UNIVERZITET CRNE GORE

Prirodno-matematički fakultet Podgorica

Danijela Damjanović

Kriptografski algoritmi za zaštitu mobilne komunikacije

SPECIJALISTIČKI RAD

Podgorica, 2017.

UNIVERZITET CRNE GORE

Prirodno-matematički fakultet Podgorica

Kriptografski algoritmi za zaštitu mobilne komunikacije

SPECIJALISTIČKI RAD

Kriptografija

Mentor: Vladimir Božović

Danijela Damjanović

Matematika i računarske nauke

Podgorica, Decembar 2017.

Apstrakt

Komunikacije preko mobilnih uređaja su neophodne, ali je njihovo korišćenje ograničeno zbog prisustva napada na komunikaciju. Autentifikacija i šifrovanje podataka su tehnike za zaštitu od takvih prijetnji. Ovaj rad ukratko opisuje najvažnije tehnike za zaštitu GSM i UMTS sistema kao i njihove nedostatke uslijed brzog razvoja tehnologija.

Abstract

Communications through mobile devices are necessary, but use of these is restricted due to the presence of attacks on communications. The encrypted authentication and data encryption are techniques to protect against such threats. This paper briefly describes the most important techniques for protecting the GSM and UMTS systems as well as their shortcomings due to the rapid development of technology.

Sadržaj

Glava 1

Uvod

Mobilna komunikacija je najbrže rastuća industrija danas, procjenjuje se da će do 2019. godine broj korisika premašiti 5 biliona. Pretplatnici mogu, ne samo da razgovaraju preko svojih mobilnih uređaja, već da imaju pristup mnogim drugim uslugama kao što su onlajn bankarstvo, prenos podataka itd. Sve veći napredak u bežičnim tehnologijama i rastuća potražnja rezultiraju i većim sigurnosnim rizicima i prijetnjama od zlonamjernih napadača. Jasno je da se veća pažnja mora posvetiti sigurnosti informacionih sistema, zaštiti podataka od neovlašćenog pristupa, modifikacija ili drugih zloupotreba, i da je neophodno stvoriti određene mehanizme koji će mobilnu mrežu učiniti sigurnom.

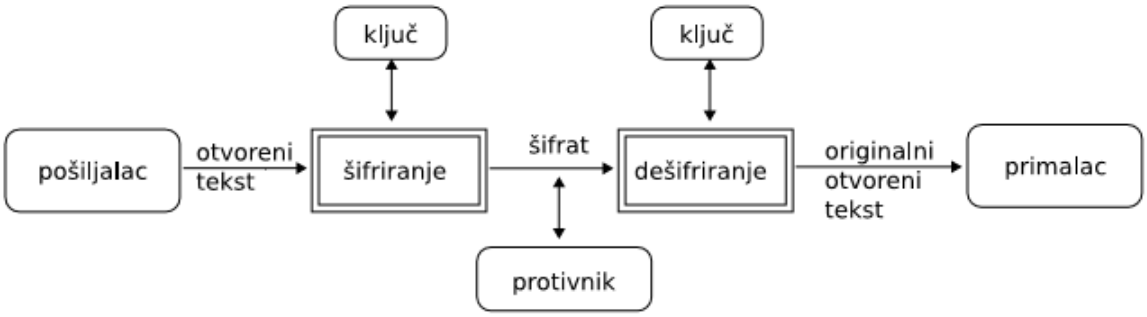
Pojavom druge generacije, GSM mreže, javlja se potreba za razvojem kriptografskih algoritama koji omogućavaju šifrovanje podataka koji se šalju putem mreže.

1.1 Osnovni pojmovi kriptografije

Kako uspostaviti sigurnu komunikaciju preko nesigurnog komunikacijskog kanala? Metode za rješavanje ovog problema proučava naučna disciplina koja se zove kriptografija (engl. *cryptography*). Osnovni zadatak kriptografije je omogućavanje komunikacije dvaju osoba (zovemo ih *pošiljalac* i *primalac* na takav način da treća osoba (njihov *protivnik*), koja može nadzirati komunikacijski kanal, ne može razumjeti njihove poruke.

Poruku koju pošiljalac želi poslati primaocu zovemo *otvoreni tekst* (engl. *plaintext*). Pošiljalac transformiše otvoreni tekst koristeći unaprijed dogovoreni ključ K. Taj se postupak zove *šifrovanje*, a dobijeni rezultat *šifrat* (engl. *ciphertext*). Nakon toga pošiljalac pošalje šifrat preko nekog komunikacijskog kanala. Protivnik prisluškujući može saznati sadržaj šifrata, ali kako ne zna ključ, ne može odrediti otvoreni tekst. Za razliku od njega, primalac zna ključ kojim je šifrirana poruka, pa može dešifrovati šifrat i odrediti otvoreni tekst.

