rada RSA algoritma, [19].

RSA algoritam radi na način da u prvo koraku se putem generatora generiraju dva prosta broja p i q. Vrijednosti p i q trebaju biti generirani kao nepredvidljivi slučajni brojevi različitih vrijednosti [18]. Zatim se generirani brojevi p i q koriste za izračunavanje $\varphi(N)$ i n. Zatim se $\varphi(N)$ koristi za izračunavanje e. Izračunati e se zatim koristi za šifriranje teksta, dok se d može dobiti putem e. Za dešifriranje šifriranog teksta koristi se d i mora se čuvati tako da ga samo korisnik može vidjeti.

$$\begin{aligned}
\textbf{Odabir slučajnog prostog broja} &= p,\ q\ (p \neq q) \\
n &= p \times q \\
\varphi(N) &= (p-1)(q-1) \\
(\varphi(N), e) &= 1 < e < \varphi(N) \\
\textbf{Izračunaj}\ \ d \rightarrow\ \ e \times d\ mod\ \varphi(N) &= 1
\end{aligned}$$

$$C = P^e\ mod\ n$$
$$P = C^d\ mod\ n$$

Slika 9. Prikaz koda RSA algoritma, [19]

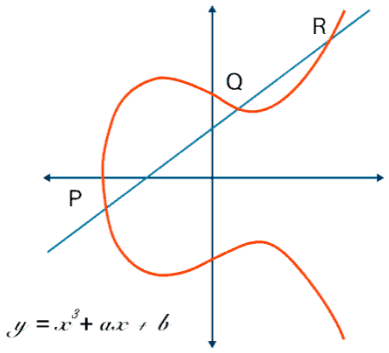
Sigurnost RSA algoritma ovisi o duljini njegovog ključa. Ključevi su obično dugački 1024 ili 2048 bita no stručnjaci vjeruju kako 1024 – bitni ključevi nisu u potpunosti sigurni protiv svih napada [19]. Iz tog razloga razne industrije i vlada nalažu minimalnu duljinu ključa od 2048 bita. Poznati napadi na RSA algoritam uključuju:

- Šifrirani napadi – napadač može otkriti sadržaj običnog teksta na osnovu šifriranog teksta koristeći prošireni euklidski algoritam
- Napad faktorizacijom – Ako napadač može saznati vrijednosti P i Q koristeći N onda može saznati i sadržaj privatnog ključa. Ovo je neizvedivo za veće brojeve, jer kada N koristi najmanje 300 dužih znamenki u decimalnim terminima, napadač ga neće moći pronaći.
- Napadi na ključ za dešifriranje i šifriranje – Preporučuje se uzimanje novih vrijednosti prostih brojeva P i Q te N i E.

3.2.2 KRIPTOGRAFIJA ELIPTIČKOM KRIVULJOM

Korištenje eliptičkih krivulja za šifriranje i dešifriranje predložili su Neal Koblitz i Victor S. Miller 1985. godine. Eliptičke krivulja za kriptografiju počele su se široko koristiti 2004. do 2005. godine [20]. Kriptografije eliptičke krivulje (Elliptic Curve Cryptography – ECC) je kriptografija s javnim ključem koji se temelji na algebarskoj strukturi eliptičkih krivulja nad konačnim poljima.

Ovakva vrsta kriptografije dopušta uporabu ključeva manje veličine u usporedbi s ostalim kriptografskim algoritmima odnosno algoritmima temeljenim na Galoisovim poljima kako bi se pružila jednaka sigurnost. Eliptičke krivulje mogu se koristiti za dogovor ključeva, pseudoslučajne generatore, digitalne potpise i druge zadatke. Također se mogu koristiti za enkripciju u kombinaciji dogovora o ključu sa simetričnim načinom šifriranja. Još jedan način upotrebe uključuje korištenje nekoliko algoritama za faktorizaciju cjelobrojnih brojeva koji se također mogu primijeniti u kriptografiji, a jedna od takvih primjena je faktorizacija Lenstrine eliptičke krivulje. Ovakva vrsta kriptografije s javnim ključem temelji se na matematičke probleme koji su nerješivi.



Slika 10. Graf eliptičke krivulje koji se koristi u kriptografiji, [21].

Prvi sustavi temeljeni na javnim ključevima obećavali su svoju sigurnost na temelju pretpostavke da je teško faktorizirati velike cijele brojeve koji su sastavljeni od dva ili više prostih faktora. Osnovna pretpostavka za metode koji se temelje na eliptičkoj krivulji je ta da je pronalaženje diskretnog logaritma nasumičnog elementa eliptičke krivulje u odnosu na poznatu referentnu točku neizvedivo. Takav problem naziva se „problem diskretnog logaritma eliptičke krivulje“.

Sigurnost ECC kriptografije ovisi o sposobnosti izračunavanja množenja u točki i nemogućnost izračunavanja množenika s obzirom na izvorne i produktivne točke [21]. Veličina eliptičke krivulje koja je mjerena ukupnim brojem nekih diskretnih parova cijelih brojeva koji zadovoljavaju jednadžbu krivulje, određuje težinu samog problema. Primarna prednost koju kriptografija eliptičke krivulje obećava je manja veličina ključa, smanjujući tako zahtjeve za pohranu i prijenos. Na primjer 256 – bitni javni ključ eliptičke krivulje trebao bi pružiti gotovo jednaku sigurnost kao RSA algoritam koji koristi 3072 – bitni javni ključ.

4. SUSTAVI AUTENTIFIKACIJE I AUTORIZACIJE U INTELIGENTNIM TRANSPORTNIM SUSTAVIMA

Autentifikacijski sustavi su sustavi koji predstavljaju implementirane sigurnosne mjere kako bi se osigurali podatci i drugi sustavi. Autentifikacija je čin dokazivanja identiteta nekog korisnika sustava [22]. Različita je od identifikacije zato jer identifikacija predstavlja odnosno označava identitet osobe, dok proces autentifikacije provjerava točnost identiteta. Autentifikacija se može podijeliti u tri vrste.

Prva vrsta autentifikacije obuhvaća prihvaćanje dokaza identiteta od strane povjerljive osobe koja sadrži dokaze kako bi potvrdila autentičnost identiteta. Centralizirani odnosi povjerenja temeljeni na autoritetu osiguravaju najsigurniju internetsku komunikaciju putem poznatih javnih autoriteta za izdavanje certifikata. Također postoji i decentralizirano povjerenje, drugačije poznato kao mreža povjerenja te se koristi za osobne usluge poput usluga e – pošte ili prijenosa datoteka. Takva vrsta povjerenja temelji se na način da poznati pojedinci međusobno potpisuju kriptografski ključ. Druga vrsta provjere autentičnosti obuhvaća uspoređivanje atributa nekog objekta s onim što nam je poznato od prije. Usporedba atributa podložna je na krivotvorenja. Na primjer fizika svjetla i zvuka u usporedbi s poznatim fizičkim okruženjem mogu se koristiti za ispitivanje autentičnosti fotografija, audio zapisa ili video zapisa. Treća vrsta provjere autentičnosti obuhvaća oslanjanje na vanjske potvrde ili dokumentaciju. U računalnoj znanosti, korisniku se može odobriti pristup sigurnosnim sustavima na temelju korisnikove potvrde odnosno vjerodajnice koja služi za potvrdu autentičnosti. Administrator je u mogućnosti dati korisniku zaporku ili neke druge pristupne uređaje kako bi mu omogućio pristup sustavu.

Faktori autentifikacije obuhvaćaju načine na koje se netko može autentificirati. Načini autentifikacije dijele se u tri kategorije [22]:

- Znanje – nešto što korisnik zna, pretežito su to zaporke ili osobni identifikacijski broj, itd.
- Vlasništvo – nešto što korisnik posjeduje, pretežito su to osobna iskaznica, sigurnosni token ili neke druge stvari poput narukvica itd.
- Inherentnost - Nešto što korisnik jest, pretežito su to otisci prsta, uzorak mrežnice, DNA sekvenca i slično.

¸ Faktori autentičnosti uzimaju u obzir niz elemenata koji su potrebni za autentifikaciju ili provjeru identiteta osobe prije nego joj se odobri pristup. Sigurnosno istraživanje došlo je do zaključka da za pravilnu autentifikaciju treba provjeriti najmanje elemente dva, a po mogućnosti i sva tri faktora.

Jednostruka provjera autentičnosti rangira se kao najslabija razina autentifikacije iz razloga što se za postupak autentifikacije identiteta pojedinca koristi samo jedna komponenta iz jedne od tri kategorije faktora. Korištenje jednostruke provjere autentičnosti

predstavlja veliki sigurnosni rizik zato jer ne nudi dovoljno veliku razinu zaštite od zlouporabe ili raznih vrsta napada [22]. Ovakva vrsta autentifikacije pogotovo nije prigodna za financijske ili osobne zahtjeve odnosno transakcije koje zahtijevaju odnosno jamče visoku razinu sigurnosti. Najčešći i najistaknutiji identifikator jednostruke provjere je lozinka. Neki od ostalih identifikatora koji se sve češće koriste je i autentifikacija SMS kodom registriranog uređaja te jednokratne zaporke koje najčešće generiraju fizički uređaji ili softveri na određenim uređajima. Kako bi se donekle zaštitili od neovlaštenih upada preporučuje se izbjegavanje korištenja starih zaporki te naravno korištenje dugačkih i složenih lozinki koji su različite za svaki račun.

