Kriptografski algoritmi za okruženje Interneta stvari

Vlahović, Ante

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Sveučilišni diplomski studij Elektrotehnika

KRIPTOGRAFSKI ALGORITMI ZA OKRUŽENJE INTERNETA STVARI

Diplomski rad

Ante Vlahović

Osijek, 2024.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac D1: Obrazac za ocjenu diplomskog rada na sveučilišnom diplomskom studiju

Ocjena diplomskog rada na sveučilišnom diplomskom studiju

Ime i prezime pristupnika:	Ante Vlahović
Studij, smjer:	Sveučilišni diplomski studij Elektrotehnika, Komunikacije i
Mat. br. pristupnika, god.	D-1487, 07.10.2022.
JMBAG:	0165083705
Mentor:	prof. dr. sc. Krešimir Grgić
Sumentor:	
Sumentor iz tvrtke:	
Predsjednik Povjerenstva:	izv. prof. dr. sc. Višnja Križanović
Član Povjerenstva 1:	prof. dr. sc. Krešimir Grgić
Član Povjerenstva 2:	mr. sc. Anđelko Lišnjić
Naslov diplomskog rada:	Kriptografski algoritmi za okruženje Interneta stvari
Znanstvena grana diplomskog rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak diplomskog rada:	U okruženju Interneta stvari (IoT, Internet of Things) postoje brojni uređaji ograničenih računalnih, memorijskih i energetskih resursa. Ova ograničenja limitiraju mogućnost uporabe kompleksnih kriptografskih algoritama, te nameću nužnost razvoja novih kriptografskih algoritama prilagođenih ovakvom okruženju. Potrebno je sustavno istražiti i analizirati kriptografske algoritme prikladne za uporabu u okruženjima s ograničenim resursima ("lagani" kriptografski algoritmi), te analizirati mogućnosti njihove uporabe u IoT okruženju. Na
Datum ocjene pismenog dijela diplomskog rada od strane mentora:	17.09.2024.
Ocjena pismenog dijela diplomskog rada od strane mentora:	Izvrstan (5)
Datum obrane diplomskog rada:	8.10.2024.
Ocjena usmenog dijela diplomskog rada (obrane):	Izvrstan (5)
Ukupna ocjena diplomskog rada:	Izvrstan (5)
Datum potvrde mentora o predaji konačne verzije diplomskog rada čime je pristupnik završio sveučilišni diplomski studij:	08.10.2024.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O IZVORNOSTI RADA

Osijek, 08.10.2024.

Ime i prezime Pristupnika:	Ante Vlahović
Studij:	Sveučilišni diplomski studij Elektrotehnika, Komunikacije i informatika
Mat. br. Pristupnika, godina upisa:	D-1487, 07.10.2022.
Turnitin podudaranje [%]:	5

Ovom izjavom izjavljujem da je rad pod nazivom**: Kriptografski algoritmi za okruženje Interneta stvari**

izrađen pod vodstvom mentora prof. dr. sc. Krešimir Grgić

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis pristupnika:

SADRŽAJ

1. UVOD

Tijekom prethodnih nekoliko godina Internet stvari (IoT, engl. *Internet of Things*) je postao jedna od glavnih tehnologija čija su upotreba i ulaganje u razvoj u konstantnom porastu. Okruženje Interneta stvari obuhvaća kompletan proces povezivanja raznih uređaja s internetom u svrhu olakšanja komunikacije i poboljšanja mobilnosti te na taj način omogućuje ljudima lakšu komunikaciju s uređajima i procesima. Okruženje Interneta stvari obuhvaća razne vrste uređaja koji se koriste u raznolike svrhe pri čemu se može navesti kao primjer manipulacija tj. rukovanje kućanskim aparatima, pametnom kućom ili stanovima pri čemu se može odnositi na upravljanje raznim sustavima poput grijanja, hlađenja, sigurnosti, upravljanja roletama, zalijevanje vrta i slično. Osim uređaja koji se svakodnevno koriste, IoT ima primjenu i u industriji, proizvodnji, nadzoru i sigurnosti, medicini te raznim drugim oblastima u koje tek prodire i gdje tek stupa na scenu.

Samim razvojem IoT-a, rastu i zahtjevi te prijetnje koje se postavljaju kao prepreke u pružanju sigurnosti i besprijekorne komunikacije. Kako bi se omogućila sigurna komunikacija između korisnika i samog upravljanog uređaja veliku važnost imaju kriptografski algoritmi. Naime, povjerljivost podataka je bitno osigurati u procesu prijenosa, obrade i pohrane. Kriptografski algoritmi funkcioniraju na način da podatke pretvaraju u kombinacije nizova znakova koji predstavljaju nerazumljiv podatak pri čemu se izvornom podatku može pristupiti uz poznavanje tajnog ključa ili na neki drugi način ukoliko se radi o drugoj vrsti zaštite.

U ovom diplomskom radu provedena je analiza kriptografskih algoritama u okruženju Interneta stvari te njihova primjena i izazovi koji se postavljaju pred njih. Potom je analizirana sigurnost kriptografskih algoritama te izloženost napadima i metode zaštite od istih pri čemu su detaljno analizirani utjecaji pojedinih napada na temelju simulacija. Izdvojene su prednosti i mane kriptografskih algoritama u IoT okruženju te njihova primjena i uloga u budućnosti.

2. KRIPTOGRAFIJA I KRIPTOGRAFSKI ALGORITMI

Od davnina samom pojavom zapisivanja poruka postojala je potreba da neke poruke ostanu tajne odnosno da je njihovo značenje skriveno i nerazumljivo ostalima. Povodom te potrebe došlo je do utemeljenja nove znanstvene discipline kriptografije. Ta znanstvena disciplina za cilj ima razvoj sustava koji mogu šifrirati informacije. Kod kriptografije su bitna tri glavna načela. Prvo načelo je načelo povjerljivosti koje za cilj ima sprječavanje pristupa podacima od strane neovlaštenih osoba. Zatim slijedi načelo integriteta koje se odnosi na očuvanje postojanosti informacije tj. kako ne bi došlo do neovlaštene izmjene samih informacija, te posljednje načelo dostupnosti, koje za cilj ima osiguranje dostupnosti informacija svim ovlaštenim pristupnicima.

U početku se kriptografija koristila pretežito u vojne svrhe još od Sparte, pa preko Rimljana do svjetskih ratova gdje je došlo do najvećeg napretka u kriptografiji pri čemu je shvaćeno da bit ne leži u tajnosti algoritma, nego u tajnosti ključa jer ako ne znamo ključ, ne možemo ni razbiti poruku. Do tada najveći skok u razvoju i najveća ulaganja u tu disciplinu su bila tijekom 2. svjetskog rata kada su Nijemci osmislili Enigmu koja je kodirala poruke na dosad neviđeni način, no saveznici su i tome doskočili i uz pomoć kriptoanalitičkih metoda uspjeli razbiti sustav Enigme. Razvojem informacijskih tehnologija i same računalne moći računala, primitivni kriptografski algoritmi su se mogli lako probijati i više nisu mogli očuvati svoju ulogu [10]. Zbog toga kriptografski algoritmi postaju sve kompleksniji te naposljetku dolazi do pojave i kvantnih računala koja omogućavaju kvantnu kriptografiju zasnovanu na principu neodređenosti. Jedno od najmoćnijih kvantnih računala je u posjedu tvrtke Google te je prikazano na slici 2.1. Kvantna kriptoanaliza je jedna od najvećih prijetnji za svaki danas poznati kriptografski algoritam.

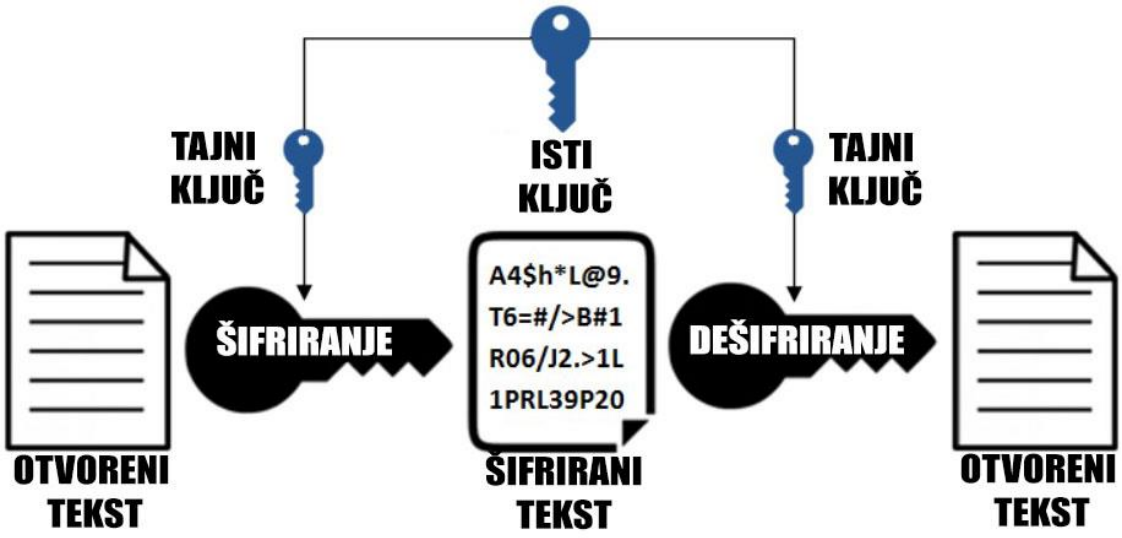
Slika 2.1. Kvantno računalo koje je u vlasništvu Google-a [29]

Značaj kriptografije i samih kriptografskih algoritama u današnjem društvu je ogroman. Kompletna online komunikacija, online poslovanje, pristup bankovnim računima, online kupovina, e-izbori u pojedinim zemljama, su podvrgnuti napadima u cilju razotkrivanja informacija te stoga kriptografski algoritmi su presudni u današnjem načinu funkcioniranja društva.

Kriptografski algoritmi predstvaljaju sekvence procesa uz pomoć kojih je omogućeno šifriranje i dešifriranje poruka tj. informacija u kriptografskom sustavu. Za cilj imaju iz otvorenog teksta koji je čitljiv i razumljiv dobiti šifrat koji je nerazumljiv te koji se može pretvoriti ponovo u razumljivu informaciju samo uz poznavanje ključa za dešifriranje. Podjela kriptografskih algoritama je načinjena u ovisnosti o ključu, pa tako postoje podjele na simetrične algoritme, asimetrične algoritme te hibridne koji su spoj prethodno navedenih.

2.1. Simetrični kriptografski algoritmi

Simetrični kriptografski algoritmi koriste isti ključ za šifriranje i dešifriranje što zahtijeva da korišteni tajni ključ kojim se šifriranje i dešifriranje obavlja nikad ne sazna izvan kruga pošiljatelj-primatelj kao što je prikazano na slici 2.2. Velika većina simetričnih algoritama kao tehnike koristi permutaciju i supstituciju te što se više ponavljanja izvodi to je sigurnost veća. Nelinearnost je izrazito bitna kod simetričnih algoritama što se postiže korištenjem nelinearnih supstitucijskih tablica pri čemu se razlikuje veličina izlaznih i ulaznih podataka.



Slika 2.2. Šifriranje i dešifriranje kod simetričnih kriptografskih algoritama [49]

Kod simetričnih kriptografskih algoritama postoji podjela na blok kodne sustave koji vrše šifriranje informacija u blokovima točno određene veličine te postoje i sekvencijalni sustavi koji vrše šifriranje niza bitova ili riječi. Kod blok sustava poruke se dijele na blokove veličine n bita te se zatim svaki blok šifrira neovisno jedan o drugom. Neke od najkorištenijih blok šifri su: DES, 3DES, AES i mnoge druge [25]. Mana sekvencijskog šifriranja je to što se odrađuje bit po bit te se daleko manje koristi u usporedbi s blok šiframa.

Prednosti simetričnih kriptografskih algoritama su manja računalna zahtjevnost potrebna za kreiranje snažnih ključeva, obrada algoritma uz efikasnu upotrebu resursa, sigurnost autentifikacije, dok manu predstavlja distribucija ključa pri čemu ključ mora ostati poznat samo pošiljatelju i primatelju, što zahtjeva sigurni komunikacijski kanal, što košta i nije uvijek lako ostvarivo. S porastom broja korisnika raste i broj ključeva, npr. za pet korisnika je potrebno 10 ključeva.

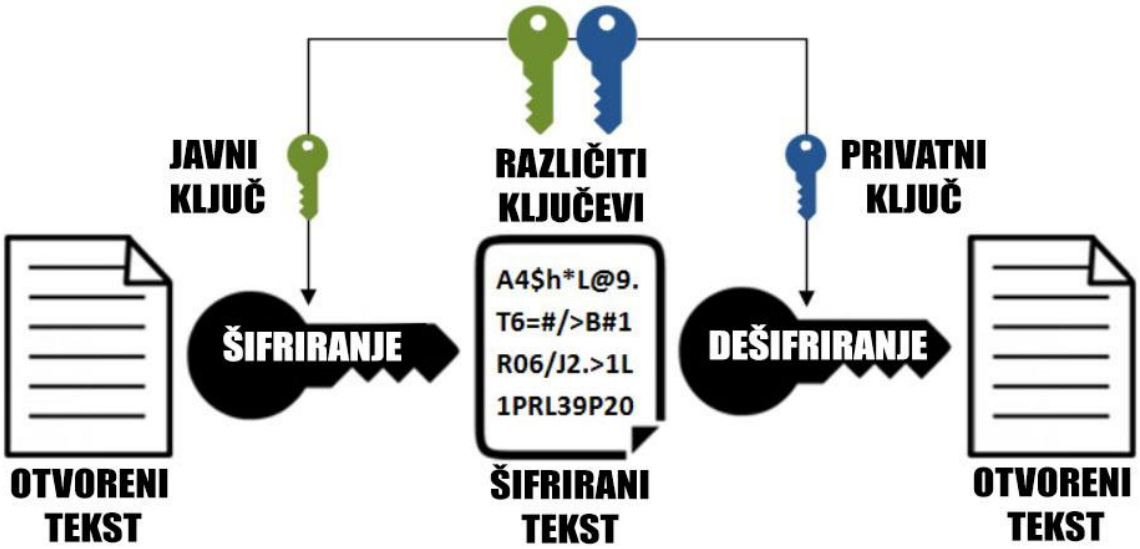
Simetrične kriptografske algoritme možemo podijeliti u nekoliko grupa kao što su: jednostavni, višenamjenski, ostali, DES prethodnici i sljedbenici te AES kandidati. U grupi DES prethodnika i sljedbenika mogu se istaknuti: Lucifer, DES, 3DES, Blowfish, DEAL, FEAL, IDEA, RC2, RC5, SHARK i drugi. Grupi jednostavnih algoritama pripadaju: 3-Way, ENIGMA, Solitare, TEA, dok u grupu višenamjenskih algoritama se mogu svrstati: Panama i Sapphire. Algoritmi u grupi AES kandidata su sljedeći: AES, MARS, RC6, FROG, Magenta, Twofish, dok u grupu ostalih se mogu svrstati mnogi drugi poput: CAST, CMEA, SAFER++, ARC4, LOKI89, LOKI91, DFC, MDC, NSEA, ORYX, Rainbow, Scop, Yarro, Crypt, CRAB itd. Pojedini od navedenih algoritama su pobliže obrađeni u poglavlju 5.

Simetrični kriptografski algoritmi se najviše koriste u bankarskom sektoru kod kartičnih transakcija, zatim kod šifriranja podataka koji se ne razmjenjuju aktivno s mrežom kao što je šifriranje podataka na tvrdim diskovima ili drugim uređajima za pohranu medija.

2.2. Asimetrični kriptografski algoritmi

Asimetrični kriptografski algoritmi funkcioniraju na način da koriste dva ključa, javni i privatni. Javni ključ je javno dostupan svima te pošiljatelj uz pomoć njega šifrira poruku i šalje primatelju koji potom primljenu poruku dešifrira sa privatnim ključem kao što je prikazano na slici 2.3. Asimetrični algoritmi su daleko sigurniji od simetričnih jer je privatni ključ poznat samo primatelju te je nemoguće doći do njega. Tvorci i prvi predlagatelji asimetrične kriptografije su:

Whitfield Diffie i Martin Hellman koji su 1976. godine javno izašli s idejom kriptografije utemeljene na dva ključa, privatnom koji je tajan i javnom ključu koji je javno obznanjen. Danas čak postoje i asimetrični kriptografski algoritmi koji su otporni ili su na dobrom putu da budu otporni na napade čak i kvantnih računala.



Slika 2.3. Šifriranje i dešifriranje kod asimetričnih kriptografskih algoritama [50]

Asimetrični kriptografski algoritmi funkcioniraju na način da se otvoreni tekst šifrira uz pomoć javnog ključa. Način samog šifriranja ovisi o odabranom algoritmu, a simboli se predstavljaju kao cjelobrojni (engl. *integer*) tip podataka. Šifrirana poruka se prenosi do primatelja koji za ispravno dešifriranje mora posjedovati ispravan privatni ključ kojeg prima od strane pošiljatelja.

Neki od najpoznatijih i najkorištenijih asimetričnih kriptografskih algoritama su: RSA (engl. *Rivest, Shamir, and Adleman*), Diffie-Hellman, ECC (engl. *Elliptic Curve Cryptography*), PGP (engl. *Pretty Good Privacy*), DSA (engl. *Digital Signature Algorithm*) i drugi pri čemu su pojedini detaljno obrađeni u poglavlju 5.