Slika 1.1: Shema simetrične kriptografije



Proces transformacije otvorenog teksta u šifrat, koji za cilj ima prikrivanje smisla njegovog sadržaja se naziva šifrovanje (engl. *encryption*). Dešifrovanje (engl. *decryption*) je inverzna tranformacija, tj. proces vraćanja šifrata u otvoreni tekst. [1]

Kriptografija mora da obezbijedi:

Integritet informacija: Podaci koji se šifruju ne smiju biti promijenjeni, brisani ili zamijenjeni drugim informacijama.

Tajnost informacija: Sadržaj informacija je dostupan samo ovlašćenim osobama, odnosno osobama koje posjeduju ključ.

Provjera identiteta: Osobe koje komuniciraju prvo moraju da se predstave jedna drugoj, nakon čega počinju razmjenu informacija.

Kriptografski algoritam ili šifra (engl. *cipher*) je matematička funkcija koja se koristi za šifrovanje i dešifrovanje. Postoji nekoliko podjela šifri: prema alfabetu šifrata, prema ključu, tj. algoritmima šifrovanja i dešifrovanja, prema tipu operacija pri šifrovanju, prema načinu na koji se obrađuje otvoreni tekst. [2]

Nama je od značaja poznavanje šifri prema načinu na koji se obrađuje otvoreni tekst i to protočna šifra. Protočna šifra transformiše otvoreni tekst simbol po simbol, odnosno kombinovanjem simbol po simbol sa nizom ključa, koji se dobija iz kriptografskog generatora pseudoslučajnih brojeva.

1.2 Princip uspostavljanja i zaštite komunikacije između korisnika

Prenos podataka u bežičnim mobilnim komunikacijama odvija se putem vazduha, te svako može da ih prisluškuje. Mobilne mreže nastoje putem utvrđenih algoritama zaštititi pravo pretplatnika na privatnost i sigurnu razmjenu informacija.

Princip uspostavljanja i zaštite komunikacije odvija se u nekoliko koraka:

- Korisnik A želi da obavi poziv sa korisnikom B. Da bi se uspostavio poziv, korisnici se prvo moraju autentifikovati mreži kako bi potvrdili svoj identitet. Na SIM kartici korisnika i na baznoj stanici implementiran je algoritam A3 koji omogućava autentifikaciju. Ključ K_i, koji predstavlja glavni ulazni parametar algoritma, bezbjedno je uskladišten na SIM kartici i nije poznat ni mobilnom uređaju. Isti takav ključ dostavlja se baznoj stanici iz glavne baze podataka svih pretplatnika. Ukoliko se izlazne vrijednosti algoritama poklapaju proces autentifikacije je završen i uspostavlja se veza.

- Analogni, glasovni podatak korisnika A se unutar samog uređaja transformiše u digitalni. Niz bitova se enkriptuje pomoću algoritma A5, implementiranog u mobilnom uređaju, koji koristi ključ K_c generisan na osnovu ključa K_i iz SIM kartice. Ključevi korisnika A i B dostavljaju se baznoj stanici iz centralnog registra pretplatnika. Po prijemu enkriptovanih podataka korisnika A, bazna stanica ih dekriptuje pomoću ključa za enkripciju/dekripciju korisnika A. Zatim otvoreni tekst enkriptuje pomoću ključa korisnika B i tako šifrovane podatke šalje korisniku B. Po prijemu, u samom mobilnom uređaju korisnika B vrši se dekripcija i pretvaranje digitalnih u analogne podatke.

U mobilnim mrežama novijih generacija nema bitnijih izmjena u principu uspostave poziva osim uvođenja dvosmjerne autentifikacije kako bi se i mreža autentifikovala korisniku. Razvojna moć računara se iz godine u godinu udvostručava te su nedostaci implementiranih sistema postali vidljivi i na meti mnogobrojnih napadača. Unaprijeđeni sistemi rješavaju neke od ovih problema uvođenjem novih algoritama, što će biti opisano u daljem tekstu rada.

Glava 2

GSM mreža

CEPT (engl. *European Conference of Postal and Telecommunications Administrations*, 1988. godine osniva ETSI, nezavisnu organizaciju za standardizaciju u oblasti telekomunikacija. ETSI je bio zadužen za razvoj i proizvodnju globalno primjenljivih standarda za informacione i komunikacione tehnologije, uključujući fiksne, mobilne, radio i internet tehnologije. GSM predstavlja jedan od standarda razvijen od strane ETSI koji opisuje protokole mobilne mreže druge generacije koju koriste mobilni telefoni.

Prethodni mobilni sistemi nisu imali nikakav vid zaštite, te su predstavljali predmet kriminalnih radnji, GSM je prvi mobilni sistem koji je razmatrao prijetnje po pitanju bezbjednosti sistema. Primjer je uvođenje hardverske komponente u telefonu, SIM (engl. *Subscriber Identity Module*) kartica, koja je predstavljala dodatnu zaštitu, jer je korisnik prije uspostavljanja veze morao da odradi proces prijavljivanja na mrežu. Cilj je bio i obezbijediti privatnost korisnika, što je u osnovi obezbijeđeno uglavnom šifrovanjem.