Višefaktorska provjera autentičnosti obuhvaća dva ili više spomenutih faktora autentifikacije. Dvofaktorska autentifikacija predstavlja poseban slušaj višefaktorske autentifikacije a to je da sadrži točno dva faktora za provjeru. Primjer korištenja dvofaktorske autentifikacije pretežito uključuje lozinku korisnika te pseudoslučajan broj koji se dobiva iz sigurnih institucija. Pristup sustavima koji imaju vrlo visoku razinu sigurnosti također mogu obuhvaćati i davanje tjelesnih karakteristika poput visine, težine, otiska prstiju u kombinaciji sa lozinkom ili dodatnim faktorima. Najsigurnija metoda višefaktorske autentifikacije uključuje brzi identitet na mreži (Fast Identity Online - FIDO2) i web autentifikaciju(Web Authentication – WebAuthn) standardne sigurnosne ključeve koji se temelje na hardveru. Poznati napadi na višefaktorsku provjeru autentičnosti su SIM Swap napadi, otmica kanala odnosno krađa mobilnog telefona ili preglednika tako da ga zarazi malverom, zatim napadi prilikom oporavka (engl. Recovery) nakon gubitka vjerodajnica, te phishing napadi koji se odnose na proces namamljivanja korisnika da bez znanja odnosno slučajno dobrovoljno daju svoje vjerodajnice za pristup sustavu. Postoji više vrsta višefaktorske autentifikacije, a to su [22]:

- Snažna autentifikacija – Odnosi se na definiranje više slojeva pristupa autentifikaciji koja se zatim dodatno oslanja na dva ili više faktora za autentifikaciju. Europska središnja banka (European Central Bank – ECB) definirala je jaku autentifikaciju kao „postupak koji se temelji na dva ili više od tri faktora autentifikacije“. Komponente koje se koriste moraju biti međusobno neovisni te najmanje jedan od faktora mora biti nemoguć za daljnju upotrebu ili repliciranje
- Kontinuirana autentifikacija – Odnosi se na sustave koji kontinuirano provode autentifikaciju korisnika te kontinuirano prate i provjeravaju autentičnost korisnika koristeći tjelesne karakteristike poput biometrijskih obilježja. Istraživanje su pokazala da je moguće koristiti i senzore pametnih telefona kako bi se izdvojile dodatne karakteristike ponašanja poput dinamika dodira, način i brzina hoda te ostali atributi.
- Digitalna autentifikacija – Odnosi se na elektroničke provjere autentičnosti te se referencira na skupinu procesa u kojima se povjerenje korisničkih identiteta uspostavlja i prezentira putem elektroničkih metoda u informacijskom sustavu.

Ovakva vrsta provjere autentičnosti može predstavljati tehničke izazove zbog potreba za autentifikacijom na daljinu.

Autorizacija obuhvaća određivanje razine prava odnosno pristupa resursima ili podatcima, te se odnosi na općenitu sigurnost informacija i računalnu sigurnost a posebno na kontrolu pristupa [23]. Autorizacija definira politiku pristupa. Tijekom rada sustava koriste se razna pravila za kontrolu pristupa kako bi se odlučilo hoće li zahtjevi autentificiranih korisnika biti odobreni ili odbijeni. Primjeri nekih resursa kojima korisnik može pristupiti nakon autorizacije su pojedine datoteke ili podatci, pristup uređajima te pristup određenim funkcionalnostima. Politika pristupa vrlo je važan aspekt prilikom pregleda kontrole pristupa u računalnim sustavima i mrežama. Proces kontroliranja pristupa može se podijeliti na faze:

- Faza definiranja politike gdje je pristup već autoriziran.
- Faza provedbe politike u kojoj su zahtjevi za pristup dopušteni ili nedopušteni.

Iz tog razloga autorizacija se smatra kao funkcija definiranja faze politike koja prethodi fazi provedbe politike gdje su zahtjevi za pristup nedopušteni ili dopušteni na temelju definiranih autorizacija. Kod kontrole pristupa također se koristi i autentifikacija za provjeru identiteta potrošača. Primjerice, kada korisnika pokuša pristupiti datoteci ili određenom resursu, aktivira se proces kontrole pristupa koji potom gleda ima li korisnik dopuštenje za korištenje resursa odnosno datoteke. Autorizacijske uloge u većini slučajeva implementira sigurnosni server koji također može kontrolirati razinu pristupa na razini pojedinih datoteka ili programa. Većina sigurnosnih sustava na internetu temelji se na procesu koji se odvija u dva koraka. Prvi korak je autentifikacija koja jamči identitet korisnika, a druga faza je autorizacija koji omogućuje razinu pristupa različitim resursima na temelju identiteta korisnika.

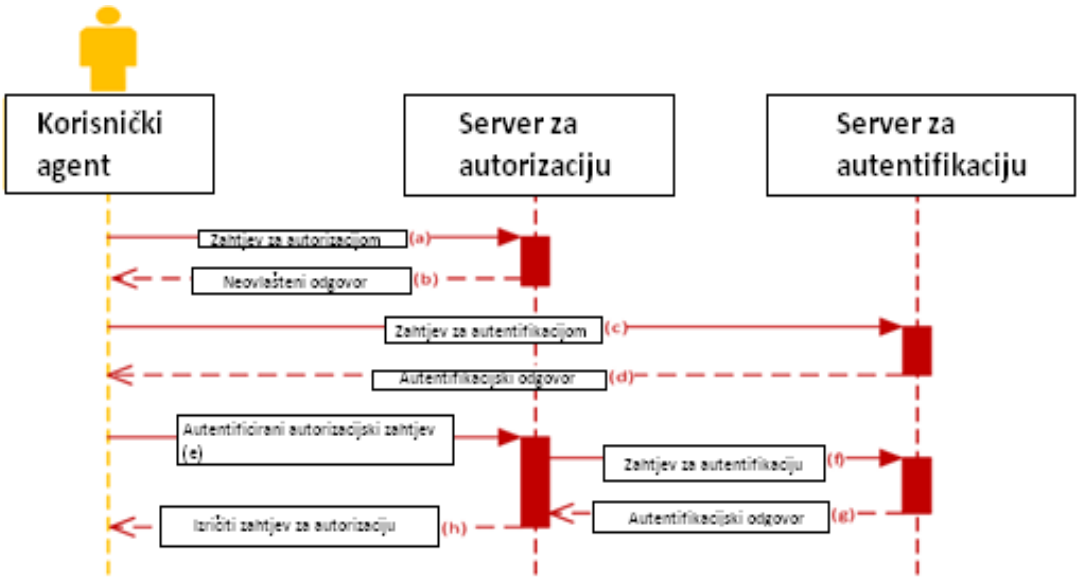
Moderni operativni sustavi ovise razini učinkovitosti dizajniranja procesa autorizacije kako bi se pojednostavnila odnosno olakšala implementacija i upravljanje aplikacijama. Prilikom autorizacije ključni aspekti koji se uzimaju u obzir su većinom vrsta korisnika, broj, vjerodajnice, te zahtijevaju provjeru povezanih radnji i uloge. Pravila za autorizaciju dio su IT discipline koja poprima naziv upravljanje identitetom i pristupom (Identity and access management – IAM). Unutar discipline upravljanja identitetom i pristupom, autorizacija i autentifikacija pomažu upraviteljima sustava da lakše kontroliraju tko ima pristup resursima te kakve privilegije odnosno razinu pristupa ima korisnik. Načini IT sustava koji se bave uslugama autorizacije vrlo su slični procesima kontrole pristupa u stvarnom svijetu. Kontrola pristupa može se podijeliti u tri kategorije [23]:

- Kontrola pristupa temeljena na atributima (Attribute Based Access Control - ABAC) – Korištenjem kontrole pristupa temeljene na atributima, računalni sustav definira ima li korisnik dovoljnu razinu pristupa određenim resursima na temelju njegovih atributa ili osobina.

- Kontrola pristupa temeljenja na ulogama (Role – Based Access Control - RBAC) – Korištenjem ove metode autorizacija se tretira kao dozvola koja je povezana s određenim ulogama a ne izravno s korisnicima. Uloga je zapravo zbirka dopuštenja. Prednost korištenja ove metode je što olakšava upravljanje autorizacijskim privilegijama, što rasterećuje upravitelje sustava tako da se oni mogu fokusirati na rješavanje pitanja dozvola i korisnika
- Kontrola pristupa temeljena na odnosima (Relationship – Based Access Control - ReBAC) – Korištenjem ove metode postavlja se pitanje „Ima li određeni korisnik dovoljan odnos prema ovom objektu ili radnji tako da mu može pristupiti?“ Odnos može doći preko korisničkih atributa, poput članstva u grupi uloga povezanih s objektom ili direktan odnos kao što je dijeljenje na dokumentu. Ponekad obilazak grafa grupa, uloga, organizacija i objekata zahtijeva istraživanje mnogih čvorova kako bi se uspostavio odnos između korisnika i onoga što pokušava učiniti. Koji su odnosi kritični za dobivanje pristupa i dopuštenja koja ti odnosi dodjeljuju ovisi o implementatoru sustava ReBAC.

4.1 KORISNIČKA AUTENTIFIKACIJA I AUTORIZACIJA

Korisnička autentifikacija i autorizacija vrlo je bitna kako bi se spriječili razni napadi na sustav. Korištenjem korisničke autentifikacije i autorizacije ublažujemo vanjske i unutarnje prijetnje koji se mogu dogoditi a drastično utječu na funkcionalnosti sustava.