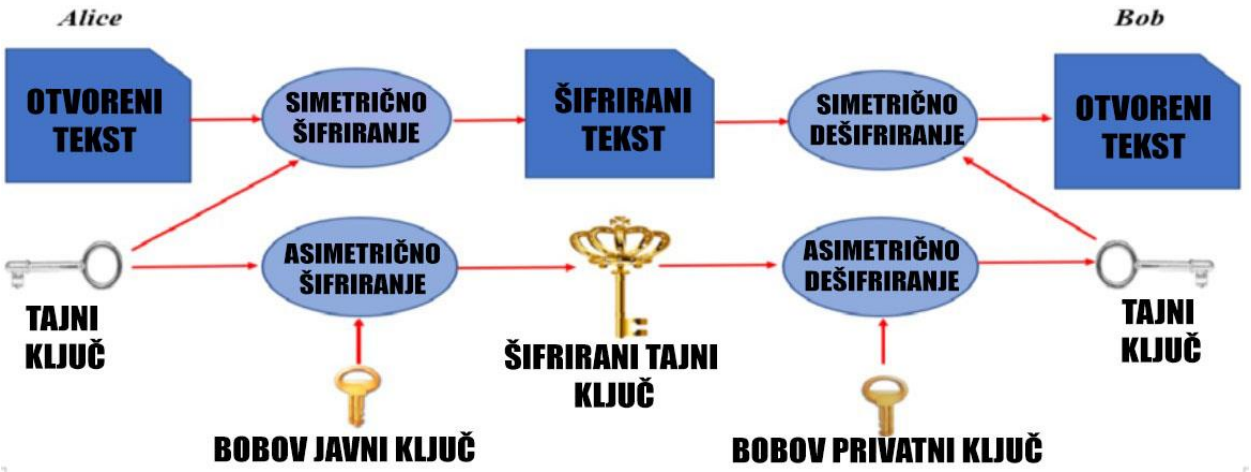
Glavni nedostatak asimetričnih kriptografskih algoritama je njihova složenost koja uzrokuje smanjenje brzine šifriranja odnosno dešifriranja podataka za razliku od simetričnih algoritama gdje je brzina daleko veća. Zbog njihove brzine, nisu najbolje rješenje za šifriranje servera, tvrdih diskova, baza podataka itd.

Unatoč prethodno navedenom problemu, korištenje različitih ključeva za šifriranje i dešifriranje znatno poboljšava sigurnost te predstavlja kao najbolji način za autentifikaciju dokumenata. Asimetrični algoritmi se uvelike koriste kod zaštite internetskog prometa, šifriranja e-mail

poruka, kod virtualnih privatnih mreža (VPN, engl. *Virtual Private Networks*), kod digitalnih potpisa itd.

2.3. Hibridni kriptografski algoritmi

Hibridni kriptografski algoritmi ujedinjuju sve dobre strane simetričnih i asimetričnih kriptografskih algoritama osiguravajući još veću sigurnost i pouzdanost. Zasnivaju se na korištenju šifriranja pomoću javnog ključa kako bi se dešifrirao simetrični ključ. Nakon uspješnog otkrivanja simetričnog ključa moguće je dešifrirat informaciju odnosno poruku kao što je prikazano na slici 2.4.



Slika 2.4. Šifriranje i dešifriranje kod hibridnih kriptografskih algoritama [51]

Prednost korištenja hibridnih kriptografskih algoritama tj. korištenja simetričnih i asimetričnih algoritama zajedno je poboljšanje performansi i sigurnosti sustava na optimalan način tako što simetrični algoritmi omogućavaju brz prijenos velike količine podataka, a asimetrični algoritmi povećavaju sigurnost ključa koji služi za dešifriranje prenesenih podataka.

Hibridna kriptografija se najviše koristi kod: digitalnih novčanika i kriptovaluta, usluga u oblaku, digitalnih potpisa, IoT-a, virtualnih privatnih mreža, kod osiguranja komunikacije putem interneta, kod sustava elektronske trgovine pri sigurnom plaćanju itd.

Neki od najkorištenijih algoritama koji kombiniraju simetrične i asimetrične algoritme, a većinski služe u svrhe autentifikacije digitalnog potpisa su: MD5 (engl. *Message Digest Algorithm 5*), SHA-256 (engl. *Secure Hashing Algorithm 256*), HMAC (engl. *Hash-based Message Authentication Code*) [24].

2.3.1. MD5 algoritam

MD5 (engl. *Message Digest Algorithm 5*) predstavlja kriptografsku *hash* funkciju koju je razvio Ronald Rivest 1991. godine. MD5 funkcionira tako što prima proizvoljno dug unos podataka pri čemu generira 128 bitni *hash*. *Hash* je uvijek fiksne duljine neovisno o količini ulaznih podataka te se koristi kao identifikator određenog unosa podataka. Služi za provjeru integriteta (provjera jesu li podaci izmijenjeni ili oštećeni), te za autentifikaciju podataka i korisnika.

Hash se kreira na način da poruka mora biti višekratnik broja 512, ukoliko nije, onda se dodaje dopuna. Zatim se ukupna poruka dijeli na blokove duljine 512 bita. Potom slijedi inicijalizacija varijabli i provođenje kompresije u četiri kruga. Nakon što su svi blokovi obrađeni, četiri varijable A, B, C, i D se kombiniraju kako bi se formirao završni *hash* od 128 bita.

Prednosti MD5 su brzina kreiranja *hash* koda, fiksna duljina izlaza te jednostavnost algoritma, dok su mane slabosti u sigurnosti, ranjivost na napade kao što su *birthday* napad i *preimage* napad.

MD5 je kroz povijest imao jako široku upotrebu kao što je: verifikacija integriteta podataka u raznim aplikacijama, kod digitalnih potpisa, kod zaštite lozinki pri skladištenju u bazu podataka, kod generiranja *hash* vrijednosti za ključeve u raznim aplikacijama itd.

2.3.2. SHA-256 algoritam

SHA-256 (engl. *Secure Hashing Algorithm 256*) predstavlja kriptografsku *hash* funkciju koja generira *hash* vrijednost fiksne dužine od 256 bita, neovisno u duljini unosa. Objavljen je 2001. godine s ciljem da bude sigurniji i otporniji na napade u odnosu na prethodnika SHA-1 algoritam. SHA-256 služi za: očuvanje integriteta podataka, autentifikaciju korisnika ili dokumenata, te za sigurnost transakcija u *blockchain* tehnologiji i digitalnim valutama.

Funkcionira tako što proizvoljno unesene podatke dopunjava kako bi postali višekratnik broja 512 (ukoliko već nisu). Zatim se ukupna poruka dijeli na blokove duljine 512 bita. Potom slijedi inicijalizacija registara i obrada svakog bloka koji prolazi kroz 64 kruga obrade gdje se koristi niz matematičkih operacija. Nakon obrade, rezultati se dodaju u inicijalne registre pri čemu se vrijednosti kombiniraju kako bi se dobio završni *hash* duljine 256 bita.

Prednosti SHA-256 su veća sigurnost u odnosu na svoje prethodnike, veća otpornost na napade, široka primjena, kompatibilnost sa različitim platformama i aplikacijama, dok su mane

smanjenje brzine zbog složenijih operacija i duže *hash* vrijednosti, računalna zahtjevnost, ranjivost na kvantne napade u budućnosti.

SHA-256 se koristi kod *blockchain* tehnologija i kriptovaluta, kod digitalnih potpisa, Hashiranja lozinki, provjere integriteta podataka, u SSL/TLS certifikatima itd.

2.3.3. HMAC

HMAC (engl. *Hash-based Message Authentication Code*) predstavlja kriptografsku tehniku koja koristi *hash* funkcije i tajne ključeve za osiguravanje integriteta i autentičnosti poruka (dolazi li poruka od legitimnog izvora, je li izmijenjena tijekom prijenosa).

HMAC funkcionira tako što koristi određenu *hash* funkciju i unaprijed dogovoreni tajni ključ. Ako je ključ kraći od bloka (npr. ukoliko se koristi SHA-256, blok je dug 512 bitova), onda se nadodaju nule, a ukoliko je ključ duži od bloka, onda se primjenjuje *hash* funkcija kako bi se ključ skratio. Tajni ključ se pomoću XOR kombinira s vrijednostima iz unosa te se potom koristi *hash* funkcija. Krajnji rezultat predstavlja jedinstvenu HMAC vrijednost koja se šalje zajedno s porukom. Primatelj ponavlja isti postupak koristeći poznati ključ i uspoređuje dobiveni HMAC s HMAC-om koji je stigao uz poruku.

Prednosti HMAC-a su: otpornost na *brute force* i *collision* napade, jednostavna implementacija koristeći postojeće *hash* funkcije kao što su SHA-256 i drugi, fleksibilnost (može koristiti različite *hash* funkcije), dok su mane lošije performanse, računalna zahtjevnost i ovisnost o tajnom ključu.

HMAC se koristi u mnogim sigurnosnim protokolima i aplikacijama kao što su: SSL (engl. *Secure Sockets Layer*), TLS (engl. *Transport Layer Security*), IPSec, JWT (engl. *JSON Web Tokens*), API autentifikacija, protokoli za autentifikaciju e-pošte itd.

2.4. Laki kriptografski algoritmi

Laki kriptografski algoritmi (engl. *lightweight algorithm*) predstavljaju kriptografske algoritme koji su prvenstveno prilagođeni ugrađenim sustavima i Internetu stvari [9]. Primarno svojstvo im je brzo izvođenje i mali računalni zahtjevi u softverskim i hardverskim implementacijama. Veličina blokova u većini algoritama je 64 bita dok ključ najčešće bude veće duljine oko 128 bita. Također su poznati po korištenju 4-bitne S kutije pri čemu se najčešće koristi 12 slojeva.

Pojedini laki kriptografski algoritmi poput Simon algoritma koriste bitovne operatore u šifriranju i dešifriranju pri čemu su najkorišteniji operatori: isključivo ILI, operator I te lijevi kružni pomak [15].

Neki od najpoznatijih i najkorištenijih lakih kriptografskih algoritama prikazani su u tablici 2.1.:

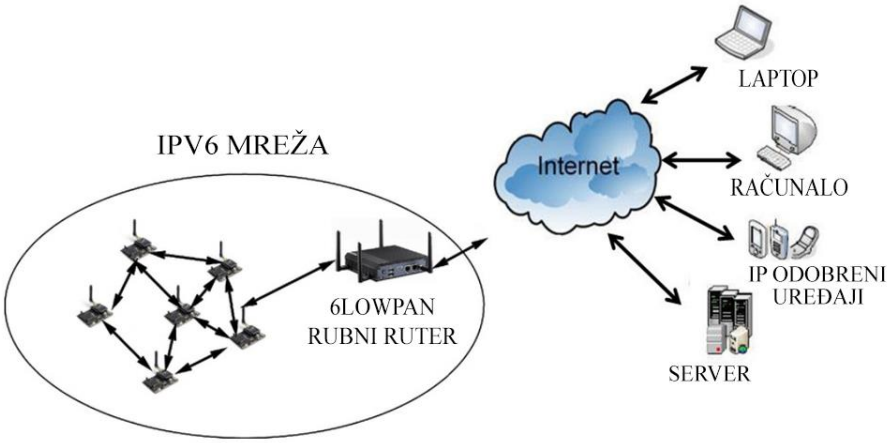
Tablica 2.1. Prikaz pojedinih lakih kriptografskih algoritama sa osnovnim podacima

ALGORITAM	BROJ RUNDI	VELIČINA KLJUČA	VELIČINA BLOKA
TEA	64	128	64
XTEA	64	128	64
LEA (23)	/	128	64
HEIGHT	32	128	64
FeW (29)	32	80/128	64
SIMON	32/36/42/44/52/54/68/69/72	64/72/96/128/144/192/256	32/48/64/92/128
PRESENT	31	80/128	64
RECTANGLE	25	80/120	64
LEA	24/28/ 32	128/192/256	128
SPECK	22/23/26/27/28/29/32/33/34	64/72/96/128/144/192/256	32/48/64/92/128
Prince (8)	11	128	64
AES	10/12/ 14	128/192/256	128
RC5	12	128	32/64/128
Hummingbird2	4	256	16

Laki kriptografski algoritmi se mogu podijeliti na četiri glavne grupe, a to su: blok šifre, protočne šifre, *hash* funkcije i kriptografija eliptične krivulje. Obilježje blok šifri je šifriranje ili dešifriranje teksta u blokovima dok protočne šifre isti zadatak obavljaju bit po bit ili bajt po bajt. Glavna značajka *hash* funkcija je generiranje fiksne duljine teksta iz proizvoljnog zadanog teksta čime se osigurava integritet. Kriptografija eliptične krivulje predstavlja asimetričnu kriptografiju zasnovanu na matematičkim jednadžbama pri čemu se koriste javni i privatni ključ.

Za osiguravanje povjerljivosti u IoT sustavima osnovni kriptografski algoritmi se modificiraju ili im se pridružuju drugi kriptografski algoritmi ili protokoli čime se zaštita značajno poboljšava. Grupe kriptografskih algoritama i protokola koje pokazuju odlične karakteristike pri zajedničkom radu, te se odlično nadopunjavaju se nazivaju kriptografskim shemama [31]. Postoji preko 30 istaknutijih kriptografskih shema baziranih na lakim kriptografskim algoritmima koje su zaživjele u širokoj upotrebi, a neke od njih su:

- Usman shema – predstavlja 64 bitnu shemu zasnovanu na supstitucijsko-permutacijskim i Feistelovim mrežama. Sastoji se od pet krugova enkripcije te su operacije šifriranja i dešifriranja gotovo identične. Prednosti Usman sheme su: manja veličina koda tj. manja potreba za memorijom, manji ciklusi šifriranja i dešifriranja. Slabosti ove sheme su već poznate slabosti Feistelove strukture.
- Green shema – zasnovana je na ABE (engl. *Attribute-based Encryption*) i El-Gamal algoritmima. Otporna je na napade odabranog otvorenog teksta i na napade odabranim šifriranim tekstom. Veliki nedostatak ove sheme je nemogućnost promjene politike pristupa i dodavanja novih prijemnika nakon puštanja u rad.
- Raza shema – utemeljena je na CoAP (engl. *The Constrained Application Protocol*), DTLS (engl. *Datagram Transport Layer Security*), 6LoWPAN mreži i Contiki operativnom sustavu. Ima puno prednosti kao što su energetska efikasnost, skalabilnost, otpornost na napade ponavljanjem i na napade uskraćivanjem resursa. Nedostatak ove sheme je ranjivost na Sybil napade, DTLS koristi značajnu količinu RAM i ROM memorije, odvijanje kompresije zaglavlja samo u 6LoWPAN mreži pri čemu je njena arhitektura prikazana na slici 2.5.



Slika 2.5. Arhitektura 6LoWPAN mreže u IoT sustavu [32]

- Kim shema – zasnovana je na polustatičnoj strujajućoj enkripciji koja koristi bilinearno mapiranje. Prednosti ove sheme su adaptivna sigurnost, smanjena veličina privatnog ključa i smanjenje veličine šifriranog teksta. Nedostatak ove sheme je što prije procesa šifriranja svi identiteti primatelja moraju biti unaprijed poznati.
- Yao shema – utemeljena na ECDDH (engl. *Eliptic Curve Decisional Diffie Hellman*) baziranom na ABE (engl. *Attribute-based Encryption*) strukturi bez bilinearnog

uparivanja. Prednost Yao sheme su smanjenje komunikacijskih i računalnih troškova, a mane su nefleksibilnost u opozivu atributa i nepostojeća podrška za aplikacije s više autoriteta.

- Baskar shema – utemeljena na XTEA, DE1 i ALTERA algoritmima. Namjenjena za upotrebu kod FPGA (engl. *Field Programmable Gate Arrays*) uređaja prikazanog na slici 2.6. Prednosti su korištenje nasumično generiranih ključeva te poboljšavanje performansi rada FPGA uređaja. Shema nije pogodna kod velikih brzina prijenosa podataka.

Slika 2.6. Spartan 7 FPGA [33]

- Tsai shema – bazirana na hash funkcijama i korištenju XOR logike pri čemu je namjenjena za Cortex-A9 procesor. Tsai je otporna na napade ponavljanjem i na napade poznatim ključem. Nedostatak ove sheme je lošija sigurnost čvorova između pametnog uređaja i servera te degradacija sigurnosti servera zbog korištenja osnovnih operacija.
- Abbassinezhad & Nikooghadam shema – koristi kriptografiju eliptične krivulje, Canetti-Krawczyk model za razmjenu ključeva, te je namjenjena za ARM Cortex-M3 kontroler prikazan na slici 2.7. Ova shema je otporna na napade čovjek u sredini napade (engl. *man in the middle attacks*) i razne druge modificirane napade. Slabosti su ranjivost na napade ponavljanjem te što prva poruka nema osiguranu provjeru integriteta.

Slika 2.7. Pločica sa ARM Cortex-M3 procesorom [34]

- Zhou shema – bazirana na kriptografiji eliptične krivulje duljine 256 bita pri čemu je namjenjena za 8 bitne AVR procesore (slika 2.8.). S ovom postavkom je na AVR procesorima ostvarena 27.3% veća brzina i 13.2% veća efikasnost koda. Ova shema iskorištava konačna polja za optimizaciju izračuna maske te operacije zbrajanja i oduzimanja obavlja brže uz pomoću predmemorije.

Slika 2.8. 8 bitni AVR procesor [35]

Osim prethodno navedenih shema, postoje i mnoge druge kao što su: Chaitanya, Diro, Salami, Sahraoui, Venukauskas, Glissa & Meddeb, Yang, Canteaut, Shahzadi, Shen, Wu, Lee, Harbi, Gupta, Wazid, Liu, Noura, Deebak i druge [30].

2.4.1. TEA

TEA (engl. *Tiny Encryption Algorithm*) je simetrični kriptografski algoritam kojeg su razvili David Wheeler i Roger Needham 1994. godine. Jednostavan je za implementaciju i ima mali memorijski otisak zbog čega je odličan za korištenje u sustavima s ograničenim resursima zbog čega je postao popularan kod ugradbenih sustava.