Slika 11. Prikaz procesa autentifikacije i autorizacije, [24]

Kod korisničke autentifikacije koristimo razne metode, neke od njih su:

1. Autentifikacija putem lozinke – Ovakva vrsta autentifikacije je najčešći oblik provjere autentičnosti. Lozinke su većinom niz od slova, brojeva ili posebnih znakova. Kako bi osigurali što bolju sigurnost trebamo obratiti pozornost na sadržaj lozinke odnosno trebamo stvoriti jaku lozinku koja sadrži sve moguće opcije. Ovaj oblik autentifikacije sklon je vanjskim napadima poput phishinga. Zaključak je da ovaj oblik autentifikacije ne pruža dovoljnu razinu zaštite zbog puno slabosti i mogućih vrsta napada.

2. Višefaktorska autentifikacija – Ova metoda pruža donekle dobru zaštitu zato jer zahtjeva dva ili više neovisnih načina potrebnih kako bi se korisnik uspješno identificirao. Autentifikacija s više faktora (Multi – factor Authentication - MFA) najčešće uz lozinku uključuje i kodove generirane na pametnom telefonu korisnika, otiske prstiju, prepoznavanje lica ili prepoznavanje glasa [25]. Zaključak je da korištenjem višefaktorske autentifikacije povećavamo povjerenje korisnika zbog više slojeva sigurnosti. Ova metoda također ima i slabosti poput gubitka telefona korisnika.

3. Autentifikacija temeljena na certifikatu – Ova metoda provjere autentičnosti uključuje izradu i provjeru digitalnih certifikata kako bi se korisnik uspješno autentificirao [25]. Digitalni certifikat je elektronički dokument poput vozačke dozvole ili putovnice, te sadrži digitalni identitet korisnika uključujući javni ključ i digitalni potpis tijela odnosno institucija koje su zadužene za izdavanje certifikata. Prilikom prijave korisnika, korisnik je dužan ustupiti digitalne certifikate kako bi poslužitelj mogao provjeriti vjerodostojnost digitalnog potpisa i certifikata. Nakon provjere poslužitelj koristi kriptografske metode kako bi potvrdio ima li korisnik ispravan privatni ključ koji je povezan s certifikatom.

4. Biometrijska autentifikacija – Ova metoda oslanja se na provjeru sigurnosti putem jedinstvenih bioloških karakteristika korisnika odnosno pojedinca. Ključne prednosti korištenja biometrijske autentifikacije jest:
    - Laka usporedivost bioloških karakteristika s ovlaštenim značajkama koje su pohranjene u bazama podataka.
    - Kontrola automatskog fizičkog pristupa putem senzora na vratima.
    - Mogućnost dodavanja biometrijske provjere u višefaktorski postupak autentifikacije.

Ovakva vrsta autentifikacije pruža visoku razinu sigurnosti bez stvaranja problema kod korisnika, te je iz tog razloga sve više i više prihvaćena. Uobičajene metode biometrijske provjere autentičnosti su [25]:

- Prepoznavanje karakteristika lica – Ova metoda usklađuje različite karakteristike lica korisnika kako bi dobio traženi pristup. Karakteristike lice sadržane su u bazi podataka. Nedostatak ovakve vrste autentifikacije je prepoznavanje lica pod kutem i korisnici koji izgledaju identično odnosno imaju slične crte lica
- Otisak prstiju – Ova metoda uspoređuje jedinstvene uzorke otisaka prstiju sa otiscima sadržanim u bazi podataka. Neki od novih skenera imaju mogućnost i odrediti odnosno procijeniti vaskularne uzorke u prstima korisnika. Ovakva vrsta autentifikacije trenutno je najpopularnija metoda biometrijske tehnologije unatoč dosta čestim nepravilnostima.
- Prepoznavanje frekvencije glasa – Ova metoda je poznatija kao glasovna biometrija. Radi na način da ispituje govorne uzorke korisnika kako bi se kreirao specifični oblik koji se koristi za autentifikaciju. Sustavi zaštićeni ovakvom vrstom autentifikacije najčešće koristi standardne riječi za identifikaciju.
- Skeneri oka – Ova metoda uključuje tehnologiju za prepoznavanje i analiziranje šarenice i mrežnice oka. Skeneri šarenice emitiraju jarku svjetlost prema oku kako bi se pronašli jedinstveni uzorci u obojenom prstenu oko zjenice oka. Prikupljeni uzorci zatim se uspoređuju s pohranjenim podatcima u bazi podataka. Negativna strana ovakve vrste autentifikacije je što osoba može nositi naočale ili kontaktne leće te provjera autentičnosti može biti netočna.

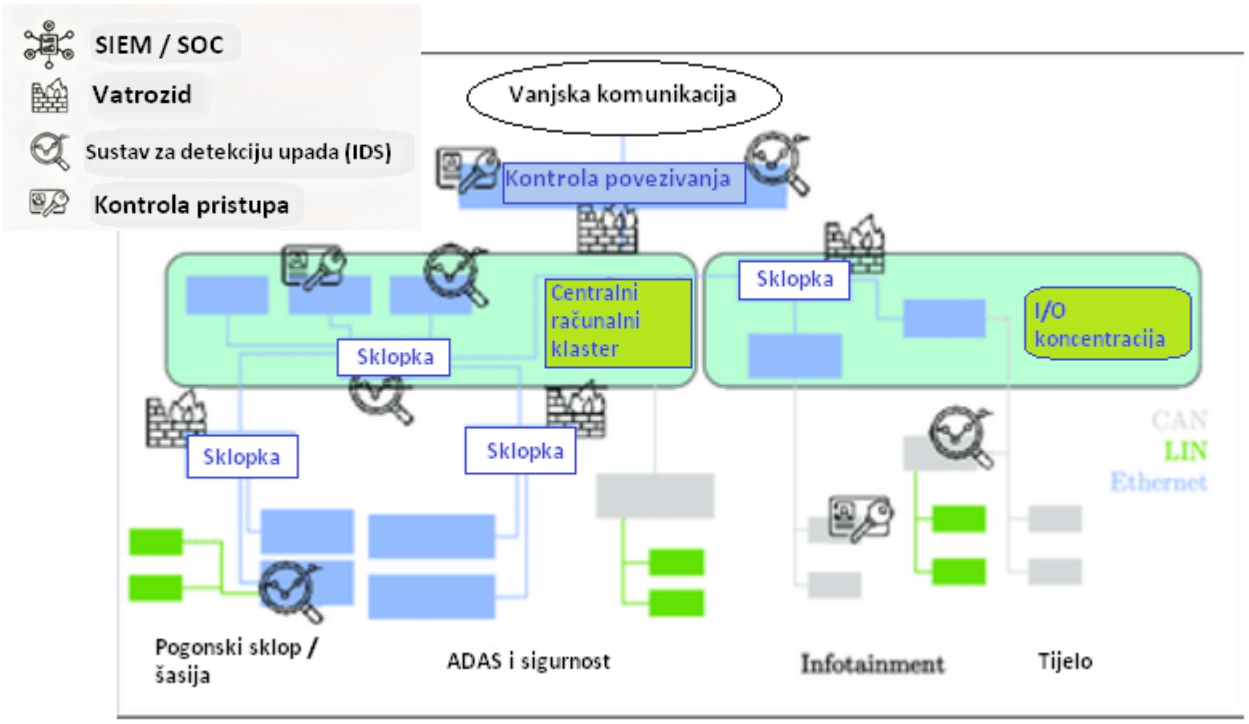
5. Autentifikacije korištenjem tokena – Ova vrsta tehnologije za provjeru autentičnosti temelji se na jedinstvenim tokenima koji omogućuju korisnicima da kad unesu zaporku zauzvrat dobiju jedinstveni šifrirani tekst koji se sastoji od niza nasumičnih znakova [25]. Nakon toga token se može koristiti bez daljnje potrebe za unosom zaporki.

Tehnologija autentifikacije i autorizacije oduvijek se mijenja te tvrtke i ostale organizacije moraju razmišljati dalje od korištenja samo zaporki ili nizova teksta kako bi se autentificirali te kako bi poboljšali korisnička iskustva. Rezultat novih i poboljšanih metoda sprječavaju razne vrste napada i time osiguravaju integritet podataka.

4.2 AUTENTIFIKACIJA I AUTORIZACIJA VOZILA

Povećanje broja međusobnih veza između vozila, predstavlja rizike od napada na interne mreže. Interne mreže skoro uvijek su zaštićene od vanjskih napada, no najčešće nemaju nikakvu unutarnju zaštitu od napadača ili zlonamjernih komponenti koji su u mogućnosti probiti zaštitni sloj [26].

Kako bi se dodatno osigurala mreža u vozilu potrebno je autentificirati i autorizirati sve komponente koje imaju mogućnost komuniciranja s vanjskim svijetom. U vozilu sve komponente trebaju biti autentificirane, a samo ovlaštenim komponentama treba dopustiti komunikaciju odnosno primanje i slanje poruka.



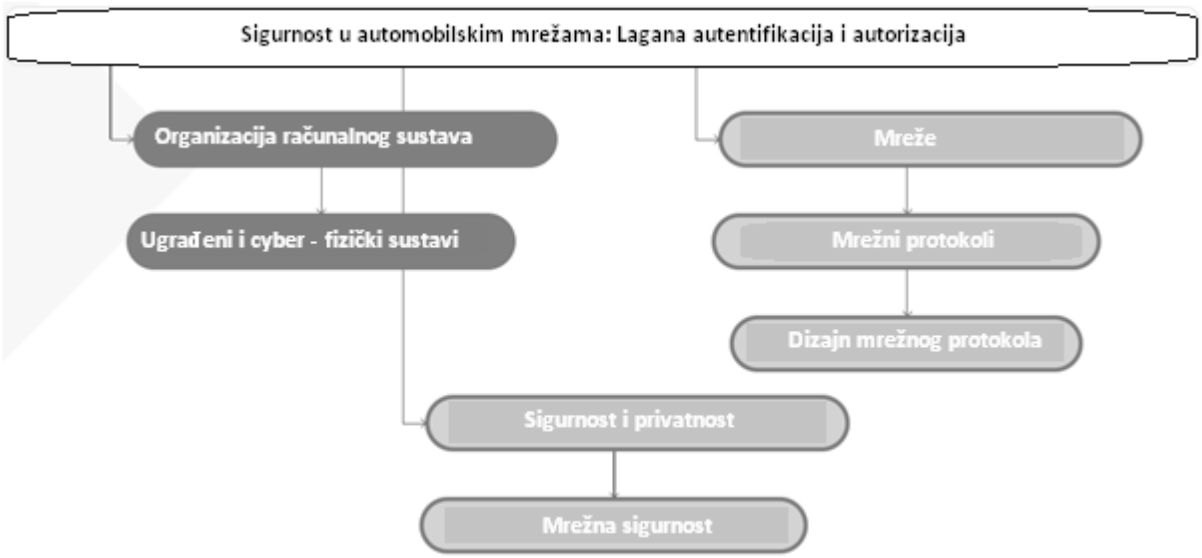
Slika 12. Prikaz zaštite komponenata unutarnje komunikacije u vozilu, [27].

Za provjeru autentičnosti i autorizacije strana kojih sudjeluju u komunikaciji, te za osiguravanje komunikacijskih kanala koristi se kriptografija. Negativna strana korištenja kriptografije je ta što se zbog zahtjeva performansi u stvarnom vremenu mreža u vozilu ne može koristiti najjača vrsta kriptografije. Metoda kriptografije koja se nikako ne može koristiti tijekom rada vozila, zbog svoje kompleksnosti je asimetrična kriptografija.

Metoda koja bi se mogla koristiti za autentifikaciju, kako bi se osigurale automobilske mreže je lagana autentifikacija za sigurne automobilske mreže (Lightweight Authentication for Secure Automotive Networks – LASAN) metoda. LASAN se procjenjuje na dva različita načina [28]:

- Analiziraju se sigurnosna svojstva protokola koristeći utvrđene tehnike provjere protokola koje se temelje na formalnim metodama
- Procjenjuju se vremenski zahtjevi LASAN sustava te ih se uspoređuje s drugim okvirima pomoću novog visoko modularnog diskretnog simulatora događaja za mreže u vozilu.

Lagana autentifikacija za sigurne automobilske mreže (LASAN) sastoji se od koncepata autentifikacijskih protokola kako bi se osigurala ponašanja u stvarnom vremenu te kompletne sigurnosti protokola i procesa potrebnih za integraciju ovakvog autentifikacijskog protokola u automobilskoj industriji.



Slika 13. Proces provjere identiteta sudionika temeljene na kriptografskim mehanizmima, [28].

Sigurnost u automobilskim mrežama je ključna za zaštitu vozila od potencijalnih prijetnji i napada. Jedan od aspekata sigurnosti u automobilskim mrežama je implementacija lagane autentifikacije i autorizacije. Lagana autentifikacija se odnosi na proces provjere identiteta sudionika u mreži, poput vozila ili uređaja koji se povezuju s vozilom. Ova autentifikacija se često temelji na kriptografskim mehanizmima koji osiguravaju da samo ovlašteni sudionici mogu pristupiti mreži i komunicirati s drugim dijelovima sustava.

5. PRIVATNOST I ZAŠTITA PODATAKA

Privatnost i zaštita podataka svodi se na zaštitu digitalnih informacije od neovlaštenog pristupa, krađe ili oštećenja. To je koncept koji obuhvaća svaki aspekt informacijske sigurnosti od fizičke sigurnosti hardvera i uređaja za pohranu do administrativnih kontrola i kontrola pristupa, kao i logičke sigurnosti softverskih aplikacija [29]. Privatnost i zaštita podataka također uključuju i organizacijske politike i procedure. Pravilnom implementacijom snažnih strategija odnosno procedura za sigurnost podataka zaštitit će informacijsku imovinu od aktivnih kibernetičkih napada, te također štite i od unutarnjih prijetnji i ljudskih grešaka koje su i dan danas među najčešćim uzrocima povrede podataka.

Sigurnost podataka odnosi se na implementaciju raznih alata i tehnologija koje poboljšavaju preglednost kritičnih podataka koji se koriste. Ovi alati bi također trebali moći pružiti zaštitu poput enkripcije, maskiranja podataka te redigiranje osjetljivih datoteka, kao i automatizirati izvještaje kako bi se pojednostavnila revizija te kako bi se osiguralo pridržavanje regulatornih zahtjeva. Postoje glavne vrste sigurnosti podataka, a to su [29]:

- Šifriranje podataka – Ova metoda koristi razne algoritme kako bi se obični tekstualni znakovi pretvorili u nečitljiv format, tako da ih samo ovlašteni korisnici mogu čitati. Šifriranje datoteka i baza podataka služe kao posljednja linija obrane osjetljivih podataka prikrivanjem njihovog sadržaja tokenizacijom ili enkripcijom.
- Potpuno brisanje podataka – Ova metoda koristi softver za potpuno brisanje podataka što je sigurnije od standardnog brisanja podataka. Softver za potpuno brisanje može se koristiti na bilo kojem uređaju za pohranjuju.
- Maskiranje podataka – Ova metoda omogućuje timovima u organizacijama korištenje stvarnih podataka. Maskiraju se podatci koji otkrivaju identitet kako bi se razvoj mogao odvijati u usklađenim okruženjima.
- Otpornost podataka – Otpornost podataka određena je time koliko dobro i brzo organizacija podnosi ili se oporavlja od različitih vrsta kvarova. Vrste kvarova uključuju probleme s hardverom, nestašicu struje te ostale događaje koji mogu ili utječu na dostupnost podataka. Brzina oporavka igra ključnu ulogu u smanjenju utjecaja.

Tehnologije i alati usmjereni na sigurnost podataka trebali bi se fokusirati na rastuće izazove svojstvenim osiguravanjem današnjih složenih, hibridnih, distribuiranih računalnih okruženja u više „oblaka“. To uključuje razumijevanje o podatcima, njihovoj lokaciji, praćenju pristupa te blokiranju visokorizičnih aktivnosti i potencijalno opasnih kretanja datoteka. Sveobuhvatna rješenja za zaštitu podataka koja omogućuju raznim poduzećima usvajanje centraliziranog pristupa praćenju te provedbu politike mogu znatno pojednostavniti zadatak. Alati za klasifikaciju i otkrivanje osjetljivih podataka mogu se nalaziti u strukturiranim i nestrukturiranim spremištima podataka, primjerice baze

podataka, platforme za velike podatke te okruženja u „oblaku“. Rješenja za otkrivanje i klasifikaciju podataka automatiziraju proces identifikacije osjetljivih podataka kao i procjenu otklanjanja ranjivosti.

Alati namijenjeni za praćenje aktivnosti datoteka analiziraju obrasce korištenja podataka, omogućujući tako timovima za sigurnost da dobiju uvid tko pristupa podatcima, uočavanje anomalija te identificiranje rizika. Za abnormalne obrasce aktivnosti mogu se implementirati načini dinamičkog blokiranja i upozoravanja. Alati za procjenu rizika i analizu ranjivosti olakšavaju proces otkrivanja i ublažavanja ranjivosti kao što su pogrešne konfiguracije, zastarjeli softver ili slabe lozinke. Također su u mogućnosti identificirati izvore podataka koji su izloženi najvećem riziku. Rješenja za zaštitu podataka s automatiziranim izvještavanjem o usklađenosti može pružiti centralizirani repozitorij za revizijske tragove usklađenosti za cijeli sustav.

5.1 STRATEGIJE ZAŠTITE PODATAKA

Strategije zaštite podataka uključuje ljude, procese i razne tehnologije. Uspostavljanje pravilnih odnosno odgovarajućih kontrola i politika odnosi se na organizacijsku kulturu jednako kao i postavljanje pravog skupa alata. To nam govori da je sigurnost informacije prioritet u svim područjima poduzeća. Postoji nekoliko strategija ta uspješnu zaštitu podataka, a to su [30]:

- Fizička sigurnost korisničkih uređaja i poslužitelja – Bez obzira jesu li podatci pohranjeni u prostorijama korporativnog podatkovnog centra ili u javnom „oblaku“, potrebno je osigurati objekte od uljeza te poduzeti odgovarajuće mjere za suzbijanje požara odnosno kontrolu klime. Ako se radi o javnom oblaku onda pružatelj usluge preuzima odgovornost za zaštitne mjere.

- Upravljanje i kontrola pristupa – U cijelom IT okruženju treba slijediti načelo „najmanje povlaštenog pristupa“. To znači dopuštanje pristupa bazi podataka, mreži te administrativnom računu što manjem broju ljudi i samo onima kojima je to potrebno za obavljanje posla.

- Sigurnost aplikacije i zakrpe – Ova strategija nalaže da sav korišteni softver treba ažurirati na najnoviju verziju što je prije moguće nakon izdavanja zakrpa ili novih verzija.

- Sigurnosne kopije – Odnosi se na održavanje upotrebljivih i temeljito testiranih sigurnosnih kopija svih kritičnih podataka te je ključna komponenta svake snažne strategije sigurnosti podataka. Sve sigurnosne kopije trebale bi odgovarati istim

fizičkim i logičkim sigurnosnim kontrolama koje upravljaju pristupom primarnim bazama podataka i temeljnim sustavima.

- Edukacija zaposlenika – Edukacija i obuka zaposlenika o važnosti dobre sigurnosne prakse, o jačinama i propustima zaporki te o prepoznavanju napada koji se odnosi na društveni inženjering pretvara ih u odgovorne i samostalne zaposlenike koji mogu imati ključnu ulogu u zaštiti podataka.