TEA koristi 64 bitne blokove podataka i 128 bitni ključ za šifriranje i dešifriranje, a osnovne operacije koje koristi su: XOR, zbrajanje i rotiranje. Funkcionira tako što podatke dijeli na dva 32 bitna bloka (lijevi i desni), pri čemu provodi šifriranje u 32 kruga koristeći osnovne matematičke operacije: XOR, zbrajanje i rotiranje. Ključ duljine 128 bita se dijeli na četiri jednaka dijela duljine 32 bita, te se u različitim krugovima primjenjuje različiti dio ključa. Dešifriranje se obavlja na isti način, samo obrnutim redoslijedom.

Prednosti TEA su: jednostavnost, mali memorijski otisak, odgovarajuća duljina ključa za zadovoljavajuću sigurnost, brzina i efikasnost, dok su mane ranjivost na diferencijalne napade, kratka duljina bloka.

TEA se najviše primjenjuje kod ugradbenih sustava, u aplikacijama za zaštitu podataka ili komunikacije, tamo gdje je potrebno brzo šifriranje i dešifriranje. Njegov nasljednik je XTEA algoritam koji je poboljšana verzija svog prethodnika.

2.4.2. SIMON

SIMON je simetrični kriptografski algoritam koji je razvijen 2013. godine od strane NSA (engl. *National Security Agency*). Dizajniran je s ciljem da bude jednostavan i efikasan u smislu hardverske implementacije, namjenjen za sustave s ograničenim resursima kao što su IoT uređaji, ugradbeni sustavi i mobilni uređaji. SIMON je optimiziran za hardverske aplikacije dok je njegov prateći algoritam SPECK, optimiziran za softverske aplikacije. Oba algoritma pripadaju obitelji NSA-inih lakih kriptografskih algoritama.

SIMON koristi različite veličine blokova podataka (32, 48, 64, 96, 128 bita) i podržava ključeve različitih duljina (64, 72, 96, 128, 144, 192, 256 bita). Pri proračunu koristi osnovne operacije: AND, XOR i rotaciju bitova. Podaci se dijele na lijevi i desni dio, koji prolaze kroz više krugova obrade ovisno o duljini bloka i ključa. Ključni dio svake runde je obavljanje XOR operacije sa dijelovima ključa.

Prednosti SIMON algoritma su: odlična optimizacija za hardver, jednostavnost, skalabilnost, mala potrošnja energije uz visoku efikasnost, dok su mane: ranjivost na kriptoanalitičke napade, veća potrošnja u softverskoj implementaciji.

SIMON se primjenjuje kod IoT uređaja, ugradbenih sustava, u bežičnim mrežama s niskom propusnosti, kod uređaja koji se napajaju baterijama ili rade u okruženjima sa ograničenim memorijskim resursima.

2.4.3. LEA

LEA (engl. *Lightweight Encryption Algorithm*) je simetrični kriptografski algoritam razvijen 2013. godine od strane Korejske agencije za internet i sigurnost. LEA je dio trenda razvoja lakih kriptografskih algoritama koji su optimizirani za resursno ograničene sustave kao što su IoT sustavi i ugradbeni sustavi. LEA osigurava visok stupanj sigurnosti i visoku efikasnost u softverskim implementacijama. Algoritam koristi 128 bitne blokove podataka i podržava tri različite duljine ključeva: 128 bita, 192 bita i 256 bita. Ovisno o duljini ključa, enkripcija se odvija u određenom broju krugova, pa tako za ključ duljine 128 bita, provodi se 24 kruga enkripcije, za ključ od 192 bita odvija se 28 krugova enkripcije, te za ključ od 256 bita se odvijaju 32 kruga enkripcije. Pri enkripciji se koriste jednostavne operacije: XOR, rotacija i zbrajanje kao i kod ostalih algoritama te je princip rada skoro identičan.

Prednosti LEA su: efikasnost u softverskim implementacijama, mala zahtjevnost u vidu softverskih i hardverskih resursa, visoka brzina, mogućnost promjene duljine ključa, otpornost na diferencijalne i linearne kriptoanalitičke napade, dok su mane: ograničena primjena izvan Azije, ranjivost u specifičnim napadima kao što su napadi zasnovani na vremenskim ili energetskim potpisima.

Algoritam se primjenjuje kod IoT uređaja, u senzorima, u pametnim uređajima, u mobilnim aplikacijama, kod ugradbenih sustava, u sigurnim protokolima za bežične komunikacije itd.

2.4.4. Lightweight ECC

Lightweight Elliptic Curve Cryptography je optimizirana verzija *Elliptic Curve Cryptography* algoritma koja je prilagođena za uređaje sa ograničenim resursima kao što su IoT uređaji, ugradbeni sustavi i mobilni uređaji. ECC se temelji na matematičkoj strukturi eliptičnih krivulja,

te omogućava visoku sigurnost uz korištenje relativno kratkog ključa što ga čini idealnim za korištenje u prethodno navedenim okruženjima. Prvobitnu verziju ECC-a su razvili Neal Koblitz i Viktor Miller 1980. godine o čemu se detaljno govori u poglavlju 5.2, dok je verzija prilagođena sustavima s ograničenim resursima zaživjela kasnije razvojem IoT područja.

Prednosti ovog algoritma su: visoka sigurnost uz korištenje kratkog ključa (ECC 256 bit ključ predstavlja ekvivalent RSA algoritmu koji koristi ključ duljine 3072 bita), mala zahtjevnost u smislu računalne snage i memorije, brža enkripcija i dekripcija u odnosu na konkurenciju, mala potrošnja energije, široka primjena, dok su mane: kompleksna implementacija, osjetljivost na bočne napade, problem s patentima i licencama jer su neki dijelovi ECC-a licencirani i zaštićeni pravima zbog čega je svaka implementacija financijski izazovna.

Princip funkcioniranja se temelji na rješavanju problema poznatog kao „*Elliptic Curve Discrete Logarithm Problem*“ (ECDLP). Privatni ključ je slučajni broj dok je javni ključ točka na eliptičnoj krivulji koju generira privatni ključ. Podaci se šifriraju kombiniranjem javnog ključa primatelja i slučajnog ključa generiranog u procesu obrade. Za dešifriranje se koristi privatni ključ kako bi se dobio originalni otvoreni tekst.

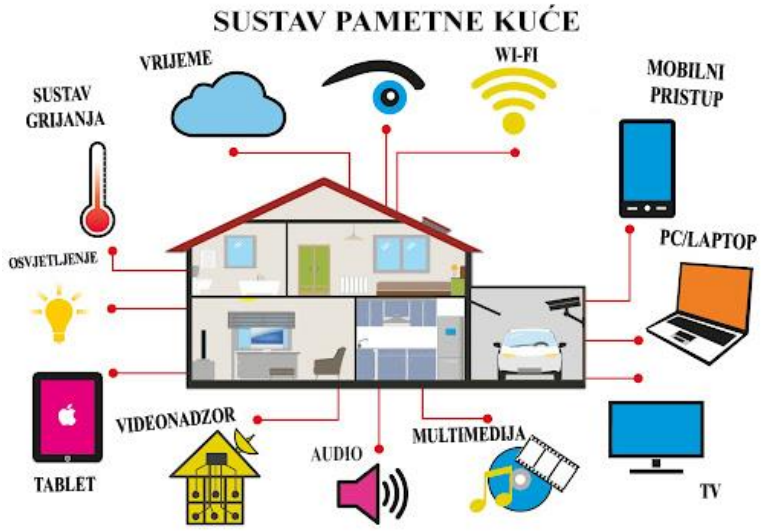
ECC široku primjenu ima kod IoT uređaja, senzora, kamera, mobilnih uređaja, kod virtualnih privatnih mreža, kod digitalnih potpisa i certifikata, u području mobilnog bankarstva i kriptovaluta, te kod bežičnih mreža.

3. IZAZOVI I PRIMJENA KRIPTOGRAFSKIH ALGORITAMA U OKRUŽENJU INTERNETA STVARI

Internet stvari s razvojem tehnologije postaje sve popularniji i polako zalazi u sve sfere života i industrije. Ovisno o području u kojem se koristi, postoje i različiti zahtjevi i potrebe pri čemu se razlikuju i zahtjevi prema samim kriptografskim algoritmima koji moraju osigurati sigurnost, povjerljivost i integritet podataka. IoT se jednostavno primjenjuje u skoro svim granama ljudskog života od čega se mogu izdvojiti one najbitnije i najvažnije te navesti neke od primjena u tim granama pri čemu je moguće uvidjeti i različite zahtjeve u pogledu sigurnosti.

3.1. Primjena i izazovi kod pametnih kuća

Primjena IoT-a kod pametnih kuća je omogućena u mnogim dijelovima od osiguranja zaštite kuće, upravljanje grijanjem, hlađenjem, svjetlima, roletama do čak i upravljanja pojedinim kućanskim uređajima [26]. Među proizvođačima koji se ističu u sferi pametnih kuća su dakako Samsung, LG Electronics, Electrolux, Tovala i mnogi drugi. Dakle bitno je osigurati sigurnu i povjerljivu komunikaciju s velikom sigurnošću na način da nije moguće neovlaštenim pristupom pristupiti sigurnosnom sustavu kuće i ugasiti ga, da nije moguće upaliti velike potrošače radilo se to o grijanju, hlađenju ili nečem drugom čime bi oštetili vlasnika velikom potrošnjom energije. Velika opasnost nastaje i pojavom manipulacije određenim kućanskim aparatima gdje može doći do požara ili neke druge štete. Uvijek postoji i bojaznost od prisluškivanja i praćenja na način da je moguće doznati dnevnu rutinu ukućana i taj podatak zloupotrijebiti. Sustav pametne kuće je prikazan na slici 3.1.



Slika 3.1. Sustav pametne kuće i njegovi dijelovi [36]

3.2. Primjena i izazovi u poljoprivredi

IoT postaje također sve popularniji i u svijetu poljoprivrede gdje polako automatizira sve više poslova i na taj način olakšava obradu polja, kultivaciju tla kao i stočarstvo i razne druge djelatnosti. Jedan od pionira primjene IoT-a u ovoj sferi je John Deere koji je počeo sa primjenom *Blue River* tehnologije na svojoj opremi kao što je prikazano na slici 3.2. [26].

Slika 3.2. John Deere Blue River tehnologija u primjeni [37]

Uz tu tehnologiju koristi i satelitsko navođenje što omogućava traktorima i ostaloj opremi navođenje i obavljanje aktivnosti bez potrebe za ljudskim rukovanjem. Također postoji i platforma Fuse koja je razvijena od strane AGCO tvrtke koja osigurava pametnu poljoprivredu te nastoji automatizirati poljoprivredu i osigurati laku manipulaciju mehanizacijom. U ovoj sferi je lako razumljivo da neovlašteni pristup ili neovlaštena promjena podataka može načiniti višemilijunsku materijalnu štetu koja može nastati zbog uništenja nasada ili same opreme koja je iznimno skupa. Stoga kao i za prethodne primjene, presudno je osigurati sigurnu komunikaciju i integritet podataka.

3.3. Primjena i izazovi kod sigurnosnih i alarmnih sustava

Primjena kod sigurnosnih i alarmnih sustava je izričito osjetljiva tema. IoT se u tim sustavima primjenjuje pri povezivanju kamera, raznih senzora kao što može biti senzor pokreta, loma stakla, buke, topline i drugih. Povezivanje svih prethodno navedenih stavki i omogućavanje pristupa s udaljene lokacije informacijama koje prikupljaju senzori i kamere ima jako puno potencijalno slabih točaka pri čemu se postavljaju jako veliki zahtjevi samim kriptografskim algoritmima. Potencijalna mogućnost isključenja ili krađe podataka alarmnog sustava kuće, tvrtke, banke, zlatare može prouzročiti ogromnu materijalnu štetu stoga je jako bitno da

kriptografski algoritmi su dovoljno jaki da izdrže napade, a opet dovoljno procesorski nezahtjevni da mogu efikasno funkcionirati kod raznih hardverskih komponenti koje nemaju veliku procesorsku moć i koje ne raspolažu sa jakim izvorom napajanja.

3.4. Primjena i izazovi kod modernih automobila

IoT se danas uvelike koristi u automobilskoj industriji gdje prednjače Audi i Tesla. Naime Audi je svojim kupcima ponudio „*Audi connect*“ koji se sastoji od niza planova pri čemu je moguće putem pametnog uređaja manipulirati vozilom. Manipulacija vozila podrazumijeva očitanje trenutnog postotka punjenja, upravljanje unutarnjim sustavom grijanja i hlađenja, parkiranje vozila u slučaju uskih prostora gdje npr. nije moguće otvoriti vrata. Sve prethodne opcije mogu se zloupotrijebiti čime se može načiniti velika materijalna šteta vlasniku vozila i nedužnoj okolini te stoga postoje veliki zahtjevi osiguranja komunikacije i autentifikacije samog vlasnika i poruka koje se šalju vozilu. Slične usluge nudi i proizvođač Tesla koji na prethodno spomenute usluge nadodaje i zakazivanje servisa, pomoći na cesti i raznih drugih usluga. Što se tiče automobilske industrije tu još postoji i Zubie koji također na temelju IoT-a omogućuje praćenje iznajmljenih vozila, stanja vozila te stanja vozača. Zubie čak bilježi i nagla ubrzavanja i kočenja te razne druge stavke koje su bitne za sigurnost vozila i vozača [4].

3.5. Primjena i izazovi u industriji

Industrijski IoT poznatiji kao IIoT predstavlja sustav pametnih uređaja koji putem interneta i drugih vidova komunikacije omogućuju manipulaciju i upravljanje elektroničkim uređajima, senzorima, mehaničkim i digitalnim strojevima te proizvodnim pogonima i objektima u cjelini koji se koriste u industriji kao što je prikazano na slici 3.3.

Slika 3.3. Karikatura IIoT-a pri upravljanju strojem [38]

IIoT uređaji imaju sposobnost prikupljanja podataka i sposobnost komunikacije sa bilo kojim od prethodno navedenih elemenata industrijskog pogona u svrhu postizanja visoke produktivnosti. Nezanemariv broj IIoT uređaja je jako osjetljiv na kibernetičke napade pri čemu može doći do uskraćivanja usluge, krađe podataka i informacija, neovlaštene promjene podataka što može uzrokovati fatalne posljedice od ugroze ljudskih života do ugroze kapitala ulagača koji zbog prethodno navedenog neće ni pomisliti implementirati IIoT tehnologiju u svoj pogon. Kako bi se sigurnosni rizici smanjili i osigurali IIoT uređaji, koristi se laka kriptografija te digitalni potpisi [6]. Što se tiče kriptografije, koriste se simetrični i asimetrični algoritmi. Zbog svojih mana i nedostataka nije dovoljno samo koristiti simetričnu ili asimetričnu kriptografiju, nego se koristi i digitalni potpis kako bi se provjerila autentičnost pošiljatelja i osigurala veća povjerljivost i očuvanje integriteta informacija. Implementacija asimetričnih algoritama u IIoT je zahtjevnija i značajno skuplja od simetrične kriptografije te se više podliježe korištenju simetričnih algoritama ukoliko se raspolaže s ograničenim resursima. Najpopularniji način kriptografije u IIoT su digitalni certifikati koji se koriste za povezivanje identiteta objekta koji može biti senzor, aktuator ili korisnik sa javnim ključem koji koristi digitalni potpis treće strane od povjerenja. Treća strana od povjerenja ima mogućnost provjere identiteta vlasnika, a kada udaljeni IIoT uređaj šalje poruku objektu, on tada prilaže uz nju digitalni certifikat koji služi za daljnje provjere i na taj način povećava sigurnost. Neovisno o dizajnu platforme, mrežni model IIoT-a je podložan brojnim kibernetičkim napadima na slojevima TCP/IP modela uključujući aplikacijski i mrežni sloj [6]. Dakle jedan od glavnih izazova s kojima se susreće IIoT odnosno Internet stvari u industriji su uskraćenje usluga, neovlašteni pristup podacima, neovlaštena izmjena podataka te nepostojanje standardiziranih sigurnosnih protokola koji štite od prethodno navedenog. Izazovi kriptografskih algoritama koji bi idelano odgovarali IIoT-u su potrebna mala računalna moć, velika brzina i kompaktnost te mala cijena koja osigurava visoku zaštitu. Veliki problem predstavljaju uređaji s ograničenim resursima gdje se prvenstveno misli na senzore i aktuatore.

3.6. Primjena i izazovi kod povezanih gradova

Kod povezanih gradova postoje razne primjene pri čemu se ističu UrbanFootprint, Telitov Smart Light sustav te HAAS sustav sigurnosti [26]. HAAS sustav sigurnosti se sastoji od sigurnosnog oblaka koji je namijenjen za sve hitne službe i drugo hitno osoblje koje može komunicirati sa stanovništvom i slati upozorenja u stvarnom vremenu. Usluge samog HAAS sustava više su informativne i preventivne prirode, no mogu se itekako zloupotrijebiti u svrhu manipulacije i

zastrašivanja stanovništva čime može utjecati na mentalno stanje populacije. Zatim postoji i Telit platforma za manipulaciju i upravljanje javnom rasvjetom pri čemu je moguće smanjiti ili povećati intenzitet javne rasvjete. Ovaj način upravljanja javnom rasvjetom se lako može zloupotrijebiti u svrhe kriminalnih radnji te stoga postoje velike potrebe za osiguravanjem zaštite i autentifikacije samih korisnika [7]. Na slici 3.4. prikazana je ilustracija veza i povezanosti u povezanom gradu.