- Nadzor i kontrola sigurnosti mreže i krajnjih točaka – Implementacijom sveobuhvatnog paketa alata i platformi za upravljanje prijetnjama, otkrivanje i odgovor na lokalno okruženje te platforme u „oblaku“ mogu ublažiti rizike i smanjiti vjerojatnost kršenja.

Strategija za zaštitu podataka trebala bi definirati koje vrste podataka treba sigurnosno kopirati, kako se podatci trebaju oporaviti prilikom katastrofe, te koji se mediji za pohranu trebaju koristiti. Sve navedene mjere trebale bi biti uključene u inicijative za kontinuitet poslovanja te oporavak od katastrofe.

5.2 REGULACIJE I TRENDOVI ZAŠTITE PODATAKA

Opća uredba EU o zaštiti podataka (General Data Protection Regulation - GDPR) najjači je i najefikasniji je zakon o privatnosti i sigurnosti na svijetu. Ovom su uredbom modernizirana i ažurirana načela Direktive o zaštiti podataka iz 1995. godine. Usvojen je 2016. godine, a u primjeni je od 25. svibnja 2018. godine [31]. GDPR definira temeljna prava pojedinca u digitalnom dobu, obveze onih koji obrađuju podatke, metode za osiguranje sukladnosti, sankcije za one koji krše pravila. GDPR je uredba o zaštiti fizičkih osoba prilikom obrade osobnih podataka te slobodnom kretanju tih podataka. Ova uredba navodi prava nositelja podataka odnosno prava pojedinaca čiji se osobni podaci obrađuju. Ova pojačana prava omogućuju pojedincima više kontrole nad njihovim osobnim podacima. Neke od uredbi su [31]:

- Potreba za jasnim pristankom pojedinca na obradu njegovih osobnih podataka.
- Lakši pristup osobnim podatcima.
- Pravo na ispravak, brisanje ili kompletno brisanje odnosno „biti zaboravljen“.
- Pravo na prigovor, uključujući korištenje osobnih podataka u svrhu „profiliranja“.
- Pravo na prijenos podataka s jednog pružatelja usluga na drugog.

Uredba također propisuje obvezu za one koji su odgovorni za obradu podataka tako da pojedincima daju transparentne i lako dostupne informacije o obradi njihovih podataka. To uključuje obvezu provedbe odgovarajućih sigurnosnih mjera koje moraju biti u skladu s rizikom uključenim u radnje za obradu podataka koje se izvršavaju. Voditelji obrade

podataka dužni su u određenim slučajevima dostaviti obavijest o povredama osobnih podataka. Tijela javnih vlasti i tvrtke koje obavljaju specifične rizične poslove obrade podataka također će morati imenovati službenika za zaštitu podataka.

Primjena pravila o zaštiti podataka potvrđuje postojeću obvezu država članica da uspostave neovisno nadzorno tijelo na nacionalnoj razini te da se uspostavi mehanizam za stvaranje dosljednosti u primjeni zakona o zaštiti podataka diljem EU – a. GDPR je sposoban ustanoviti da se u prekograničnim slučajevima u koje je uključeno nekoliko nadzornih tijela donosi jedna nadzorna odluka. Ovo je jedno od načela, poznatije i kao načelo „one – stop – shop“ koje znači da će se tvrtka koja ima nekoliko podružnica u nekoliko država članica morati imati posla samo s tijelom za zaštitu podataka u onoj državi u kojoj joj se nalazi sjedište [31]. Europski odbor za zaštitu podataka osigurava potpunu primjenu GDPR – a. Odbor se sastoji od predstavnika 27 neovisnih nadzornih tijela.

Trendovi zaštite podataka odnosi se na novije tehnologije poput umjetne inteligencije (Artificial Intelligence - AI), kvantnih računala te Multicloud sigurnosti. Upotreba umjetne inteligencije povećava sposobnost sigurnosnih sustava zato jer može obraditi velike količine podataka u prihvatljivom vremenu. Podskup umjetne inteligencije odnosno kognitivno računalstvo obavlja identične zadatke kao i drugi sustavi umjetne inteligencije, no to radi simulirajući ljudske misaone procese. Vezano za sigurnost podataka, omogućuje relativno brzo donošenje odluka u za vrijeme kritične potrebe. Kako rastu mogućnosti oblaka proširila se definicija sigurnosti podataka. U današnje vrijeme organizacije zahtijevaju složenije rješenja jer ne traže zaštitu samo za podatke, nego i za aplikacije i vlasničke poslovne procese koji se izvode preko javnih i privatnih oblaka. Kvanta računala odnosno kvantna tehnologija obećava da će eksponencijalno zamijeniti mnoge tradicionalne tehnologije. Algoritmi za šifriranje postat će mnogo složeniji i mnogo sigurniji nego današnji algoritmi.

6. KRIPTOGRAFSKI STANDARDI I NORME

U današnje vrijeme postoji niz kriptografskih standarda ovisno o njihovoj upotrebi. Nacionalni institut za standarde i tehnologiju (National Institute if Standards and Technology – NIST) je tijelo zakonski odgovorno za razvoj kriptografskih standarda i smjernica za zaštitu informacija o ne nacionalnim sigurnosnim sustavima koji se široko koriste u saveznoj vladi [32]. Zajednica su proteklih godine proširila te danas radi na globalnoj razini, kao što i interes za postojanje sustava koji će na prikladan način štititi i osigurati visoku razinu sigurnosti digitaliziranih informacija. NIST zajednica uključuje razne akademske stručnjake, vladine agencije te ostale organizacije koje su voljne prihvatiti NIST kriptografske standarde i smjernice. Ključni dio za razvoj najsigurnijih i najpouzdanijih kriptografskih standarda su otvoreni i transparentni procesi. NIST nastoji uključiti sve svoje dionike procesa te kontinuirano radi na jačanju utjecaja u ovom području. NIST se vodi definicijom da robusni, široko razumljivi i participativni razvojni procesi proizvode najjače, najpouzdanije, najučinkovitije te široko prihvaćene kriptografske standarde i smjernice. Principi za određivanje kriptografskih standarda i smjernica su [32]:

- Transparentnost – Sve zainteresirane strane moraju imati pristup bitnim informacijama u vezi aktivnosti vezanih za standarde i smjernice tijekom cijelog razvojnog procesa. Transparentnost se odnosi na razvoj i dokumentiranje kriptografskih standarda s obzirom na područje fokusa, kriterije odabira i ocjenjivanje, specifikacije, sigurnost te druge izvedbene karakteristike.
- Otvorenost – Sudjelovanje je otvoreno za sve zainteresirane strane. Svi dionici imaju priliku za značajno uključivanje u proces razvoja standarda i smjernica
- Ravnoteža – Nastoji se postići ravnoteža interesa među dionicima, na način da se određuju zajednički interesi za razvoj kriptografskih standarda i smjernica koje su sigurne i učinkovite, te s naglaskom na promicanje interoperabilnosti. Zahtijevaju se podaci i dokazi širokog raspona dionika, industrija te akademskih zajednica kako bi se da su standardi jaki, praktični te da zadovoljavaju potrebe savezne vlade kao i šire zajednice korisnika
- Integritet – NIST služi kao objektivan tehnički autoritet za razvijanje kriptografskih standarda i smjernica. Prilikom ocjenjivanja odabira i standardizacije kriptografskih algoritama, nastoji se zadržati objektivnost dok se oblikuju i dokumentiraju odluke. Procesi odabira i razvojni standardi provodite će se s jasnim kriterijima te čuvati protiv nedopuštenog ili neprimjerenog utjecaja uzimajući u obzir legitimne interese dionika. Dio procesa razvoja standarda je izbjegavanje ili prikladno upravljanje sukobima interesa, sljedeći postupke kao što su upravljanje rizikom koji predstavljaju ti sukobi te osiguravanje odgovarajuće obuke za osoblje.
- Tehničke zasluge – Odluke tijekom razvoja kriptografskih standarda i smjernica temelje se na tehničkim vrijednostima prijedloga uz vođenje računa o

privatnosti, sigurnosti, politici i poslovnim razmatranjima. NIST nastoji standardizirati algoritme za sigurnu kriptografiju, sheme te načine rada čija su sigurnosna svojstva dobro poznata i učinkovita te otporna na zloupotrebu i promiču interoperabilnost. Pregled tehničkih vrijednosti uključuje preciznu i formalnu izjavu o sigurnosnim zahtjevima koji se temelje na pretpostavki minimalne sigurnosti te su potkrijepljeni dokumentiranom kriptoanalizom i smanjenom sigurnosti.