Slika 3.4. Ilustracija veza u povezanom gradu „connected city“ [39]

4. SIGURNOST U OKRUŽENJU INTERNETA STVARI

Sa sve većom popularizacijom upotrebe IoT-a i zalaženjem u sve moguće pore života pri čemu se koristi sklopovlje različitih proizvođača s raznolikom procesorskom moći postaje sve teže osigurati zaštitu pri čemu algoritmi trebaju efikasno funkcionirati i na procesorskim slabim i računalno ograničenim objektima pa sve do onih dijelova sustava gdje računalna moć nije upitna, no postoje neki drugi zahtjevi poput ograničenja memorije, napajanja ili slično. Stoga IoT teži ka pet osnovnih stupova sigurnosti koji se moraju osigurati, a to su:

- Povjerljivost – podrazumijeva sprječavanje neovlaštenih korisnika od pristupanja tajnim informacijama. Ovdje se koriste mehanizmi kao što su: autentifikacija i enkripcija.
- Autentifikacija – svaki objekt tj. čvor u IoT sustavu mora biti u mogućnosti provjeriti druge čvorove i biti siguran da komunicira s pravim čvorom, a ne „čovjekom u sredini“ koji može slati podatke lažno se predstavljajući kao neki objekt.
- Dostupnost – glavna svrha i cilj IoT-a su da informacije, podaci, komunikacija i usluge budu stalno dostupni i na raspolaganju korisnicima jer u protivnom IoT sustav nema smisla i ne koristi ako je nedostupan.
- Integritet – kod razmjene podataka od presudne je važnosti da primljeni podatak dolazi od točno određenog entiteta te da tijekom te komunikacije nije došlo do uplitanja neovlaštenog entiteta pri čemu može doći do neovlaštene promjene podataka što može kobno utjecati na rad sustava.
- Detekcija – kod brige za sigurnost i zaštitu jako je bitno imati sustav detekcije i provjere rada hardvera te same komunikacije. Naime u slučaju kvara senzora ili nekog drugog objekta u IoT sustavu, korisnik može primati lažne i netočne informacije koje mogu kobno utjecati na razinu sigurnosti. Dakle bitno je imati provjeru ispravnosti svih dijelova sustava jer na taj način je IoT sustav siguran i zaštićen.

4.1. Sigurnost slojeva u IoT arhitekturi

Kako je IoT sustav baziran na prijenosu podataka putem interneta, to pruža potencijalnim napadačima slabu točku tj. točku mogućeg proboja sustava. IoT arhitektura se sastoji od slojeva

te je moguće ovisno o tipu sloja i njegovoj ulozi istaknuti potencijalne slabosti i napade kojima su pojedini slojevi izloženi.

Percepcijski sloj predstavlja fizički sloj u IoT arhitekturi te je njegova najveća mana procesorska snaga te količina memorije kojom raspolaže što dovodi do određenih sigurnosnih rizika. Neke vrste napada kojima je percepcijski sloj izložen su sljedeće [21] :

- *Spoofing* napad – napadači u ovom slučaju šalju lažne poruke kako bi pristupili IoT sustavu te se najčešće radi o RFID spoofingu.
- Napad uskraćivanjem usluge (DoS, engl. *Denial of Service*) – napadači pokušavaju izvršiti stres na mrežu ili sustav kako bi usluga bila nedostupna pravim korisnicima.
- Napad ometanjem signala – cilj napadača je prekinuti komunikacijski kanal te na taj način onemogućiti pružanje usluge. Najčešće se radi o ometanju signala koji su upućeni sa samih senzora ka sustavu.
- Napad distribuiranog uskraćivanja usluge (DDoS, engl. *Distributed Denial of Service*) – radi se o sličnoj vrsti napada kao što je prethodno navedeni DoS napad, no u ovom slučaju se odvija više napada u isto vrijeme.
- Napad neovlaštenog hvatanja čvora – napadači najčešće žele zauzeti pristupni čvor pri čemu mogu doći do osjetljivih informacija, ključeva itd...
- Napad ponavljanjem – napadači hvataju poruku iz komunikacije i ponavljaju njeno slanje kako bi dokazali svoj identitet.
- Napad lažnim čvorom – napadači kreiraju lažni čvor i lažni identitet te na taj način povećavaju promet i štetno utječu na mrežnu komunikaciju.
- *Mass Node Autentification* napad – radi se o napadu gdje se šalje ogroman broj autentifikacija čime se utječe na smanjenje performansi sustava.
- Napad uskraćivanjem sna – napadači konstantno vrše napad na uređaj s ciljem ispražnjenja baterije sve dok uređaj ne prestane funkcionirati.

Sljedeći sloj koji je na udaru napada je mrežni sloj koji za cilj ima prijenos podataka od percepcijskog sloja do aplikacijskog sloja. Neki od najkorištenijih napada u ovom spektru su sljedeći [21]:

- *Acknowledgement Flooding* napad – ovaj napad pripada skupini DoS napada. Napadači nastoje distribuirati lažne informacije susjednim čvorovima pri radu algoritama za usmjeravanje.

- Napad uskraćivanjem usluge (DoS) – sličan je napadu u percepcijskom sloju gdje je cilj uskratiti dostupnost usluga.
- *Hello-flood* napad – napadači nastoje emitirati zahtjev za „hello“ poruku pomoću lažnog čvora pri čemu povećavaju kašnjenje i smanjuju mrežne performanse.
- Napad prisluškivanjem – vrlo popularna vrsta napada u mrežnom sloju gdje se nastoji doći do povjerljivih i tajnih informacija.
- *Man in the middle* napad (MitM) – ovaj napad je napredna verzija spoofing napada gdje su napadači posrednici između dva objekta koja obavljaju komunikaciju te su u mogućnosti propustiti prave podatke, izmjeniti ih ili jednostavno ne propustiti.
- *Routing* napad – cilj je manipulacija usmjeravanjem podataka u svrhu povećanja mrežnog prometa i zakrčenja.
- Napad selektivnog prosljeđivanja – napadači lažiraju ili kompromitiraju čvorove pri čemu mogu obaviti iste akcije kao i u MitM napadu. Dakle imaju mogućnost propuštanja, stopiranja ili izmjene stvarnih podataka.
- *Sybil* napad – zlonamjeran uređaj ili čvor raspolaže identitetom više uređaja ili čvorova čime smanjuje učinkovitost, forsira njihov rad što može dovesti do uskraćivanja usluge.

Podaci koji ostanu postojani na putu od percepcijskog sloja preko mrežnog sloja do aplikacijskog sloja podložni su još napadima i samim sigurnosnim rizicima koje ima aplikacijski sloj [21]. Napadi koji su najzastupljeniji u aplikacijskom sloju su sljedeći:

- *Sniffing* napad – cilj ovog napada je upasti u sustav i pronaći i ukrasti osjetljive podatke kao što su lozinke, FTP datoteke, e-poštu ili druge bitne podatke.
- Napad ubrizgavanjem zlonamjernog koda – napadači nastoje ubaciti zlonamjerni kod u memoriju čvorova ili uređaja pri čemu zlonamjerni kod može prouzrokovati gubitak svih podataka, oštećenje podataka, pad sustava, neovlaštenu izmjenu podataka ili nešto drugo.
- *Phishing* napad – napadači krivotvore phishing poruke ili web mjesta u svrhu krađe identiteta i dolaska do vjerodajnice za pristup sustavu.
- Napad zatrpavanjem međuspremnika – napadači nastoje preopteretiti i zatrpati radnu memoriju kako bi prouzrokovali pad aplikacije.

- Napad zlonamjernim softverom – IoT uređaji su ugroženi od strane zlonamjernih softvera kao što su trojanski konj, crvi i virusi. Malver ubačen na bilo kojem uređaju može prouzrokovati krađu podataka ili uskraćivanje usluge te trenutno ne postoji integrirani sigurnosni softver koji štiti od prethodno navedenog.
- Softverske ranjivosti i nedostaci – slabosti u konstrukciji softvera te bugovi koji su neizbježni u programiranju uvelike doprinose ranjivosti sustava te se mogu iskoristiti u zlonamjerne svrhe.
- Napad uskraćivanjem usluge (DoS) – kao i u prethodnim slojevima ova vrsta napada je sveprisutna te dovodi do uskraćivanja usluge.

4.2. Najkorišteniji IoT protokoli i njihova sigurnost

IoT svoje usluge pruža putem komunikacijskih protokola kao što su MQTT (engl. *Message Queueing Telemetry Transport*), DDS (engl. *Data Distribution Service*), LoRaWAN (engl. *Long Range Wide Area Network*), AMQP (engl. *The Advanced Message Queuing Protocol*) i drugih koristeći njihov standard za prijenos poruka na siguran način [22]. U sljedećoj podjeli spomenuti su najkorišteniji protokoli te pojedinosti o njima:

- BLE protokol (engl. *Bluetooth Low Energy*) – BLE protokol je protokol izričito male potrošnje energije koji je upravo dizajniran i osmišljen za uređaje s ograničenom količinom energije. Protokol se masovno koristi u završnom dijelu komunikacije prema samom korisniku.
- MQTT protokol (engl. *Message Queuing Telemetry Transport*) [12] – osmišljen je za lake senzor uređaje te prijenos podataka između njih. Sastoji se od tri glavne komponente koje su publisher, broker i subscriber. Publisher šalje podatke prema brokeru dok subscriber ovisno o tome na koji se broker pretplatio, prima informacije s navedenog brokera.
- AMQP (engl. *Advanced Message Queueing Protocol*) – radi se o prijenosnom višekanalnom protokolu s dobrom zaštitom. Autentifikacija se obavlja uz pomoć SASL-a ili TLS-a. Radi na principu TCP protokola te je vrlo brz i dizajniran za okruženje s više klijenata te ima brzu obradu zahtjeva.
- CoAP (engl. *Constrained Application Protocol*) – protokol osmišljen za primjenu pametnog sustava koji koristi REST API strukture, kontrolu zagušenja i unakrsni protokol.

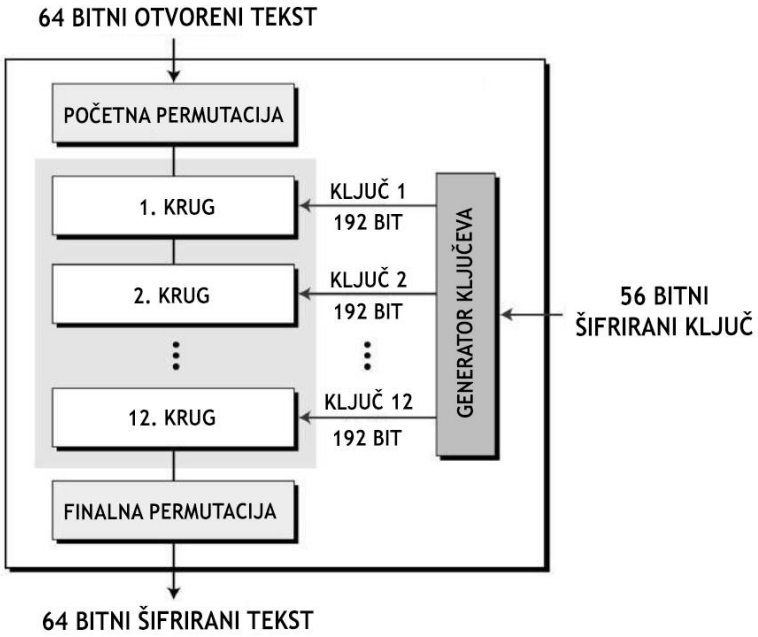
- DDS protokol (engl. *Data Distribution Service*) – radi se o protokolu dizajniranom za komunikaciju M2M (engl. *machine to machine*) odnosno stroj prema stroju. Sličan princip rada ima kao i MQQT protokol, ima mali memorijski otisak te za *Quality of Service* koristi *Multicasting*.

5. NAJBOLJI KRIPTOGRAFSKI ALGORITMI ZA IoT OKRUŽENJE

Neki od najkorištenijih i najbolje ocijenjenih kriptografskih algoritama su: *The Data Encryption Standard* (DES) i *Triple-DES*, *Elliptical Curve Cryptography* (ECC), *Advanced Encryption Standard* (AES), *Digital Signature Algorithm* (DSA), *Rivest-Shamir-Adleman* (RSA), *Blowfish* i *Twofish*. U nastavku će se govoriti o svakom od prethodno navedenih šest kriptografskih algoritama, njihovim primjenama, obilježjima i povijesti.

5.1. Data Encryption Standard (DES) i Triple-DES (3DES)

Data Encryption Standard (DES) koristi ključ veličine 56 bita. Zbog navedene veličine ključa od 56 bita, DES uzima blok od 64 bita čistog teksta kao ulaz i generira blok od 64 bita šifriranog teksta. Kod DES algoritma svaki korak se stručno naziva krugom, te ovisno o veličini ključa varira i broj krugova koji se mora izvesti npr. za ključ od 128 bitova potrebno je izvesti 10 krugova dok za ključ od 192 bita je potrebno izvesti 12 krugova kao što je prikazano na slici 5.1. koja prikazuje princip rada DES algoritma [23].

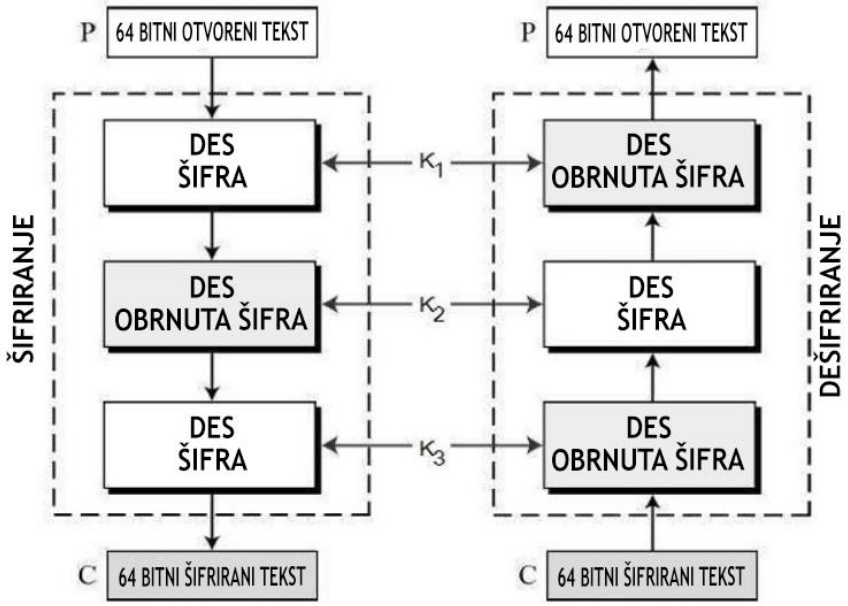


Slika 5.1. Princip funkcioniranja DES algoritma kod dužine ključa 192 bita te 12 krugova [40]

U svojoj biti DES predstavlja algoritam kao blok šifru sa simetričnim ključem što znači da se isti ključ koristi za šifriranje i za dešifriranje. DES se temelji na Feistelovoj blok šifri nazvanoj Lucifer koja je kreirana 1971. godine od strane IBM-ovog istraživača kriptografije Horst Feistel-

a. DES je odobren kao standard šifriranja davne 1976 godine, a svoju dominaciju je izgubio 2002. godine pojavom *Advanced Encryption Standard*-a (AES-a).

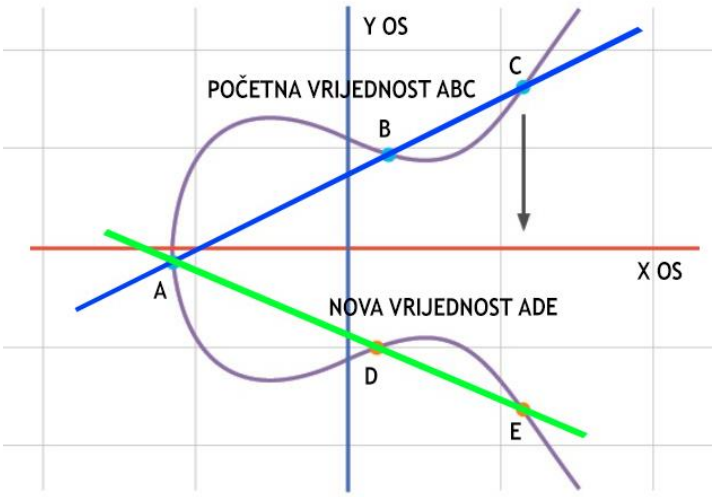
Bitno je napomenuti kako je *Triple-DES* (3DES) odobren za osjetljive vladine podatke sve do 2030. godine. *Triple DES* je simetrična ključ-blok šifra koja primjenjuje DES. Funkcionira na način da šifriranje obavlja prvim ključem (k1), zatim dešifrira drugim ključem (k2) te naposljetku šifrira trećim ključem (k3) kao što je prikazano na slici 5.2.



Slika 5.2. Princip funkcioniranja 3DES algoritma gdje P oznaka predstavlja otvoreni tekst, C oznaka šifrirani tekst i K oznaka pojedine ključeve. [41]

5.2. Elliptical Curve Cryptography (ECC)

Elliptical Curve Cryptography (ECC) je tehnika šifriranja javnim ključem utemeljena na teoriji eliptične krivulje koja je osmišljena s ciljem stvaranja bržih, manjih i učinkovitijih kriptografskih ključeva. Eliptična krivulja u tom slučaju ne predstavlja elipsu nego liniju koja čini petlju koja siječe dvije osi te je krivulja potpuno simetrična duž X osi kao što je prikazano na slici 5.3. [13]. ECC funkcionira na način da koristi dva ključa od čega je jedan javan i svima poznat, a drugi privatan i poznat samo pošiljatelju i primatelju podataka. Matematička jednadžba s javnim i privatnim ključem se može upotrijebiti kako bi se došlo od točke B do točke D, no bez poznavanja privatnog ključa i njegove veličine jako je teško te čak i nemoguće doći od točke D do točke B.