- Globalna prihvatljivost – Iako je zakonska osnova za rad u kriptografiji potreba za zaštitom nenacionalnih sigurnosnih saveznih informacijskih sustava, NIST standardi su temelj mnogih proizvoda i usluga informacijske tehnologije. NIST organizacija prepoznaje ulogu svojih kriptografskih standarda u osiguravanju konkurentnosti u isporuci proizvoda i usluga, te je fokusiran na osiguranje standarda i smjernica kako bi bili međunarodno prihvaćeni.
- Upotrebljivost – Cilj je razviti kriptografske smjernice i standarde koji pomažu implementatorima stvoriti sigurne i upotrebljive sustave za korisnike koji podržavaju poslovne potrebe i tijekom rada. Takvi sustavi moraju se moći lako implementirati u postojeće i buduće sustave i planove. Kriptografske standarde i smjernice treba odabrati na način da se zahtjevi za korisnike i implementatore svedu na minimum kao i neželjene posljedice ljudskih pogrešaka i kvarova opreme.
- Kontinuirano poboljšanje – Kako se kriptografski algoritmi razvijaju na dnevnoj bazi odnosno i tijekom upotrebe zajednica se potiče da identificiraju slabosti, ranjivosti ili neke druge nedostatke u algoritmima navedenim u NIST publikacijama. Prilikom identificiranja ozbiljnih problema, NIST se povezuje sa širom kriptografskom zajednicom kako bi se što prije riješili. Provode se razna istraživanja kako bi se omogućili nove kriptografske napretke koji mogu utjecati na prikladnost standarda i smjernica.
- Inovacija i intelektualno vlasništvo – Tijekom razvijanja kriptografskih standarda i smjernica za nenacionalne sigurnosne sustave, jaka sklonost odnosni se na korisnike te na rješenja koja nisu opterećena patentiranim tehnologijama koje plaćaju postotke nositeljima prava. Preferira se odabir algoritama koji su neopterećeni tvrdnjama o intelektualnom vlasništvu, no mogu se odabrati i algoritmi s povezanim patentima ako tehničke koristi nadmašuju potencijalne troškove koji nastaju prilikom implementacije patentirane tehnologije. Važno je uravnotežiti prava nositelja IP – a i onih koji žele koristiti tehnologije uključujući prava intelektualnog vlasništva.

Trenutni standardi i smjernice današnjih kriptosustava uključuju algoritme odnosno tehnike blok šifriranja, pregled kripto publikacija, digitalne potpise, hash funkcije, laganu kriptografiju (engl. Lightweight cryptography), kodove za provjeru autentičnosti poruka (engl. Message Authentication Code), kriptografije s pragom više strana, postkvantne

kriptografije (engl. Post – Quantum Cryptography), kriptografije za poboljšanje privatnosti (engl. Privacy – Enhancing Cryptography) te nasumično generiranje bitova.

Odobreni algoritmi blokovnih šifri koje su povoljne za korištenje te za primjenu kod kriptografske zaštite odnosno za dešifriranje i šifriranje su AES i 3DES, dok su prethodno odobreni algoritmi DES i Skipjack. Međutim DES i Skipjack odobrenje je povučeno zbog nedostatka sigurnosti te zbog uspješnih napada na poruke kriptirane putem tih algoritama [33]. Digitalni potpis jamči da je navedeni potpisanih zaista potpisao neki tekst ili informaciju te da podatci nisu promijenjeni nakon generiranja potpisa. Federalni standard za obradu informacija (Federal Standard for Information Processing – FIPS) navodi da Standard za digitalni potpis (Digital Signature Standard – DSS) mora koristiti sljedeća tri algoritma odobrena od strane NIST – a, a to su: DSA, RSA i ECDSA [34]. Sva tri se koriste za generiranje i provjeru digitalnih potpisa u kombinaciji s odobrenom hash funkcijom.

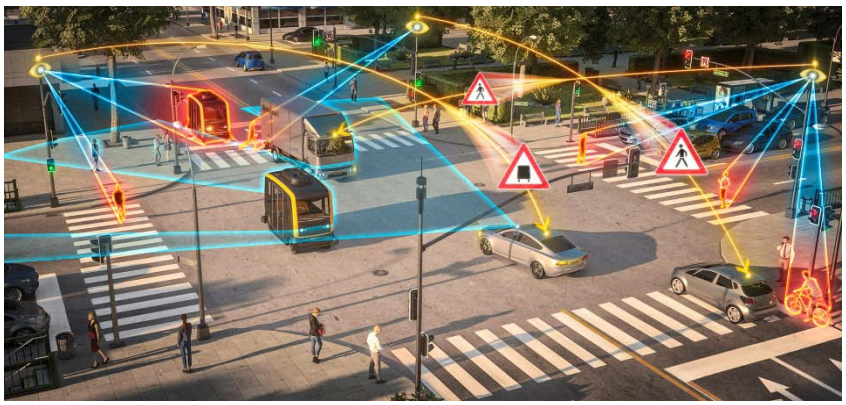
Hash algoritam koristi se za preslikavanje poruke proizvoljne duljine u sažetak poruke fiksne duljine. Odobreni hash algoritmi koji se koriste za generiranje sažetog prikaza poruke definirani su u dva savezna standarda za obradu informacija: FIPS 180 – 4, Secure Hash Standard i FIPS 202, SHA – 3 standard [35]. FIPS 180 – 4 definira sedam hash algoritama: SHA – 1 (Secure Hash Algorithm – 1) i SHA – 2 obitelj algoritama SHA – 224, SHA – 256, SHA – 384, SHA – 512, SHA – 512/224 i SHA – 512/256. SHA – 1 je zabranjen 2011. godine zbog uspješnih napada čistom silom (engl Brute Force). FIPS 202 navodi nove SHA – 3 inačice funkcija koje se temelje na permutaciji temeljenu na KECCAK – u. FIPS 202 specificira četiri hash algoritma fiksne duljine: SHA3 – 224, SHA3 – 256, SHA3 – 384 i SHA3 – 512 te dvije blisko povezane funkcije proširivog izlaza (XOR), a to su: SHAKE128 i SHAKE256 [35]. Trenutačno su samo četiri SHA – 3 algoritma fiksne duljine odobreni algoritmi raspršivanja, pružajući alternative SHA – 2 sklopu funkcija raspršivanja. XOF funkcije mogu biti specijalizirani za hash funkcije.

Uspjeh i standardi lagane kriptografije oslanjaju se na napore istraživača iz kriptografske zajednice koji pružaju sigurnost, implementaciju te analizu performansi algoritama. Potiče se javna procjena i objavljivanje rezultata tijekom cijelog procesa kako bi se pronašla najbolja opcija za šifriranje odnosno dešifriranje podataka.

Posljednjih godina provedena su brojna istraživanja o kvantnim računalima odnosno strojevima koji iskorištavaju kvantno – mehaničke fenomene za rješavanje matematičkih problema koji su teško rješivi za konvencionalna računala. Predviđa se da će kvantna računala biti u mogućnosti razbiti mnoge kriptosustave s javnim ključem koji se trenutno koriste. Cilj postkvantne kriptografije je razviti kriptografske sustave koji su zaštićeni od kvantnih i klasičnih računala, te koji mogu biti interoperabilni s postojećim komunikacijskim protokolima i mrežama.

7. ANALIZA PRAKTIČNIH PRIMJERA PRIMJENE KRIPTOGRAFIJE U PODRUČJU INTELIGENTNIH TRANSPORTNIH SUSTAVA

Primjer primjene kriptografije u području inteligentnih transportnih sustava omogućava komunikaciju između vozila (Vehicle – to – Vehicle – V2V) i između vozila i infrastrukture (Vehicle – to – Infrastructure – V2I). V2V i V2I komunikacija koristi se u pametnim prometnim sustavima koji najčešće koriste namjensku komunikaciju kratkog dometa (Dedicated Short Range Communication – DSRC) ili *C – V2X* (engl. Cellular Vehicle – to – Everything) tehnologije kako bi vozila mogla uspješno komunicirati i razmjenjivati informacije s drugim vozilima i prometnom infrastrukturom. Tehnologije DSRC i C – V2X koriste specifične radiofrekvencijske kanale za bežičnu komunikaciju među vozilima, a protokoli i enkapsulacija podataka unutar tih kanala obično su standardizirani na višem sloju aplikacije [36].



Slika 14. Primjer DSRC i C – V2X komunikacije s infrastrukturom i ostalim prometnim entitetima, [36].

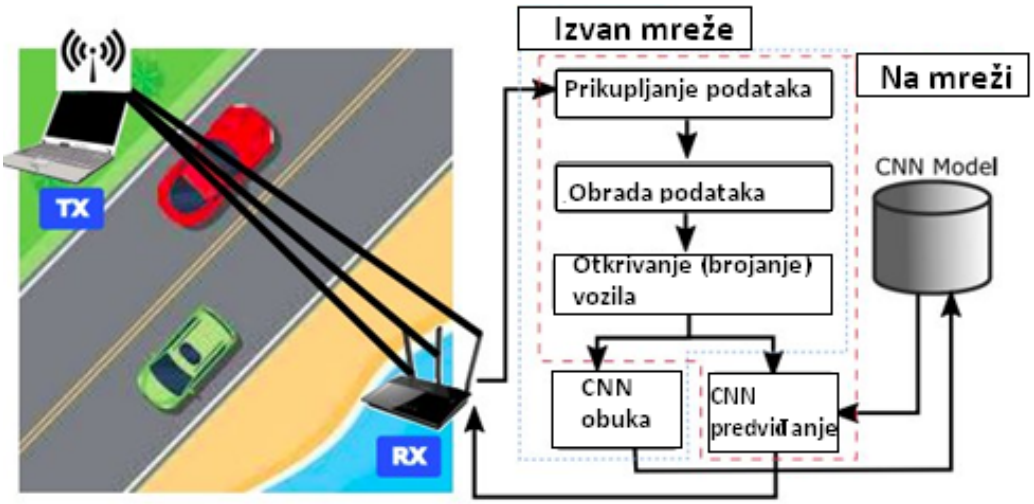
Kriptografija se koristi kako bi se osigurala povjerljivost, sigurnost te autentičnost podataka koji se prenose između vozila i infrastrukture. Primjer primjene kriptografije u komunikaciji vozila uključuje:

1. Šifriranje podataka – Podaci koji se prenose između vozila i infrastrukture moraju biti šifrirani kako bi se osigurala njihova povjerljivost.
2. Autentifikacija – Prilikom autentifikacije također koristimo kriptografiju. Svako vozilo i svaki dio infrastrukture sadrže digitalne certifikate i javne odnosno privatne ključeve. Ključevi se koriste za identifikaciju te provjeru integriteta podataka. Primjerice, digitalni certifikati mogu se koristiti za potvrdu identiteta vozila, čime se sprječava neovlašteni pristup komunikaciji.
3. Potpisivanje poruka – Potpisivanje poruka služi kako bi se provjerio odnosno osigurao integritet podataka, jer se bilo kakve promjene u podacima mogu

otkriti prilikom provjere digitalnog potpisa. Time se sprječavaju neovlaštene manipulacije s podacima u komunikaciji.

Uz DSRC i C –V2X komunikaciju, postoje i slučaju gdje dva vozila komuniciraju putem Wi – Fi mreže ili su povezani putem Bluetooth mreže. Vozila mogu biti opremljena Wi – Fi uređajima koji podržavaju bežičnu komunikaciju. Princip rada bazira se na tome da svako vozilo može djelovati kao Wi – Fi pristupna točka (engl. Access Point) ili klijent (engl. Client) te koristiti određene Wi – Fi protokole za razmjenu podataka. Primjerice, vozilo A djeluje kao pristupna točka , dok vozilo B ima ulogu klijenta te se povezuje na tu pristupnu točku.

Bluetooth mreža koristi Bluetooth tehnologiju za razmjenu podataka. Bluetooth tehnologija osigurava bežičnu komunikaciju između dva uređaja koja su međusobno uparena. Uparena vozila stvaraju vezu kratkog dometa. Nakon što su vozila uparena i u dometu, tada mogu razmjenjivati podatke putem bluetooth protokola. Kada su vozila povezana putem Bluetooth mreže ili Wi – Fi mreže, koriste se odgovarajući protokoli za razmjenu podataka. Najčešći protokoli koji se koriste se TCP/IP protokol, HTTP protokol te drugi protokoli ovisno o vrsti upotrebe.



Slika 15. Sustav za praćenje prometa temeljen na Wi – Fi mreži koji koristi proces dubokog učenja, [37].

Ovaj relativno novi sustav razvijen od tima istraživača sa Sveučilišta u Memphisu kombinira Wi – Fi uređaje i dubinsko učenje kako bi što učinkovitije pratio promet. Ovo je jedna od ključnih komponenata u inteligentnim transportnim sustavima koja ima za cilj poboljšati učinkovitost i sigurnost transporta.

Sustav radi na način da prikuplja podatke o prometu koji se odnosne na performanse sustava mjereći parametre kao što su broj vozila, gustoću vozila, brzinu i klasu. Istraživači su dizajnirali konvolucijsku neuronsku mrežu (Convolutional – neural – Network – CNN) koja može automatski dohvatiti optimalne značajke podataka, te se zatim uvježbali model na

prethodno prikupljenim i obrađenim podatcima [37]. Uz konvolucijske neuronske mreže koristile su se i druge tehnike za poboljšanje točnosti klasifikacije modela, primjerice ublažavanjem učinaka uzrokovanih preprekama oko vozila, uključujući predmete ili ljude koji se kreću malim brzinama.

Vrsta podataka koju je potrebno šifrirati kako bi spriječili propuste, odnose se na brzinu kretanja, položaj vozila, smjer kretanja, geolokacijski podaci te ostale bitne podatke vezane za stanje vozila. Prilikom slanja podataka koristimo kriptografiju kako bi zaštitili podatke. Proces slanja podataka uključuje:

- Generiranje ključeva – Svako vozilo mora generirati javni i privatni ključ. Javni ključ može se sigurno razmijeniti između vozila-
- Enkripcija podataka – Prije slanja podaci se šifriraju koristeći javni ključ te se pretvaraju u nesmislen oblik. Enkripcija se obavlja algoritmom za koji se zna da je siguran, u ovom slučaju može se koristiti AES simetrični kriptografski algoritam.
- Prijenos podataka – Nakon što su podaci šifrirani, šalju se putem raznih komunikacijskih kanala.
- Dekripcija podataka – Primljeni podaci dešifriraju se privatnim ključem vozila koji prima podatke.
- Provjera integriteta – Integritet podataka provjerava se digitalnim potpisom na način da vozilo koje šalje podatke generira potpis na temelju izvornih podataka i privatnog ključa, te zatim vozilo koje prima podatke provjerava digitalni potpis odnosno integritet podataka javnim ključem vozila koji šalje podatke.

Ovime smo ukratko opisali proces slanja podataka vozilima ili prometnoj infrastrukturi na siguran i učinkovit način. Koristeći svih pet koraka na siguran i odgovoran način sprječavaju se razni mogući napadi na prometnu infrastrukturu ili prometne entitete te se osigurava pouzdanost i stabilnost sustava.

8. ZAKLJUČAK

Primjena kriptografije u inteligentnim transportnim sustavima vrlo je važan postupak za očuvanje prometnih podataka, sprječavajući neovlašteni odnosno neautorizirani pristup ili čitanje osjetljivih informacija. Korištenjem kriptografije osigurava se sigurnost, povjerljivost te autentičnost podataka. Trenutni standardi i smjernice današnjih kriptosustava uključuju algoritme odnosno tehnike blok šifriranja, pregled kripto publikacija, digitalne potpise, hash funkcije, laganu kriptografiju (engl. Lightweight cryptography), kodove za provjeru autentičnosti poruka (engl. Message Authentication Code), kriptografije s pragom više strana, postkvantne kriptografije (engl. Post – Quantum Cryptography), kriptografije za poboljšanje privatnosti (engl. Privacy – Enhancing Cryptography) te nasumično generiranje bitova.

Kriptografske metode i sustavi služe nam za sigurno prenošenje informacija među korisnicima iako je sadržaj poruke vidljiv on je kriptiran i nerazuman je svima onima kojima nije dopušteno vidjeti pravi sadržaj poruke. Kriptografija je razumijevanje i proučavanje raznih tehnika za sigurnu komunikaciju u kojoj sudjeluju i treće strane. Glavna grana kriptografije je matematika odnosno aritmetika te računalne znanosti. U današnje vrijeme postoji niz kriptografskih standarda ovisno o njihovoj upotrebi. Nacionalni institut za standarde i tehnologiju (National Institute if Standards and Technology – NIST) je tijelo zakonski odgovorno za razvoj kriptografskih standarda i smjernica za zaštitu informacija o ne nacionalnim sigurnosnim sustavima koji se široko koriste u saveznoj vladi. Kako bi se osiguralo da standardi i smjernice pružaju visoku kvalitetu, ekonomičnu sigurnost mehanizma, NIST blisko surađuje sa širokom zajednicom dionika kako bi uspješnije identificirao područja potrebe te kako bi se mogli razviti standardi i dodatne smjernice.

Primjer primjene kriptografije u području inteligentnih transportnih sustava omogućava sigurnu komunikaciju između vozila (Vehicle – to – Vehicle – V2V) i između vozila i infrastrukture (Vehicle – to – Infrastructure – V2I). V2V i V2I komunikacija koristi se u pametnim prometnim sustavima koji najčešće koriste namjensku komunikaciju kratkog dometa (Dedicated Short Range Communication – DSRC) ili *C – V2X* (engl. Cellular Vehicle – to – Everything) tehnologije kako bi vozila mogla uspješno komunicirati i razmjenjivati informacije s drugim vozilima i prometnom infrastrukturom.

Vrsta podataka koju je potrebno šifrirati kako bi spriječili propuste, odnose se na brzinu kretanja, položaj vozila, smjer kretanja, geolokacijski podaci te ostale bitne podatke vezane za stanje vozila. Prilikom slanja podataka koristimo kriptografiju kako bi zaštitili podatke.

9. LITERATURA

1. Yiheng Feng, Shihong Huang, Qi Alfred Chen, Henry X.Liu, Z. Morley Mao. *„Vulnerability of traffic system under cyber-attacks using falsified data“* Preuzeto s: https://www.ics.uci.edu/~alfchen/pubs/yiheng_trb18.pdf [Pristupljeno: 20.5.2023.].

2. InfoSec Institute. *„Network Traffic Analysis for Incident Response: Basic Protocols in Networking."* Preuzeto s: https://resources.infosecinstitute.com/topic/network-traffic-analysis-for-ir-basic-protocols-in-networking/ [Pristupljeno: 20.5.2023.].

3. Imperva. (n.d.). *„TCP (Transmission Control Protocol).“* Preuzeto s: https://www.imperva.com/learn/DDOS/tcp-transmission-control-protocol/ [Pristupljeno: 20.5.2023.].

4. Nikola Šoltić. *„Wi-Fi mreža Čakovec".* Disertacija. Međimursko veleučilište u Čakovcu, Čakovec, 2015. Nacionalni repozitorij završnih i diplomskih radova: ZIR Nacionalna i sveučilišna knjižnica u Zagrebu. Preuzeto s: https://zir.nsk.hr/islandora/object/mev%3A282 [Pristupljeno 20. 5. 2023.]

5. Microsoft. (n.d.). *„What is a DDOS attack?.“* Preuzeto s: https://www.microsoft.com/hr-hr/security/business/security-101/what-is-a-DDOS-attack/ [Pristupljeno: 21.5.2023.].

6. Code42. (n.d.). *„Detecting and Responding to Unauthorized Access*.“ Preuzeto s: https://www.code42.com/blog/detecting-and-responding-to-unauthorized-access/ [Pristupljeno: 21.5.2023.].

7. MakeUseOf. (n.d.). *„What is Data Manipulation and How Can You Avoid It?*.“ Preuzeto s: https://www.makeuseof.com/what-is-data-manipulation-and-how-can-you-avoid-it/ [Pristupljeno: 22.5.2023.].