Slika 5.3. Prikaz eliptične krivulje i pravaca simetričnih na os x

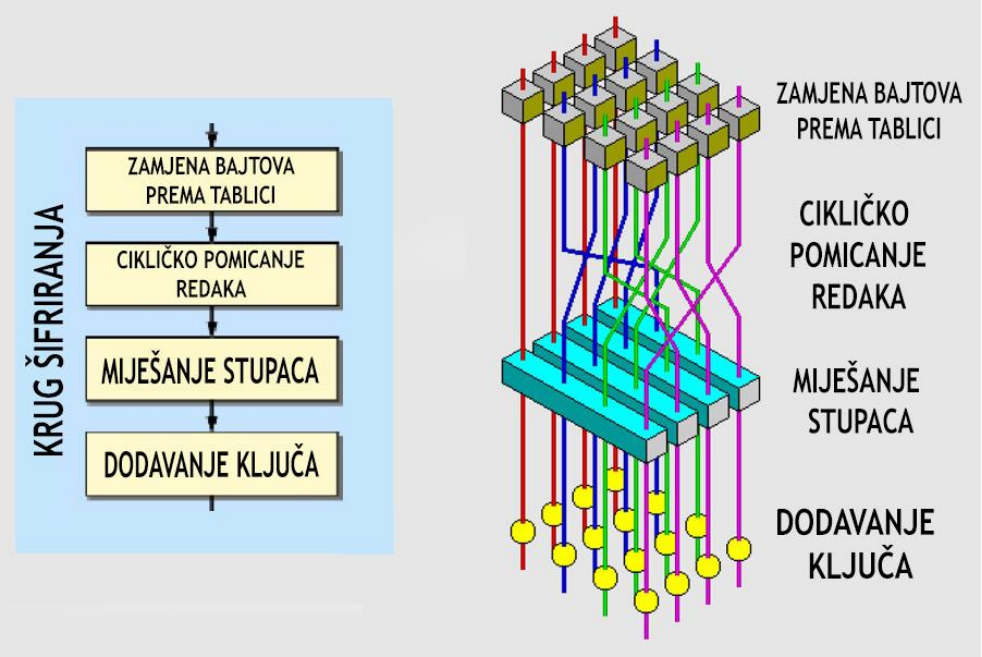
Svojstva i funkcije eliptičnih krivulja se proučavaju više od 160 godina, a prva upotreba u kriptografiji je počela 1985. godine od strane IBM-a. ECC je prvi razvio Certicom, pružatelj sigurnosti mobilnog e-poslovanja. ECC u svojim proizvodima su podržali razni svjetski globalno poznati proizvođači kao što su: Motorola, Siemens, Verifone i mnogi drugi. Korištenje ECC-a u javnom i privatnom sektoru je u velikom porastu u prethodnih 5 godina te se uspijeva boriti sa svojim najvećim konkurentom RSA algortimom. ECC najveći porast upotrebe bilježi upravo u IoT-u kod prijenosa šifriranih podataka s uređaja ograničenih računalnih moći. ECC se smatra vrlo sigurnim ukoliko je veličina ključa zadovoljavajuća. Vlada SAD-a je propisala korištenje ECC-a veličinom ključa od 256 ili 384 bita za internu komunikaciju pri čemu ovisi o razini povjerljivosti podataka. Bitno je napomenuti kako po sigurnosti ECC nije nimalo nesigurniji u odnosu na glavne „konkurente“ kao što je RSA kriptografski algoritam pri čemu je čak u prednosti u vidu memorijskog otiska i brzine šifriranja i dešifriranja.

5.3. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) je način simetrične blok šifre odobrene od strane vlade Sjedinjenih Američkih Država koji za cilj ima zaštitu povjerljivih podataka. AES je implementiran u programsku podršku i sklopovlje širom svijeta te ima jako veliku upotrebu diljem svijeta za šifriranje povjerljivih podataka. Koristi se uveliko za očuvanje državne računalne sigurnosti, kibernetičke sigurnosti i za zaštitu elektroničkih podataka. AES funkcionira tako što obavlja više rundi šifriranja te dijeli poruku u manje blokove veličine 128 bita te je zbog toga sigurniji i pouzdaniji od starijih metoda simetrične enkripcije koje su prethodile [19]. Simetričnost kod AES-a znači da koristi isti ključ za šifriranje i dešifriranje podataka. Pošiljatelj

i primatelj moraju znati i koristiti isti tajni ključ. To AES razlikuje od asimetričnih algoritama koji koriste različite ključeve za šifriranje i dešifriranje. AES dijeli poruku u manje blokove te svaki blok zasebno šifrira te na taj način otvorenu tekstualnu poruku pretvara u nerazumljiv oblik odnosno u šifrirani tekst.

AES također koristi više kriptografskih ključeva od kojih svaki prolazi kroz više krugova enkripcije pri čemu se značajno poboljšava sigurnost te se povećava povjerljivost i integritet. Krug šifriranja se sastoji od nekoliko koraka. Prvi korak je zamjena bajtova prema zadanoj tablici. Nakon tog slijedi cikličko pomicanje redaka. Zatim slijedi miješanje stupaca pri čemu se na kraju obavlja xor operacija sa zadanim ključem tog kruga, kao što je prikazano na slici 5.4.



Slika 5.4. Prikaz jednog kruga šifriranja kod AES algoritma [42]

Za zaštitu povjerljivih i tajnih informacija mogu se koristiti razne duljine ključeva. AES-128 pruža odličnu zaštitu i visoku sigurnost od napada za većinu korisničkih aplikacija. Informacije koje su klasificirane kao strogo povjerljive ili kao državne ili vojne tajne zahtijevaju dodatnu sigurnost te se u tom slučaju koriste veći ključevi kao što su 192 ili 256 bita. Svako povećanje duljine ključa zahtjeva osjetno veću procesorsku moć te sami proces šifriranja i dešifriranja traje duže.

U samo šest godina AES je zaživio u svim bitnim aspektima korištenja te je 2003. godine već bio zadani algoritam za korištenje čak i kod vladinih i povjerljivih informacija. Danas je AES jedan

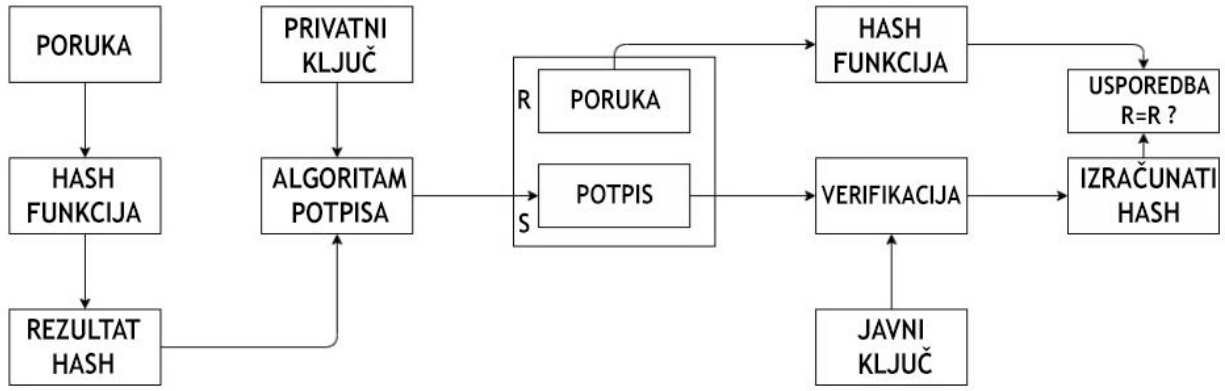
od najpoznatijih i najkorištenijih kriptografskih algoritama sa simetričnim ključem. Primjeri upotrebe su mnogobrojni kao kod npr:

- Podaci na medijima za pohranu (USB i tvrdi diskovi)
- Aplikacije za elektroničku komunikaciju
- Internet preglednici
- Programske biblioteke
- Bežične mreže
- Baze podataka
- Vjerodajnice za prijavu
- VPN

Prednosti AES-a u odnosu na starije algoritme su povećanje sigurnosti budući da uključuje više krugova enkripcije što otežava probijanje, presretanje i krađu šifriranih informacija. Zatim AES ima veliku prednost što je algoritam otvorenog koda koji je dostupan svima te stoga isplativ za implementaciju. Što se tiče provedbe AES je fleksibilan i jednostavan za upotrebu što ga u konačnici čini sigurnim, jeftinim i jednostavnim za korištenje.

5.4. Digital Signature Algorithm (DSA)

Digital Signature Algorithm (DSA) je algoritam koji služi kao način provjere od strane primatelja kako bi bio siguran da je poruka poslana s valjanog i ovjerenog identiteta. DSA funkcionira na način da koristi hash funkciju za stvaranje hash koda. Nasumično generirani broj k se kombinira s prethodno spomenutim *hash* kodom kao ulaz u funkciju potpisa. Funkcija potpisa ovisi o privatnom ključu pošiljatelja te skupu poznatih parametara pri čemu se taj cjelokupni skup može smatrati globalnim javnim ključem. Izlaz funkcije potpisa je potpis s dvije komponente (npr. komponenta s i komponenta r). Kod primanja dolazne poruke generira se hash kod za primljenu poruku. Generirani hash kod se kombinira s potpisom i unosi u funkciju provjere pri čemu kao izlaz iz funkcije provjere se dobije vrijednost jednaka prethodnoj komponenti „r“ ako je potpis valjan kao što je prikazano na slici 5.5.[14].



Slika 5.5. Princip funkcioniranja DSA algoritma [43]

Funkcija potpisa je kreirana na način da samo pošiljatelj uz poznavanje privatnog ključa može generirati valjan potpis.

Prednosti DSA su sljedeće:

- Autentifikacija (sigurni smo tko je pošiljatelj)
- Integritet (bilo kakvom promjenom potpis postaje nevažeći)
- Učinkovitost (omogućuje brze mrežne transakcije)
- Smanjenje troškova (smanjenje papirologije i transporta iste)
- Vremensko označavanje (zaštita od napada ponavljanjima, svježina potpisa)
- Prihvaćenost u svijetu

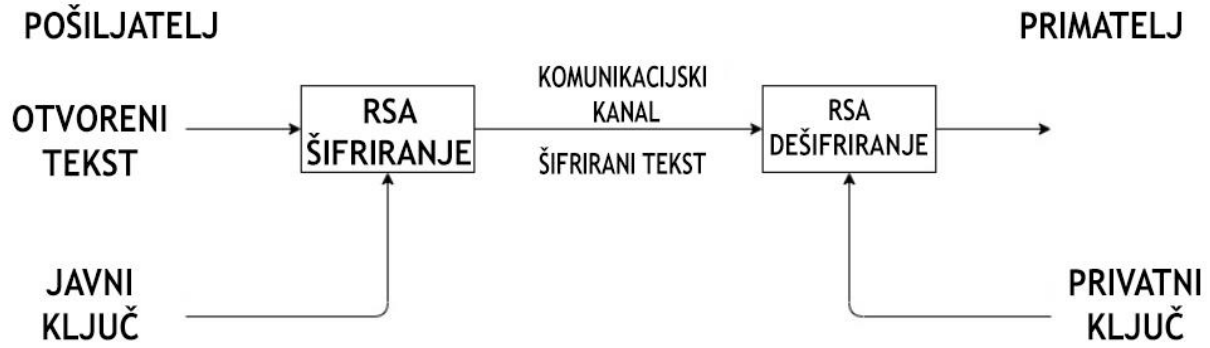
Nedostaci DSA su sljedeći:

- Složenost upravljanja ključem na siguran način
- Ovisnost o infrastrukturi
- Početni troškovi postavljanja
- Pravni i regulativni izazovi
- Potrebna edukacija korisnika
- Ranjivost na kompromitaciju ključa

5.5. Rivest-Shamir-Adleman (RSA)

Rivest-Shamir-Adleman (RSA) algoritam je prethodnik DSA algoritma. Osmišljen je 1977. godine od strane trojice kriptografa i znanstvenika pri čemu je dobio i ime po njihovim

prezimenima, a radi se o Ron Rivest-u, Adi Shamir-u, Leonard Adleman-u. RSA algoritam koristi javni i privatni ključ. Sigurnost algoritma se oslanja prvenstveno na rastavljanje umnoška dva velika prosta broja zbog čega ga je jako teško probiti, te ne postoje javno objavljene metode za probijanje RSA u slučaju korištenja dovoljno velikog ključa. RSA je relativno spor algoritam te se stoga ne koristi za izravno šifriranje korisničkih podataka [27]. Kod RSA pristupa, poruku koju je potrebno potpisati se prvo unosi u hash funkciju pri čemu se generira sigurni hash kod fiksne duljine. Zatim se koristi privatni ključ pošiljatelja za šifriranje *hash* koda te se tako dobije potpis. Potom slijedi slanje potpisa i poruke željenom primatelju. Primatelj vrši provjere validnosti primljene poruke izračunavajući njen *hash* kod. Primatelj pomoću javnog ključa pošiljatelja dešifrira već šifrirani potpis kao što je prikazano na slici 5.6.



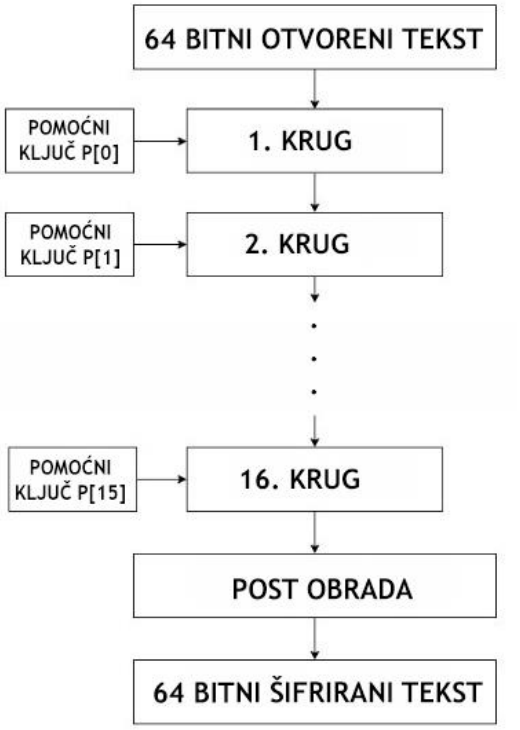
Slika 5.6. Princip rada RSA algoritma [44]

U slučaju da se dešifrirani potpis podudara s hash kodom koji je izračunao primatelj, potpis se smatra valjanim. Budući da samo pošiljatelj ima pristup privatnom ključu, jasno je tko jedini može biti kreator važećeg potpisa.

5.6. Blowfish i Twofish

Blowfish je simetrična 64-bitna blok šifra promjenjive duljine kreirana od strane Bruce Schneier-a 1993. godine kao alternativa DES algoritmu. Prednosti nad DES-om su bili znatno veća brzina i dobar „*encryption rate*“. Blokovi su fiksne veličine od 64 bita, dok veličina ključa može varirati od 32 do 448 bitova. Algoritam funkcionira tako što kreira 18 pomoćnih ključeva koje sprema u niz. Zatim se kreiraju četiri zamjenska pretinca pri čemu svaki ima 256 unosa. Potom slijedi šifriranje koje se sastoji od dva dijela. Prvi dio je šifriranje koje se sastoji od 16 rundi pri čemu

se u svakoj unosi čisti tekst iz prethodne i odgovarajući ključ. Drugi dio je post obrada prethodnog dijela čime se dobije šifrirana poruka u blokovima kao što je prikazano na slici 5.7.



Slika 5.7. Princip šifriranja kod Blowfish algoritma [45]

Kod dešifriranja slijedi identičan tijek pri čemu se pomoćni ključevi koriste u obrnutom redoslijedu [1].

Blowfish je brz algoritam osim u slučaju promjene ključeva jer svaki novi ključ zahtjeva prethodnu obradu koja iznosi veličine 4KB teksta. Brži je i puno bolji od DES algoritma što je veliki benefit. Mana mu je korištenje blokova veličine 64 bita što ga čini ranjivim na neke vrste napada kao što su „*Birthday attack*“. Poznato je da *Blowfish* sa smanjenim brojem rundi tj. prolazaka je ranjiv na napade običnim tekstom (diferencijalni napadi 2. reda – 4. runde).

Twofish je simetrična blok šifra veličine blokova 128 do 256 bita. Jedan je od pet finalista *Advanced Encryption Standard Contest*-a, no nije odabran za standardizaciju. Nasljednik je svog prethodnika *Blowfish*-a. Također kao i *Blowfish*-u, struktura je zasnovana na Feistelovim mrežama, koristi isto 16 rundi. Prednost mu je povećanje veličine bloka dok je veličina ključa više ograničena nego kod *Blowfisha* te veličina ključa može iznositi od 128 do 256 bitova [2]. Što se tiče sigurnosti otporan je na poznate napade te pruža dobru razinu zaštite.

Prednosti *Twofish*-a su sljedeće:

- Visoka razina sigurnosti (otporan na kriptoanalitičke napade)
- Promjenjiva duljina ključa (prilagodba sigurnosti shodno zahtjevima)
- Učinkovite performanse usprkos robusnosti
- Prikladan za širok raspon aplikacija

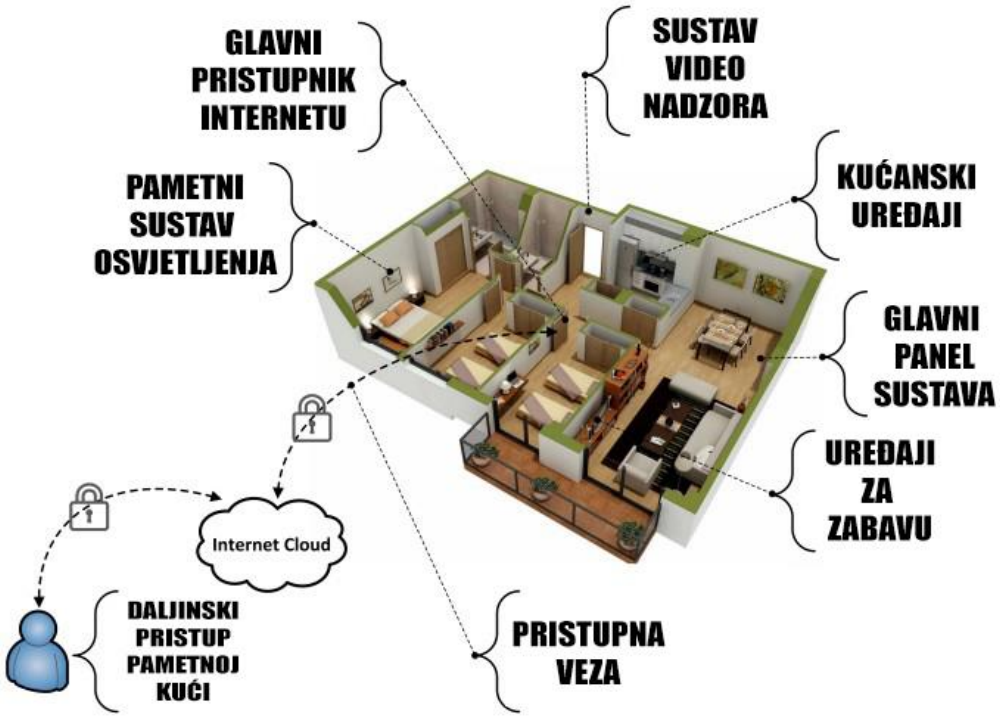
Jedan od najvećih nedostataka je složeniji raspored ključeva zbog čega je nešto sporiji od AES-a te manja popularnost koja zapravo nije mana, nego je uzrokovana neodabirom na izboru „*Advanced Encryption Standard Contest*“ pri čemu nije *Twofish* ušao u standardizaciju i zaživio „punim plućima“.