8. TechTarget. (n.d.). *„Car hacking.“* Preuzeto s: https://www.techtarget.com/iotagenda/definition/car-hacking [Pristupljeno: 22.5.2023.].

9. Petit, J. & Shladover, S. E. (2015). *„Potential cyberattacks on automated vehicles“.* IEEE Transactions on Intelligent Transportation Systems, Preuzeto s: https://www.researchgate.net/publication/266780575_Potential_Cyberattacks_on_Automated_Vehicles [Pristupljeno: 23.5.2023.].

10. Black Knight GPS Tracking. (2018). *„What is Signal Jamming?.“* Preuzeto s: https://www.blackknighttracking.com/post/2018/09/19/what-is-signal-jamming [Pristupljeno: 24.5.2023.].

11. ScienceDirect. (n.d.). *„Cryptographic Systems and Methods.“* Preuzeto s: https://www.sciencedirect.com/science/article/abs/pii/S0140366499000304 [Pristupljeno: 24.5.2023.].

12. ScienceDirect. (n.d.). *„Symmetric Cryptography.“* Preuzeto s: https://www.sciencedirect.com/topics/computer-science/symmetric-cryptography [Pristupljeno: 25.5.2023.].

13. Delfs, H. & Knebl, H. (2007). *„Symmetric-key encryption".* Introduction to cryptography: principles and applications. Springer. ISBN 9783540492436. Preuzeto s: https://books.google.hr/books?id=Nnvhz_VqAS4C&pg=PA11&redir_esc=y#v=onepage&q&f=false [Pristupljeno: 25.5.2023.].

14. CIS. (2003). *„DES Algorithm.“* Preuzeto s: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-06-24.pdf [Pristupljeno: 26.5.2023.].

15. Feasyblue. (n.d.). *„AES (Advanced Encryption Standard) Encryption."* Preuzeto s: http://ba.feasyblue.com/info/aes-advanced-encryption-standard-encryption-76701554.html [Pristupljeno: 26.5.2023.].

16. CIS. (2003). *„AES Algorithm.“* Preuzeto s: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-08-37.pdf [Pristupljeno: 27.5.2023.].

17. Dujella, A. (n.d.). *„Kriptografija: Kriptosustavi s javnim ključem.“*. Preuzeto s: https://web.math.pmf.unizg.hr/~duje/kript/kriptografija.html [Pristupljeno: 28.5.2023.].

18. Calderbank, M. (2007-08-20). *„The RSA Cryptosystem: History, Algorithm, Primes"*, Preuzeto s: http://203.223.190.196:86/RMVLMS/claroline/backends/download.php?url=L2Vzc2VudGlhbHMgb2YgbWF0aHMgaW4gRGF0YSBTY2llbmNlL1JTQSAoY3J5cHRvc3lzdGVtKSAtIFdpa2lwZWRpYS5wZGY%3D&cidReset=true&cidReq=MSC2019 [Pristupljeno: 29.5.2023.].

19. MDPI. (n.d.). *„RSA Cryptography: Overview and Perspectives.“* Preuzeto s: https://www.mdpi.com/2079-9292/9/2/246 [Pristupljeno: 30.5.2023.].

20. Koblitz, N. (1987). Mathematics of Computation, *“Elliptic curve cryptosystems”.* Preuzeto s: https://www.ams.org/journals/mcom/1987-48-177/S0025-5718-1987-0866109-5/ [Pristupljeno: 31.5.2023.].

21. Avi Networks. (n.d.). Elliptic *„Curve Cryptography.“* Preuzeto s: https://avinetworks.com/glossary/elliptic-curve-cryptography/ [Pristupljeno: 31.5.2023.].

22. The Economic Times. *„What is Authentication? Definition of Authentication, Authentication Meaning."* Preuzeto s: https://economictimes.indiatimes.com/definition/authentication [Pristupljeno: 1.6.2023.].

23. Auth0. (n.d.). *„What is Authorization?"* Preuzeto s: https://auth0.com/intro-to-iam/what-is-authorization [Pristupljeno: 2.6.2023.].

24. ResearchGate. (n.d.). *„User Authorization Flow."* Preuzeto s: https://www.researchgate.net/figure/User-Authorization-Flow-2_fig2_309365153 [Pristupljeno: 2.6.2023.].

25. ID R&D. (n.d.). *„5 Authentication Methods That Can Prevent the Next Breach.“* Preuzeto s: https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/ [Pristupljeno: 2.6.2023.].

26. Cornell Univerity (n.d.). *„Security in Automotive Networks: Lightweight Authentication and Authorization.“* Preuzeto s: https://arxiv.org/abs/1703.03652 [Pristupljeno: 3.6.2023.].

27. ResearchGate. (n.d.). *„The connected vehicle, its internal network, and common security measures - Schematic."* Preuzeto s: https://www.researchgate.net/figure/The-connected-vehicle-its-internal-network-and-common-security-measures-Schematic_fig1_353468613 [Pristupljeno: 4.6.2023.].

28. Association for Computing Machinery (n.d.). *„Security in Automotive Networks: Lightweight Authentication and Authorization.“* Preuzeto s: https://dl.acm.org/doi/abs/10.1145/2960407 [Pristupljeno: 4.6.2023.].

29. IT Business Edge. *„Knowing Your Data to Protect Your Data."* 2017-09-25. Preuzeto s: https://www.itbusinessedge.com/it-management/knowing-your-data-to-protect-your-data/ [Pristupljeno: 4.6.2023.].

30. IBM. (n.d.). *„Data security."* Preuzeto s: https://www.ibm.com/topics/data-security [Pristupljeno: 5.6.2023.].

31. Europsko vijeće. (n.d.). *„Data protection regulation."* Preuzeto s: https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/ [Pristupljeno: 5.6.2023.].

32. Nacionalni institut za standarde i tehnologiju (NIST). (n.d.). *„NIST Interagency Report 7977: Algorithm and Key Lengths for Use with the SHA-256 Algorithm for Cryptographic Applications."* Preuzeto s: https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.7977.pdf [Pristupljeno: 6.6.2023.].

33. Nacionalni institut za standarde i tehnologiju (NIST). (n.d.). *„Block Cipher Techniques."* Preuzeto s: https://csrc.nist.gov/projects/block-cipher-techniques [Pristupljeno: 7.6.2023.].

34. Nacionalni institut za standarde i tehnologiju (NIST). (n.d.). *„Digital Signatures."* Preuzeto s: https://csrc.nist.gov/projects/digital-signatures [Pristupljeno: 8.6.2023.].

35. Nacionalni institut za standarde i tehnologiju (NIST). (n.d.). *„Hash functions."* Preuzeto s: https://csrc.nist.gov/projects/hash-functions [Pristupljeno: 9.6.2023.].

36. ASTER. (n.d.). *„V2X: Why Should We Accelerate Adoption?"* Preuzeto s: https://aster-fab.com/v2x-why-should-we-accelerate-adoption/ [Pristupljeno: 10.6.2023.].

37. TechXplore. (2019, siječanj). *„DeepWiTraffic: Wi-Fi-based traffic deep learning system.„* Preuzeto s: https://techxplore.com/news/2019-01-deepwitraffic-wi-fi-based-traffic-deep.html [Pristupljeno: 11.6.2023.].

POPIS KRATICA I AKRONIMA

1. ITS (Intelligent Transportation System) Sustav inteligentnog prometa
2. I2I (Infrastructure to Infrastructure) Komunikacija infrastrukture sa infrastrukturom
3. V2I (Vehicle to Infrastructure) Komunikacija vozila i infrastrukture
4. V2V (Vehicle to Vehicle) Komunikacija vozila i vozila
5. TCP (Transmission Control Protocol) Protokol za kontrolu prijenosa
6. UDP (User Datagram Protocol) Protokol korisničkog datagrama
7. HTTP (Hypertext Transfer Protocol) Hiper sustavni protokol prijenosa
8. HTTPS (Hypertext Transfer Protocol Secure) Hiper sustavni sigurnosni protokol prijenosa
9. FTP (File Transfer Protocol) Protokol prijenosa datoteka
10. SFTP (Secure File Transfer Protocol) Sigurni protokol prijenosa datoteka
11. DNS (Domain Name System) Sustav imena domena
12. DDOS (Distributed Denial of Service) Distribuirani napad uskraćivanja usluge
13. SQL (Structured Query Language) Strukturirani upitni jezik
14. NSA (National Security Agency) Nacionalna sigurnosna agencija
15. DES (Data Encryption Standard) Standard za šifriranje podataka
16. AES (Advanced Encryption Standard) Napredni standard šifriranja
17. RSA (Rivest-Shamir-Adleman) Rivest-Shamir-Adleman (kriptografski algoritam)
18. LoRaWAN (Long Range Wide Area Network) Širokopojasna mreža s dugim dometom
19. TLS (Transport Layer Security) Sigurnost transportnog sloja
20. GDPR (General Data Protection Regulation) Opća uredba o zaštiti podataka
21. LASAN (The Lightweight Authentication for Secure Automotive Networks) Lagana autentifikacija za sigurne automobilske mreže

22. DSRC (Dedicated Short Range Communications) Komunikacije na posve kratkom dometu

23. C-V2X (Cellular Vehicle-to-Everything) Komunikacija mobilnog vozila prema svemu

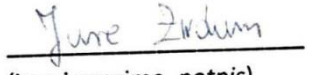
POPIS SLIKA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je *završni rad* isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Student/ica:



(ime i prezime, *potpis*)

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom „Primjena kriptografije u inteligentnim transportnim sustavima“, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

U Zagrebu, 24.6.2023.