6. METODE ZAŠTITE PAMETNIH KUĆA I STANOVA

Sustavi Interneta stvari duboko su ušli u sferu korištenja kod kuća, stanova, hotela te ostalih prostora i objekata namijenjenih za život. U IoT paradigmi najosjetljiviji i najranjiviji dio sustava je sama komunikacija međusobno između uređaja ili između uređaja i korisnika, zatim autentifikacija korisnika i sami pristup sustavu te podacima. U prethodnim poglavljima govorilo se o samoj arhitekturi IoT-a, slojevima te arhitekture i napadima kojima je IoT izložen. Pojedini sigurnosni problemi rješivi su boljim kriptografskim algoritmima, a pojedini razvojem boljih algoritama za detekciju, autentifikaciju itd. U nastavku slijedi analiza glavne raspodjele objekata u pametnoj kući, rizika kojima su ti objekti izloženi te način zaštite kojim se mogu ti objekti i sami vlasnici pametne kuće zaštititi. Prije toga potrebno je definirati što je to „pametna kuća“.

Pametna kuća predstavlja sustav senzora, kućanskih aparata i pametnih uređaja povezanih putem interneta s ciljem postizanja daljinskog upravljanja i daljinskog pristupa stambenoj okolini [8]. Dakle u cjelini sustav se sastoji od malih računalnih objekata namijenjenih za prepoznavanje i pružanje personaliziranih usluga korisnicima koji vrše interakciju. Cilj pametne kuće je osigurati automatizaciju, udobnost i sigurnost. Maskirani cilj koji se krije iza udobnosti i sigurnosti je zasigurno smanjenje ispuštanja štetnih plinova, ušteda i pojednostavljanje baratanja energijom u samom objektu. Osim samog pružanja luksuza gdje pomoću jednog klika se može npr. manipulirati klima uređajem ili sustavom grijanja, jako bitna je i perspektiva uštede i olakšanje baratanja sustavima koji su najveći potrošači u samom domu što će postati sve bitnije u budućnosti i zelenoj tranziciji.

Tehnički gledano sustav pametne kuće se može podijeliti na pet jedinica: senzori i aktuatori, uređaji kojima se manipulira, kontrolna mreža, upravljač i daljinski upravljač. Sustav kućne automatizacije se dijeli na dvije kategorije: lokalnu kontrolu i daljinsku kontrolu. Lokalna kontrola se odnosi na provođenje manipulacije upravljačem koji je stacionaran ili bežično povezan sa sustavom te se koristi unutar doma. Daljinska kontrola se odnosi na manipulaciju sustavom posredstvom internetske veze s osobnog računala ili mobilnog uređaja. Zbog raznolikih tipova uređaja, različitih vrsta komunikacije te različitih procesorskih moći i memorijske ograničenosti, postići sigurnost predstavlja pravi izazov [18]. Svaka od prethodno pet navedenih podjela ima svoje slabe strane i potencijalne načine zaštite i prostor za poboljšanje, no bitnu ulogu igra i novac jer od svakog uređaja se očekuje da bude funkcionalan, lijepo dizajniran, kvalitetan sa što više funkcija, a da cijena bude pristupačna i niska pri čemu se dolazi u proturječje s prethodno navedenim.



Slika 6.1. Ilustracija pametne kuće i dijelova sustava

Sustav pametne kuće najčešće ima implementirane sljedeće podsustave koji su ujedno i najpopularniji među korisnicima, a to su: pametni sustav upravljanja osvjetljenjem, pametni sustav video nadzora i sigurnosti, pametni sustav upravljanja kućanskim uređajima, pametni sustav upravljanja uređajima za zabavu, sustav glavnog panela, sustav pristupa internetu i oblaku namjenjen za daljinski pristup kao što je prikazano na slici 6.1. [8]. Svaki od prethodno spomenutih podsustava i sustava ima svoje mane i ranjive točke. Tako sustav upravljanja osvjetljenjem koji je među najpopularnijim sustavima korištenim u pametnim kućama ima za cilj zaštititi se od manipulacije podacima što ujedno može proizvesti i najveću štetu po vlasnika objekta. Kako bi se sustav upravljanja osvjetljenjem zaštitio, potrebno je imati jako dobro šifrirane podatke i autentifikaciju na visokoj razini. Sustav video nadzora i sigurnosti je glavni na udaru te se izlaže najvećim rizicima od napada. Tu postoje veliki rizici od manipulacije kamerama, alarmnim sustavom, senzorima i krađe podataka. Ukoliko provalnik dođe do alarmne šifre, lako može ugasiti sigurnosni sustav čak i fizički tako da u tom dijelu postoje veliki rizici. Osim dobre enkripcije i autentifikacije bitno je i fizički sakriti upravljački dio sigurnosnog sustava te na taj način otežati pronalazak. U sustavu upravljanja kućanskim uređajima najveći rizici su pristup log podacima i manipulacija uređajima. Sama sigurnost kućanskih aparata se može poboljšati promjenom obične konfiguracije koja dolazi s uređajima na neku prilagođenu koja se razlikuje te time otežava pristup, manipulaciju i krađu log podataka. Sustav uređaja za

zabavu najčešće je izložen zlonamjernom kodu koji usporava sustav, obavlja štetne radnje. Problem kod ovog dijela je što zlonamjerni kod može postojati jako dugo na određenom uređaju dok ne dođe do okidanja pokretača koji ga pokreće gdje on kreće raditi štetu ili zlonamjerne radnje. Ovaj dio sustava se može nadgledati stalnom provjerom performansi sustava ili sigurnosnim skeniranjima. Sustav glavnog panela je najmoćnija točka u pametnoj kući. Ukoliko dođe do neovlaštenog pristupa, moguće je rukovati svim sustavima i napraviti ogromnu štetu. Najveći rizik je dakle rizik od neovlaštenog pristupa što se mora osigurati ekstremno jakom autentifikacijom. Sustav pristupa internetu i sam WiFi sustav također su jedna od bitnih meta. Sustav pristupa WiFi-ju mora imati jaku zaštitu kako ne bi došlo do otuđenja WiFi pristupne točke. Sustav pristupa internetu ima najveću bojaznost od samog presretanja prometa. Kako bi se osigurao taj dio sustava, potrebno je pratiti stalno količinu prometa, imati jako dobru enkripciju tj. koristiti dobre i pouzdane kriptografske algoritme. Preporučeno je koristiti IDS, sustav namijenjen praćenju mrežnog prometa i događaja koji ima implementiranu analizu i detekciju sigurnosnih prijetnji. Također popularan je i preporučljiv IPS sustav koji kao glavnu značajku ima detekciju upada [5].

Glavni problem pri zaštiti pametnih kuća je nedostatak računalne moći, velikog prostora za pohranu i velike količine memorije. Zbog prethodno navedenog nije moguće implementirati ozbiljne i zahtjevne sustave sigurnosti te ta rješenja jednostavno nisu uvijek dostupna. Rješenje za taj problem je primjena distribuiranog mehanizma šifriranja i energetski učinkovite enkripcije kako bi sa što manje resursa postigli što veću razinu zaštite. IoT pristupnik je osjetljiv na razne vrste napada koji su objašnjeni u prethodnim poglavljima te je jako bitno koristiti učinkovite kriptografske algoritme poput kriptografije eliptične krivulje (engl. *Elliptical Curve Cryptography*, ECC) i drugih lakih kriptografskih algoritama i kriptografskih shema koje su u prethodnom dijelu rada navedene.

7. METODE ZAŠTITE PAMETNIH INDUSTRIJSKIH POGONA

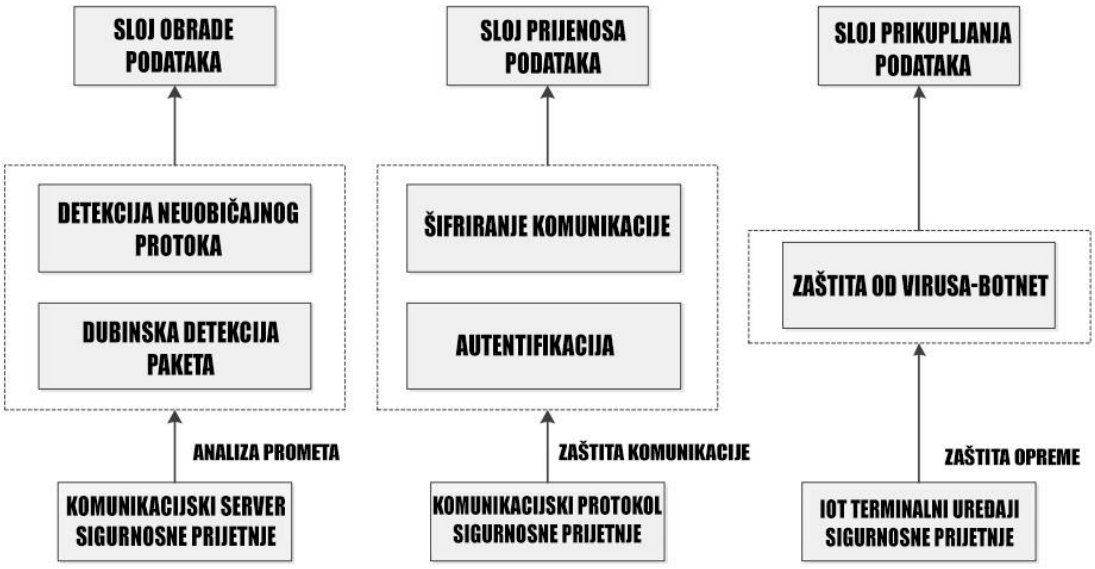
Industrijski IoT se može smatrati kombinacijom automatiziranih industrijskih sustava i samog IoT sustava. U same industrijske sustave potrebno je u cjelini uvesti senzorske sustave, automatizirane industrijske sustave praćenja i proizvodnje te računalne analize i internet. Analiza i obrada industrijskih podataka koja je na ovaj način daleko olakšana utječe značajno na poboljšanje kvalitete proizvoda, povećava proizvodnu učinkovitost i značajno smanjuje troškove upravljanja.

Industrijski Internet stvari se smatra podskupom Interneta stvari. Industrijski IoT se prema načinu prikupljanja, prijenosa i obrade informacija može podijeliti na 3 sloja [16] :

- sloj prikupljanja podataka
- sloj prijenosa podataka
- sloj obrade podataka

Sloj prikupljanja podataka obuhvaća upravljačke uređaje i upravljačku opremu pod koju spadaju PLC (engl. *Programmable Logic Controller*) i drugi kontroleri te uređaji u polju koji uključuju razne vrste senzora koji su odgovorni za prikupljanje podataka. Operator može na temelju podataka direktno djelovati na sustav te manipulirati istim prije prijenosa i obrade. Sljedeći sloj je sloj prijenosa podataka koji predstavlja otvorenu mrežu koja povezuje i vrši integraciju između senzorskih mreža, mobilnih mreža i interneta. Ta mreža je projektirana prema međunarodnim ili industrijskim standardima te najčešće koristi tehnologije bežične komunikacije kao što su Wi-Fi, Bluetooth, RFID, Zig Bee, WAN male snage, mobilne mreže, razne internetske mreže, MQTT te LPWAN koja je namijenjena baš za IoT sustave. Naime LPWAN predstavlja širokopojasnu mrežu niske snage koja omogućuje komunikaciju dugog dometa pri niskoj brzini prijenosa između IoT uređaja kao što su senzori koji se napajaju baterijama. LPWAN se u praksi najviše koristi za stvaranje privatne bežične senzorske mreže gdje raspolaže brzinom od 0.3kbit/s do 50 kbit/s po kanalu [3]. Posljednji sloj je sloj obrade podataka koji uključuje komunikacijske poslužitelje, podatkovne servere i terminale za daljinsko praćenje. Industrijski IoT kao i klasični koristi pohranu u oblaku, no ima puno više podataka te koristi specifičnu programsku podršku za obradu istih što zahtjeva provjeru integriteta i povjerljivosti industrijskih podataka te identifikaciju terenske terminalne opreme. Umrežavanje uređaja i industrijskih platformi u oblaku ima i svoje slabe strane kao što su ranjivost na upad, moguće uzrokovanje zastoja i prekida u proizvodnji, materijalne štete, opasnost za ljude i okoliš...

Ovisno o prethodno navedenoj arhitekturi i podijeli na 3 glavna sloja, svaki sloj ima svoje slabe točke i prijetnje kojima je izložen te protumjere koje osiguravaju veću sigurnost i potencijalnu zaštitu. Veliki problem predstavlja mogućnost upada u LAN mrežu pri čemu napadači lako mogu presretati podatke i saznati povjerljive informacije. Trenutno najkorišteniji protokoli za komunikaciju s oblakom su MQTT, AMQP, XMPP [20]. Problem kod protokola za komunikaciju je to što komunikacijski proces nije šifriran niti autentificiran što omogućava napadačima koji su upali u mrežu da lako presretnu podatke pritom se kod MQTT-a može postaviti lažni MQTT klijent na MQTT poslužitelj te može slati lažne informacije. Glavni problem MQTT je šifriranje podataka koji se može osigurati raznim kriptografskim algoritmima te veliki problem je i autentifikacija. Prijenos podataka otvorenim tekstom koji nije šifriran može biti poguban. Kako MQTT podržava TCP protokol to omogućava izvođenje napada „*Man in the middle*“ čovjek u sredini s lažnog klijenta. Takav način prijenosa informacija bez dodatne zaštite kriptografskim algoritmima je poguban i predstavlja veliki sigurnosni rizik za postrojenje, ljude i okolinu. MQTT psolužitelj je zasigurno jedna od glavnih meta napadača jer ako napadač uspije zaobići autentifikaciju u sloju prijenosa podataka, napadač može slati podatke s lažnim informacijama, te zatrpavati poslužitelj s paketima što će rezultirati kvarom i neispostavljanjem usluge. Tradicionalni vatrozidi ne mogu zaštititi od ovakvih vrsta napada u potpunosti, nego je potrebno provesti detaljnu inspekciju paketa.



Slika 7.1. Sigurnosni sustav i potrebe industrijskog IoT-a [16]

Rješenje za poboljšanje sigurnosti kod industrijskog IoT-a je prikazano na slici 7.1. Kako bi se poboljšala sigurnost sloja prikupljanja podataka moraju se zaštititi terminalni uređaji koji prikupljaju podatke. Moraju se skenirati i pratiti portovi te postaviti efikasne obrambene mjere od pojedinih vrsta napada (npr. *Zombie* napad) te mora se osigurati provjera terminalnih uređaja i njihovog stanja tj. jesu li oteti ili ne. Sigurnost sloja prijenosa podataka mora implementirati visok stupanj autentifikacije i jaku enkripciju. Podaci se moraju šifrirati s učinkovitim kriptografskim algoritmima kako bi se zaštitili od krađe podataka. Za sigurnost sloja obrade podataka potrebno je zaštititi poslužitelj detaljnom analizom paketa. Dubokom analizom potrebno je spriječiti dospijeće lažnih paketa do poslužitelja, te spriječiti sve ostale vrste napada koje se temelje na lažnim paketima i zatrpavanjem poslužitelja istim.

8. PREDNOSTI I NEDOSTACI KORIŠTENJA KRIPTOGRAFSKIH ALGORITAMA U OKRUŽENJU INTERENTA STVARI

Korištenje kriptografskih algoritama u okruženju Interneta stvari je od presudnog značaja jer upravo najranjivija točka IoT sustava je komunikacija tj. prijenos podataka ka oblaku putem raznih protokola gdje su podaci najranjiviji te najizloženiji sigurnosnim rizicima. Ukoliko se kao kod MQTT-a podaci prenose nešifrirani, tada je cijeli sustav izložen nesnosnom riziku te je samo pitanje vremena kada će postati zanimljiv nekom od napadača koji će to zloupotrijebiti u ostvarivanju svog cilja. Dakle bitno je navesti kako korištenje kriptografskih algoritama predstavlja glavni stup u osiguravanju zaštite IoT sustava i sigurne komunikacije u konačnici.

Pojedini kriptografski algoritmi pružaju veću sigurnost nego ostali, no zahtijevaju i veću računalnu moć ili imaju manju brzinu. U samom projektiranju sustava, ovisno o čemu se radi i koji su zahtjevi postavljeni kao cilj, potrebno je odabrati i pogodan kriptografski algoritam. Pojedini kriptografski algoritmi su simetrični što znači da koriste isti ključ za šifriranje i dešifriranje dok su pojedini asimetrični što znači da koriste različite ključeve za šifriranje odnosno dešifriranje. Ovisno o situaciji i primjeni sustava bira se i sama vrsta algoritma pa se može istaknuti kako asimetrični algoritmi nisu pogodni za industriju zbog svoje kompleksnosti u komunikaciji pri čemu u industriji se barata s daleko više informacija i podataka nego u pametnoj kući. Potom je također bitna i veličina bloka te veličina ključa. U pojedinim sustavima ako se želi maksimalna sigurnost, onda se koristite algoritmi koji omogućavaju velike dužine ključa. S druge strane ako informacije koje se prenose u pojedinoj komunikaciji nisu na razini izrazito povjerljivih informacija, pogodno je koristiti manji ključ što omogućava bržu obradu i zahtijeva manju računalnu moć. Nekada je potrebno imati veću sigurnost, a ograničenje hardvera to ne dopušta zbog ograničenosti u računalnoj moći, memoriji ili nekom drugom segmentu te je tada potrebno napraviti kompromis u sigurnosti ili prisegnuti za nekim manje robusnim algoritmima koji mogu pružiti približnu razinu zaštite [11].

Među najkorištenije kriptografske algoritme se polako probija i ECC (kriptografija eliptične krivulje) koja predstavlja tehniku šifriranja koja zahtjeva relativno male računalne zahtjeve, ima zadovoljavajuću brzinu te nema veliku robusnost. No navedena tehnika npr. ne odgovara u sustavima gdje se raspolaže s brojnim resursima i želi postići značajna razina sigurnosti pa tako ovisno o potrebama mogu se koristiti razni kriptografski algoritmi koji odgovaraju traženim zahtjevima.

Najbitnije kod odabira kriptografskih algoritama je točno postaviti zahtjeve kojima se teži te točno znati s kojim resursima se raspolaže. Kada je to jasno postavljeno onda se treba težiti sljedećem:

- Odabir vrste kriptografije prema resursima i potrebama
- Odabir algoritma s odgovarajućom dužinom ključa
- Odabir algoritma s odgovarajućom veličinom bloka
- Odabir algoritma s zadovoljavajućom brzinom
- Odabir algoritma s zadovoljavajućom robusnosti

Ukoliko se zahtjevi ne postave dobro, vrlo lako može doći do korištenja kriptografije i algoritma koji pruža premalo ili previše u odnosu na postavljene zahtjeve što ni u jednom slučaju nije dobro. Ukoliko je algoritam podkapacitiran, neće pružiti dovoljnu razinu zaštite. Ukoliko je prekapacitiran imat ćemo zaštitu koju ćemo platiti visokom cijenom što se tiče sporosti i neefikasnosti sustava. Istaknut će se problemi s padovima i sporosti te uskraćenju usluga jer resursi kojima se raspolaže nisu dostatni za efikasno funkcioniranje. Zbog svega prethodno navedenog, najveći potencijal za primjenu u IoT zaštiti imaju razne kriptografske sheme koje funkcioniraju na temelju lakih kriptografskih algoritama. One predstavljaju skup raznih protokola i algoritama koji zajedno čine cjelinu i poboljšavaju razinu zaštite.

9. ZASTUPLJENOST I BUDUĆNOST KRIPTOGRAFSKIH ALGORITAMA U OKRUŽENJU INTERNETA STVARI

U samim počecima Interneta stvari kriptografski algoritmi nisu ozbiljno bili shvaćeni niti duboko implementirani. Primjer za to je i najpopularniji MQTT i drugi koji nisu šifrirali svoju komunikaciju tj. prijenos informacija. Sa samom popularizacijom IoT-a i zadiranjem u sve moguće pore života, došlo je do implementacije u sustave koji zahtijevaju sigurnost jer u protivnom može doći do ozbiljnih posljedica i ugroze imovine, ljudi i okoliša. Veliki problem u samim počecima je bio i nedostatak algoritama namijenjenih za IoT jer ti algoritmi pogotovo u to vrijeme kada je oprema bila ograničenija računalno nego danas, su morali pružati efikasno šifriranje i dešifriranje s minimalnom robusnosti. Algoritmi koji bi ispunjavali rad na takvim uređajima te još pružali dobru brzinu su bili nužni te je krenuo onda i razvoj algoritama koji bi omogućili traženo i ispunili potrebne zahtjeve. S razvojem sklopovlja gdje se na manje čipove moglo smjestiti više toga uz manju cijenu postalo je čak moguće koristiti i starije algoritme jer više nije bio presudan utrošak resursa te sami resursi s kojima se raspolaže.

Kriptografski algoritmi postaju osnova za sigurnost te svaka ozbiljna implementacija IoT sustava je nezamisliva bez njih. IoT je na osnovu korištenja i razvoja efikasnih kriptografskih algoritama uspio ući i u područja gdje je sigurnost i povjerljivost informacija na prvom mjestu kao što su primjena u vojne svrhe, industrijske svrhe, baratanje podacima koji su klasificirani kao strogo povjerljivi, primjena u bankama, automobilskoj industriji i drugo.

IoT se danas primjenjuje u raznim granama, a kriptografski algoritmi su neizostavan dio IoT sigurnosti. Neke od primjena su sljedeće:

- Pametne kuće
- Pametni gradovi
- Industrija (primarni,sekundarni i tercijarni sektor)
- Vojska
- Automobilska industrija i automobili
- Poljoprivreda
- Briga o zdravlju
- Medicina
- Banke, državne institucije i drugo...

Budućnost kriptografskih algoritama je svakako i dalje u primjeni u IoT svijetu i to u daleko većoj mjeri nego danas. S razvojem tehnologije postavljaju se sve veći zahtjevi kako pred IoT u cjelini tako i pred kriptografske algoritme koji moraju osigurati integritet, povjerljivost i zaštitu podataka. U budućnosti će kriptografski algoritmi morati biti još sigurniji bilo to u vidu dužih ključeva, većih blokova, provođenja više rundi u procesu šifriranja ili provođenju neke nove dosad neviđene tehnike jer napadači napreduju zajedno u korak s algoritmima te nikada ne stoje u mjestu niti se može očekivati da će jedan algoritam koji je moguće razviti sada, biti dostatan i u bližoj budućnosti za osiguravanje zaštite podataka pri samoj komunikaciji [17]. Što se tiče industrije i vojske zasigurno postoji velika potreba za još sigurnijim kriptografskim algoritmima koji će uz male računalne zahtjeve i malu potrošnju energije i resursa osigurati još veću zaštitu.

U cjelini kada sagledamo trenutnu situaciju u IoT svijetu, taj svijet ne bi mogao zaživjeti punim plućima bez kriptografskih algoritama tako da taj dio i razvoj samih algoritama će samo pogurati i IoT da prodre u upotrebu čak i u najosjetljivijim granama gdje je sigurnost uvijek upitna.

Slika 9.1. Ilustracija primjene kriptografije

10. UTJECAJI I POSLJEDICE NAPADA NA IOT SUSTAV

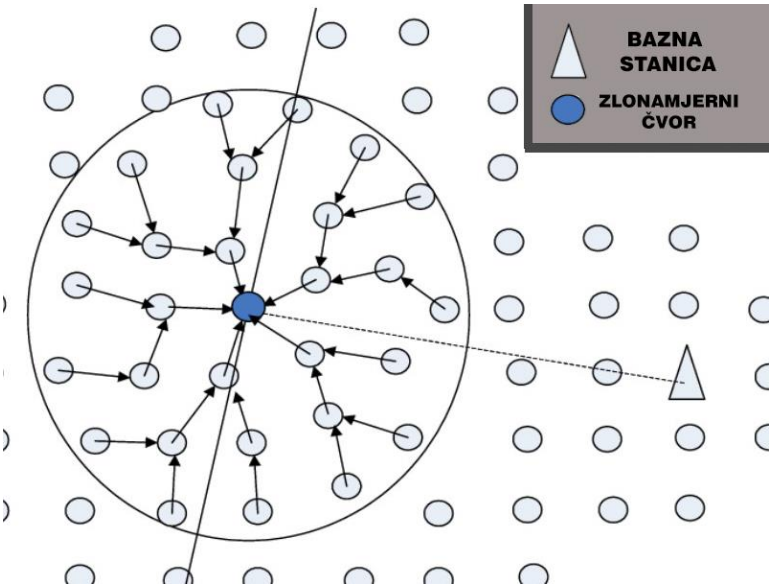
Sustavi Interneta stvari ovise o raznim ograničenjima i propustima zbog kojih sadrže potencijalno slabe točke koje napadači nastoje pronaći. Pod ograničenjima se smatraju ograničenja u vidu količine memorije, ograničenja u vidu napajanja ili količine energije koju pojedine komponente imaju na raspolaganju. Naime, ukoliko pojedina vrsta komunikacije zahtjeva više energetskih resursa nego što možemo osigurati, tada dolazi do kompromisa koji štetno utječe na samu sigurnost jer odabir lošijeg algoritma ili kriptografije nas izlaže daleko većem riziku. Osim memorije i napajanja, bitna je i procesorska moć, udaljenost komunikacije, kvaliteta komponenti i ostalo. Povrh svega glavni uvjet je novac odnosno kapital koji je na raspolaganju za projektiranje pojedinog sustava jer jeftinije komponente rezultiraju većoj izloženosti i slabijoj zaštiti. Usprkos svemu, veliku ulogu ima i ljudska pogreška pri kreiranju sustava, projektiranju sustava, samom osposobljavanju sustava, kreiranju softvera itd. Odabir pogrešne tehnologije može lako upropastiti sve prethodno odrađene korake. Primjer odabira loše tehnologije je korištenje MQTT-a koji nema nikakvu zaštitu za prijenos podataka što se mora nadoknaditi implementacijom šifriranja poruka gdje se mora osigurati odgovarajući stupanj zaštite. IoT sustavi su izvrgnuti raznim vrstama napada koji su detaljno opisani u poglavlju 4.1., a u ovom poglavlju će se detaljnije prikazati pojedini napadi te posljedice koje oni uzrokuju i potencijalna rješenja koja bi u budućnosti osigurala zaštitu od istih.

10.1. Sinkhole napad

Sinkhole napad funkcionira na način da mrežni promet preusmjeri na zlonamjerni čvor koji je pod kontrolom napadača. Ne predstavlja se kao najkraći put, ali manipulira usmjeravanjem kako bi promet putovao preko zlonamjernog čvora. Uzrok ove vrste napada je slabost u mrežnoj infrastrukturi i ranjivost protokola usmjeravanja što omogućava preusmjeravanje prometa preko željenog čvora koji ima mogućnost analiziranja, izmjene ili odbacivanja paketa.

Ova vrsta napada direktno utječe na IoT sustav tako što omogućava manipulaciju, izmjenu i odbacivanje paketa podataka čime se direktno utječe na rad sustava. Naime, ako je sustav očitao postojanje dima, povišen CO_2 , a napadač ispusti taj paket ili ga izmjeni može prouzrokovati totalnu štetu čiji je uzrok požar. Ista situacija se može odnositi na bilo koja druga očitanja i akcije za koje je IoT sustav projektiran. Ova vrsta napada je pogubna za sustave koji obrađuju

podatke u stvarnom vremenu. Na slici 10.1. prikazana je shema *Sinkhole* napada te zaraženi čvor.



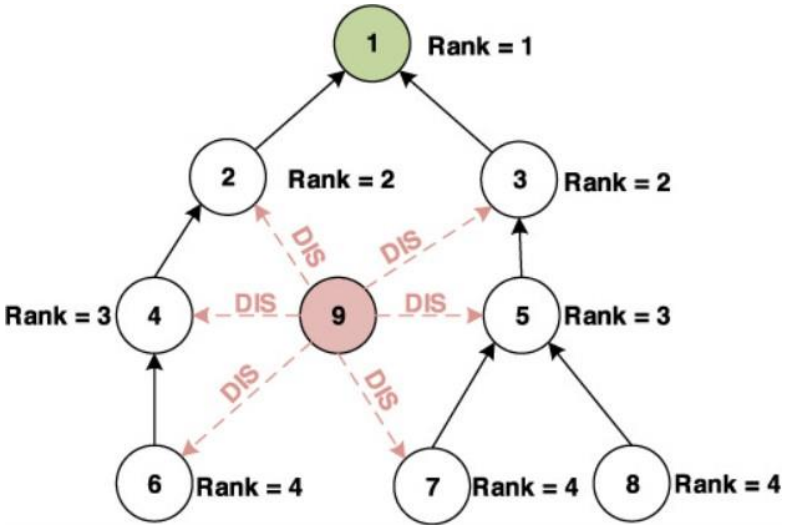
Slika 10.1. Ilustracija Sinkhole napada [46]

Za zaštitu od ove vrste napada moguće je provesti nekoliko strategija. Potrebno je koristiti sigurne i robusne protokole za usmjeravanje koji imaju mogućnost otkrivanja zlonamjernog čvora i sprječavanje manipuliranja usmjeravanjem kako ne bi došlo do usmjeravanja prometa preko zlonamjernog čvora. Potrebno je osigurati autentifikaciju svih uređaja u mreži međusobno kako bi se prepoznao lažni čvor i na vrijeme spriječila komunikacija i usmjeravanje preko istog. Jako bitnu ulogu imaju sustavi za otkrivanje upada koji se implementiraju za nadzor mrežnog prometa i otkrivaju neobično ponašanje te mogu detektirati *Sinkhole* napad. Jako bitnu ulogu ima šifriranje podataka gdje se mora osigurati dovoljno jaka enkripcija koja bi spriječila zloupotrebu podataka koji su presretnuti. Posljednja strategija je primjena segmentacije gdje se uređaji raspoređuju u različite mrežne segmente na temelju njihovih funkcionalnosti ili sigurnosnih zahtjeva. Skup ovih strategija uvelike bi osigurao dobru zaštitu i prevenciju protiv *Sinkhole* napada.

10.2. DIS Flood napad

Kod LoWPAN mreža koje su IPv6 bazirane koristi se RPL protokol koji ima veliku slabost koja se iskorištava za novu vrstu napada zvanu DIS *Flood* napad. Kod RPL protokola važnu ulogu ima čvor za pridruživanje mreži koji šalje DIS poruke ostalim čvorovima kako bi dobili

informacije o usmjeravanju. Napadač može iskoristiti ovaj mehanizam i strukturu tako što bi zlonamjernim čvorom slao DIS poruke susjednim čvorovima i zatrpavao ih traženjem nelegitimnih informacija o usmjeravanju. U normalnoj situaciji novi čvor šalje DIS poruke (poruke koje se koriste se za održavanje topološke baze podataka između čvorova) dok ne primi DIO poruku (poruka koja se koristi se za usmjeravanje u mrežama s niskom potrošnjom energije i visokom otpornošću na gubitak podataka) nekog od susjednih čvorova te onda slijedi traženje pristupa dodijeljenom čvoru kao što je prikazano na slici 10.2.



Slika 10.2. Princip slanja DIS poruka susjednim čvorovima od strane čvora 9 [47]

Na ovaj način DIS napadi utječu na performanse mreže i sustava tako što dolazi do opterećenja, smanjenja brzine prijenosa i odziva te mogućeg preopterećenja mreže.

Tom vrstom napada dolazi do opterećenja čvorova koji odgovaraju na DIS poruku i time dolazi do kašnjenja i smanjenja brzine prijenosa i odziva. Primanje DIS poruka kod čvorova uzrokuje ponovno postavljanje mjerača vremena što uzrokuje problem zastoja i kašnjenja.

Moguća zaštita od DIS *Flood* napada je izbjegavanje korištenja mreža koje koriste RPL protokol jer sam njegov mehanizam ima nedostatak pogodan iskorištavanju i zloupotrijebi. Druga mogućnost je korištenje mehanizma koji ima dovoljno dobru detekciju zlonamjernog čvora i DIS napada pa na taj način omogućuje dovoljno brzu reakciju koja bi spriječila daljni nastanak štete.

Tablica 10.1. Prikaz rezultata DIS napada na IOT sustav na pokaznom javno objavljenom primjeru tvrtke Tetcos [28]

	PROPUSNOST (Mbps)		**KAŠNJENJE (ms)**	
Stopa generiranja (Kbps)	**Pod DIS napadom**	**Bez DIS napada**	**Pod DIS napadom**	**Bez DIS napada**
60	0.06	0.06	1394.49	51.80
80	0.06	0.08	9896.58	51.75
100	0.07	0.10	15553.54	51.76
120	0.07	0.12	19988.49	239.62

10.3. Zero-day napad

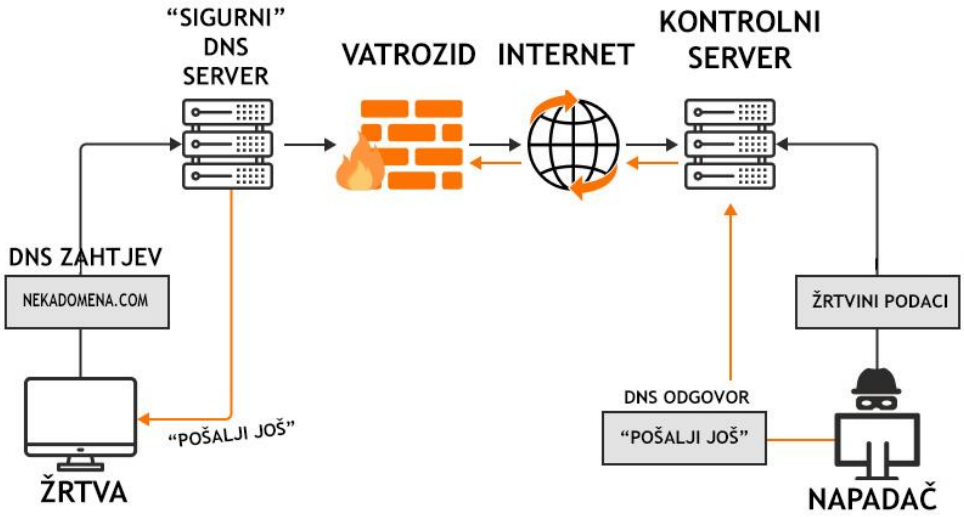
Zero-day napad predstavlja iskorištavanje nedostataka softvera pri čemu su nedostaci nepoznate proizvođačima i korisnicima te se tek trebaju otkriti i ispraviti sigurnosnim zakrpama. Također ova vrsta napada može se izvesti na uređajima koji nisu ažurirali najnovije zakrpe te na taj način nisu se osigurali i dovoljno zaštitili protiv napada. Kod ovog napada koristi se zlonamjerni softver „Mirai“ koji je snažan softver otvorenog koda koji usmjerivače, kamere i druge uređaje IoT sustava čini dijelom botneta koji je sposoban pokretati DDoS napade dosad nezamislivih veličina koji mogu načiniti dosad nezamislivu štetu.

Zaštita od ove vrste napada je moguća ažuriranjem svih kamera što prije je moguće, promjenom zadanih lozinki i onemogućavanjem nepotrebnih značajki i usluga. Također jedna od korisnih strategija je nadzor mrežnog prometa i anomalija koje se mogu pojaviti.

10.4. DNS tuneliranje

DNS tuneliranje je jedan od novijih napada koji postaju sve popularniji u napadu na IoT sustave. To je tehnika koje koristi DNS protokol koji je odgovoran za prevođenje naziva domena u IP adrese. DNS tuneliranje se može koristiti u razne svrhe, a trenutno najpopularnija je kontrola zlonamjernog softvera i zloupotreba u cilju pristupanja ograničenim resursima kao što je prikazano na slici 10.3.

Zaštita od ove vrste napada trenutno je moguća uz pomoć DNS vatrozida i DNS sigurnosne usluge koja može otkriti i blokirati zlonamjerni DNS promet. Zaštitu od ove vrste napada je moguće provesti koristeći VPN i provodeći šifriranje podataka pomoću jakih kriptografskih algoritama.



Slika 10.3. Ilustracija napada DNS tuneliranjem [48]

11. ZAKLJUČAK

Sustavi Interneta stvari su modernizirali i unaprijedili ljudski život i obavljanje raznih aktivnosti na način da su ih automatizirali, te omogućili daljinsko upravljanje i nadzor istih. IoT je tek u svom uzletu čiji se vrhunac može očekivati u budućnosti. Internet stvari ne bi mogao zaživjeti bez kriptografskih algoritama jer slabost IoT sustava je upravo izražena pri slanju podataka ka oblaku putem interneta. Bez korištenja kriptografije, informacije su izložene raznim vrstama napada, krađe, zloupotrebe. S druge strane kriptografski algoritmi su imali u počecima probleme raspolaganja s malom računalnom moći, ograničenom memorijom i drugim problemima u vidu ograničenih resursa. S razvojem hardvera tj. terminalnih uređaja, senzora i drugih uređaja koji se koriste u IoT sustavu, na istu veličinu čipa smješteno je puno više toga pa je na taj način omogućeno raspolaganje s više resursa. Što se tiče kriptografskih algoritama, oni se u začetku dijele na simetrične i asimetrične kriptografske algoritme. Ta podjela je napravljena prema samoj upotrebi ključa za šifriranje odnosno dešifriranje. Simetrični kriptografski algoritmi koriste jedan ključ za šifriranje i dešifriranje čime su manje zahtjevni, manje robusni, no i nesigurniji. Naime, ukoliko neovlaštena osoba sazna ključ, primijenjena kriptografija nema nikakvog smisla i sva zaštita pada u vodu. Zatim postoji asimetrični kriptografski algoritmi koji koriste dva različita ključa za šifriranje i dešifriranje. Naime šifriranje se obavlja javnim ključem te se šifrirani podaci šalju primatelju pri čemu primatelj podatke dešifrira privatnim ključem koji je poznat samo njemu. Kako nema slanja privatnog ključa, sigurnost je daleko veća, ali je veća i računalna zahtjevnost i robusnost. Za primjenu u industriji puno je lakše baratati i obrađivati podatke pri korištenju simetričnih algoritama jer se obavlja slanje jako velikog broja podataka što zahtjeva jako puno resursa i time čini cijenu sustava visokom. Zatim, ovisno o zahtjevima koje sustav ima te o razini sigurnosti koja se zahtjeva i resursima kojima se raspolaže, moguće je birati algoritme koji koriste različite veličine blokova. Optimalna veličina bloka je 64 bita dok postoje i veće. Osim veličine bloka presudna je i veličina ključa. Ukoliko se želi postići maksimalna sigurnost te se radi o prijenosu povjerljivih informacija, onda se koriste najduži mogući ključevi koje pojedini algoritam podržava. Što je ključ veći to je veća i sigurnost, ali se s druge strane utječe na robusnost, računalnu zahtjevnost, povećanje potrošnje resursa i smanjenje brzine. U kriptografiji moguće je još manipulirati i brojem rundi odnosno prolazaka. Što je broj rundi veći, veća je sigurnost, ali se također utječe na smanjenje brzine i potrošnju resursa. IoT se primjenjuje u raznolikim granama te prema tome se postavljaju i raznoliki zahtjevi pred kriptografske algoritme. Ovisno o sustavu, primjeni i zahtjevima, potrebno je odabrati i odgovarajući kriptografski algoritam. Ukoliko je potrebna zaštita razine 5 na skali od 1 do 10, a

odabere se podkapacitiran algoritam koji nema mogućnost zaštite na željenoj razini, sigurnost neće biti na željenoj razini te taj algoritam će možda odgovarati s brzinom i zahtjevnošću, ali zaštitom ne. Ukoliko se opet odabere kriptografski algoritam koji pruža daleko više od onoga što se zahtjeva, nepotrebno će se trošiti resursi i utjecati na opterećenost sustava i smanjenje brzine. Dakle, presudno je klasificirati zahtjeve, potrebe te resurse kojima se raspolaže i shodno njima odabrati odgovarajući kriptografski algoritam i konfiguraciju. Neki od najpopularnijih i najkorištenijih kriptografskih algoritama u IoT-u su: *Data Encryption Standard* (DES), *Triple-DES* (3DES), Kriptografija Eliptične Krivulje (ECC), *Advanced Encryption Standard* (AES), *Digital Signature Algorithm* (DSA), *Rivest-Shamir-Adleman* (RSA) algoritam, *Blowfish* algortiam i *Twofish* algoritam. Osim klasičnih algoritama, u IoT sustavu sve veću ulogu preuzimaju kriptografske sheme koj predstavljaju grupu više algoritama i protokola baziranih na lakim kriptografskih algoritmima zbog smanjenja potrebnih resursa, hardvera i cijene. Neki od najpopularnijih napada kojima su izloženi IoT sustavi i sami algoritmi su: *Spoofing* napad, Napad uskraćivanjem usluge (DoS), Napad distribuiranog uskraćivanja usluge (DDoS), Napad ponavljanjem, *Mass Node Autentification* napad, *Acknowledgement Flooding* napad, *Hello-flood* napad, *Man in the middle* napad (MitM), *Routing* napad, *Sybil* napad, *Phishing* napad, napad zatrpavanjem međuspremnika, Napad ubrizgavanjem zlonamjernog koda i mnogi drugi. IoT i sami kriptografski algoritmi u budućnosti će se upotrebljavati sve više te nije moguće precizirati njihov vrhunac, no jasno je da će ta branša samo rasti s razvojem tehnologije te zalaziti sve više u ona područja koja su zbog sigurnosnih rizika bila zatvorena prema IoT-u. U budućnosti pred kriptografske algoritme će se postavljati sve veći zahtjevi te će postojati potreba za sve većom sigurnosti što će potaknuti mnoge da se upuste u razvoj i istraživanje tog područja.

LITERATURA

[1] (n.d.). Preuzeto 1. 6 2024 iz Blowfish Algorithm with Examples: https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/

[2] (n.d.). Preuzeto 21. 5 2024 iz Twofish Encryption Algorithm: https://www.geeksforgeeks.org/twofish-encryption-algorithm/

[3] Wikipedia. (n.d.). Preuzeto 27. 5 2024 iz Low-power wide-area network: https://en.wikipedia.org/wiki/Low-power_wide-area_network

[4] Zubie. (n.d.). Preuzeto 23.6.2024 : https://zubie.com/zubie-fleet-connect/driver-performance/

[5] Abu-Tair, M. D. (2020). Towards secure and privacy-preserving IoT enabled smart home: architecture and experimental study.

[6] Ahmed, A. A. (2021). Lightweight digital certificate management and efficacious symmetric cryptographic mechanism over industrial internet of things.

[7] Alavi, A. H. (2018). Internet of things-enabled smart cities: State-of-the-art and future trends.

[8] B. Ali, A. I. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes.

[9] Bandyopadhyay, S. &. (2013). Lightweight internet protocols for web enablement of sensors using constrained gateway devices.

[10] Beović, I. (2023). Preuzeto 10. 4 2024 iz Kriptografija, kriptografski algoritmi i informacijska sigurnost: https://urn.nsk.hr/urn:nbn:hr:227:537376

[11] Ding, J. (n.d.). IoT connectivity technologies and applications.

[12] Diro, A. R. (2020). Lightweight authenticated-encryption scheme for internet of things based on publish-subscribe communication.

[13] Froehlich, A. (n.d.). Preuzeto 7. 5 2024 iz Elliptical curve cryptography (ECC): https://www.techtarget.com/searchsecurity/definition/elliptical-curve-cryptography

[14] Geeksforgeeks. (n.d.). Preuzeto 16. 5 2024 iz Digital Signature Algorithm (DSA): https://www.geeksforgeeks.org/digital-signature-algorithm-dsa/

[15] Golub, M. (n.d.). *Kriptografski blok simetrični algoritmi prilagođeni ugrađenim sustavima i Internetu stvari Tehnička dokumentacija Verzija 1.* Preuzeto 11. 5 2024 iz http://sigurnost.zemris.fer.hr/algoritmi/projekt_2018_19/media/download/Lightweight%20Block%20Ciphers%20-%20Tehnicka%20Dokumentacija.pdf

[16] Ha. Chen, M. H. (n.d.). Research on Industrial Internet of Things Security Architecture and Protection Strategy.

[17] Mishra, N. (n.d.). Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: a systematic review.

[18] Mocrii, D. (n.d.). IoT-based smart homes: a review of system architecture, software, communications, privacy and security.

[19] R. Awati, C. B. (n.d.). Preuzeto 1. 5 2024 iz Advanced Encryption Standard (AES): https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard

[20] R. Kumar, P. K. (n.d.). *A survey: review of cloud IoT security techniques, issues and challenges.*

[21] S. Duangphasuk, P. D. (2020). Review of Internet of Things (IoT): Security Issue and Solution.

[22] S. Kumar, S. S. (2022). Comparative Analysis of Security Techniques in Internet of Things.

[23] Simplilearn. (n.d.). *What Is DES (Data Encryption Standard)? DES Algorithm and Operation*. Dohvaćeno iz https://www.simplilearn.com/what-is-des-article
[24] Šekrst, A. (2018). *Kriptografski algoritmi*. Preuzeto 17. 4 2024 iz https://urn.nsk.hr/urn:nbn:hr:142:242657
[25] T. Mantoro, M. A. (2011). *Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts.*
[26] Thomas, M. (n.d.). *30 Internet of Things Examples You Should Know*. Preuzeto 2024. 5 21 iz https://builtin.com/articles/iot-examples
[27] Wikipedia. (n.d.). Preuzeto 2024. 5 14 iz RSA (cryptosystem): https://en.wikipedia.org/wiki/RSA_(cryptosystem)
[28] Tetcos (n.d.). Preuzeto 18. 8 2024 iz DIS Flooding attack in IoT networks running RPL: https://www.tetcos.com/pdf/v12.1/DIS_Flooding_Attack_IOT_RPL.pdf
[29] Matthew Sparkes (n.d.). Preuzeto 2024. 3 9 iz Google demonstrates vital step towards large-scale quantum computers: https://www.newscientist.com/article/2283945-google-demonstrates-vital-step-towards-large-scale-quantum-computers/
[30] Y. Harbi, Z. Aliouat, A. Refoufi, S. Harous (2021). Recent Security Trends in Internet of Things: A Comprehensive Survey
[31] M. N. Khan, A. Rao, S. Camtepe (2021). Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey
[32] Borhanuddin Mohd Ali (n.d.). Preuzeto 13. 9 2024. iz 6LoWPAN architecture: https://www.researchgate.net/figure/6LoWPAN-architecture_fig1_266064775
[33] (n.d.). Preuzeto 13. 9 2024. iz Spartan 7 Boards, Kits, and Modules: https://www.xilinx.com/products/boards-and-kits/device-family/nav-spartan-7.html
[34] (n.d.). Preuzeto 13. 9 2024. iz ARDUINO DUE ARM Cortex-M3 Board: https://www.tomsonelectronics.com/products/arduino-due-arm-cortex-m3-board?variant=37681687396547
[35] (n.d.). Preuzeto 13. 9 2024. iz ATmega328 8-Bit AVR MCUs - Microchip Technology: https://hr.mouser.com/new/microchip/atmelatmega328/
[36] (n.d.). Preuzeto 13. 9 2024. iz Smart home: https:// http://visioforce.com/smarthome.html
[37] (n.d.). Preuzeto 13. 9 2024. iz Deere launches See & Spray™ Ultimate: in-season targeted spray technology combined with a dual product solution system for corn, soybeans, and cotton: https://www.deere.com/en/news/all-news/see-spray-ultimate/
[38] (n.d.). Preuzeto 13. 9 2024. iz How is the Industrial IoT transforming industry?: https://www.themanufacturer.com/articles/how-is-the-industrial-iot-transforming-industry/
[39] (n.d.). Preuzeto 13. 9 2024. iz The Future of the Connected City: https://www.ft.com/reports/future-connected-city
[40] (n.d.). Preuzeto 13. 9 2024. iz Data Encryption Standard: https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm
[41] (n.d.). Preuzeto 13. 9 2024. iz Triple DES: https://www.tutorialspoint.com/cryptography/triple_des.html
[42] (n.d.). Preuzeto 13. 9 2024. iz Advanced Encryption Standard: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#/media/File:AES_(Rijndael)_Round_Function.png
[43] (n.d.). Preuzeto 13. 9 2024. iz Digital Signature Algorithm (DSA) in Cryptography: https://www.includehelp.com/cryptography/Images/dsa-1.jpg
[44] (n.d.). Preuzeto 13. 9 2024. iz Difference between RSA algorithm and DSA: https://www.geeksforgeeks.org/difference-between-rsa-algorithm-and-dsa/

[45] (n.d.). Preuzeto 13. 9 2024. iz Blowfish Algorithm with Examples: https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/
[46] Edith Ngai (n.d.). Preuzeto 13. 9 2024. iz Network flow in the attacked area: https://www.researchgate.net/figure/Network-flow-in-the-attacked-area_fig2_222815987
[47] (n.d.). Preuzeto 13. 9 2024. iz DIS flooding attack scenarios A The malicious node 9 targets nodes: https://www.researchgate.net/figure/DODAG-multicast-DIS-flooding-attack-scenarios-A-The-malicious-node-9-targets-nodes_fig2_336472255
[48] (n.d.). Preuzeto 13. 9 2024. iz DNS Tunneling Attack: https://cdn.prod.website-files.com/5ff66329429d880392f6cba2/644cd0fd955aee02ec7135fb_How%20Does%20DNS%20Tunneling%20Works.jpg
[49] (n.d.). Preuzeto 14. 9 2024. iz Symmetric vs. Asymmetric Encryption – What are differences?: https://www.ssl2buy.com/wp-content/uploads/2015/12/Symmetric-Encryption.png
[50] (n.d.). Preuzeto 14. 9 2024. iz Symmetric vs. Asymmetric Encryption – What are differences?: https://www.ssl2buy.com/wp-content/uploads/2015/12/Asymmetric-Encryption.png
[51] (n.d.). Preuzeto 14. 9 2024. iz Hybrid Cryptography: https://www.researchgate.net/publication/363656300/figure/fig1/AS:1143128109928433 7@1669243394863/Hybrid-Cryptography-Model.png

SAŽETAK

Naslov: Kriptografski algoritmi za okruženje Interneta stvari

U ovom radu izvršeni su pregled i analiza kriptografskih algoritama namijenjenih za primjenu u okruženju Interneta stvari. Proveden je cjelovit pregled područja Interneta stvari odnosno pruženi su odgovori na pitanje što je to IoT, što sve obuhvaća, kako funkcionira i koju perspektivu ima u budućnosti. Upotreba IoT-a u današnjem vremenu je nemoguća bez kriptografskih algoritama, a povećanje upotrebe i popularizacija IoT-a iz dana u dan zahtjeva sve bolje i sigurnije algoritme i načine kriptiranja kako bi integritet i sigurnost podataka ostali očuvani, što je glavni preduvjet za rast i prodiranje u nova područja primjene. Pred kriptografske algoritme se postavljaju sve veći zahtjevi, te postoje sve veće potrebe za istraživanjem i razvojem još sigurnijih i boljih kriptografskih algoritama.

Ključne riječi: kriptografija, kriptografski algoritmi, Internet stvari, IoT, pametna kuća, pametni gradovi, industrijski Internet stvari, laki kriptografski algoritmi

ABSTRACT

Title: Cryptographic algorithms for the Internet of Things enviroment

In this paper, an overview and analysis of cryptographic algorithms intended for application in the Internet of Things (IoT) environment is provided. A comprehensive overview of the Internet of Things domain is presented, answering questions about what IoT is, what it encompasses, how it functions, and its future prospects. The use of IoT in today's world is inseparable from cryptographic algorithms. The increasing use and growing popularity of IoT require more robust and secure algorithms and encryption methods to preserve integrity and security, which are essential for growth and expansion into new areas of application. As a result, cryptographic algorithms face increasing demands, creating a growing need for the research and development of even safer and more advanced cryptographic solutions.

Keywords: cryptography, cryptographic algorithms, Internet of Things, IoT, smart home, smart city, industrial Internet of Things, lightweight cryptographic algorithms

ŽIVOTOPIS

Ante Vlahović, rođen u Slavonskom Brodu 14.06.2000. Osnovnu školu završio u Slavonskom Brodu 2015. godine. Nakon osnovne škole upisuje Tehničku školu u Slavonskom Brodu. Nakon završene srednje Tehničke škole stječe zanimanje elektrotehničar i upisuje preddiplomski sveučilišni studij Elektrotehnike na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija u Osijeku. U rujnu 2022. godine završava preddiplomski studij i upisuje diplomski studij na istom fakultetu.