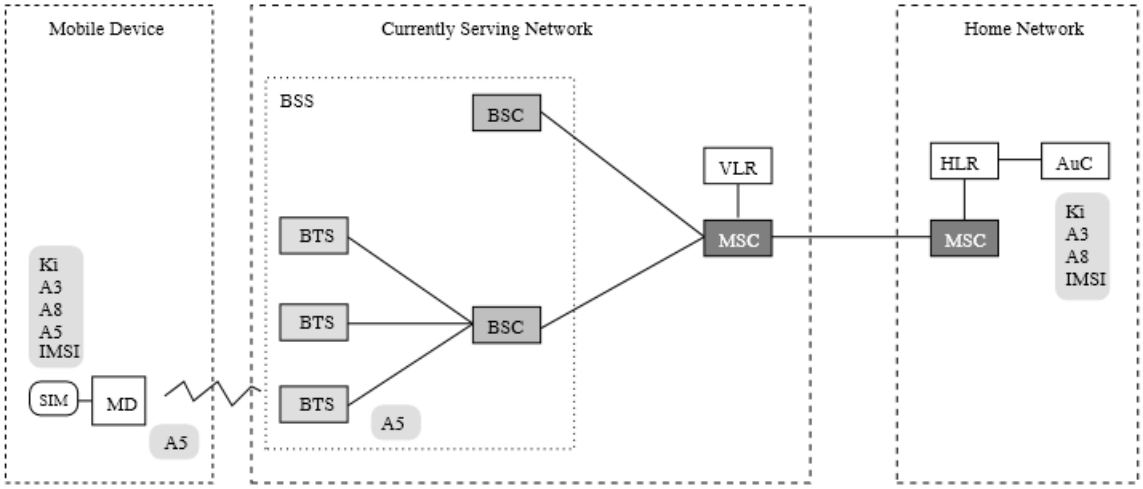
2.1 Sigurnost i privatnost u okviru GSM mreže

Sigurnost i privatnost podataka su od velikog značaja, posebno u komunikacijskim sistemima gdje se podaci prenose putem radio talasa. Ovakva vrsta prenosa podataka otvara vrata neželjinim upadima i prisluškivanjima na mreži.

Sigurnosni elemenati GSM mreže podijeljeni su na tri komponente sistema:

- SIM kartice
- Mobilne stanice
- GSM mreže

Slika 2.1: Struktura GSM mreže



U GSM mreži sigurnosni podaci se dijele između autentifikacionog centra (AUC), HLR (engl. *home location register*) registra i VLR (engl. *visitor location register*) registra. HLR registar predstavlja centralnu bazu podataka koja sadrži detalje o svakom pretplatniku mobilnog telefona koji je autorizovan za korišćenje GSM mreže.

VLR registar predstavlja bazu podataka pretplatnika koji se trenutno nalaze u geografskoj oblasti koju kontroliše MSC. MSC je čvor GSM mreže odgovoran za usmjeravanje glasovnih poziva, SMS poruka i ostalih usluga. AUC je odgovoran za stvaranje brojeva potrebnih kod autentifikacije i u postupku kriptovanja koji se spremaju u HLR i VLR.

Širok opseg napada čini mobilne komunikacije osjetljivim na prisluškivanje, krađu identiteta i mijenjanje sadržaja poruka. Uopšteno, svi napadi zasnivaju se na slabostima fizičke zaštitite mobilnog uređaja i end-to-end šifrovanja, gdje je poziv šifrovan od strane pozivaoca a koje može dešifrovati samo primalac. Kako bi zaštitili korisnike od neželjenih napada u GSM mreži je ugrađeno nekoliko fukcija koje osiguravaju privatnost korisnika. Pored sigurno skladištenog ključa K_i, vrši se autentifikacija korisnika i sigurnost prenosa podataka se obezbjeđuje šifrovanjem.

Najvažnije bezbjednosne funkcije, koje su predstavljene u ovom radu, su sigurnost podataka šifrovanjem i autentifikacija. Sa razvitkom digitalne komunikacije, javlja se potreba za korišćenjem kriptografskih algoritama koji direktno mogu da šifruju i dešifruju digitalni tok podataka. Takvi algoritmi su implementirani u odvojene hardverske komponente. GSM mreža koristi kriptografske algoritme u tri svrhe:

- Algoritam A3 - Autentifikacija
- Algoritam A8 - Generisanje ključa
- Algoritam A5 - Šifrovanje podataka

2.1.1 Autentifikacija GSM i UMTS mreže

Autentifikacija predstavlja proces utvrđivanja identiteta korisnika ili mobilne mreže, odnosno proces u okviru kog korisnik ili mobilna mreža dokazuju da su onaj za koga se

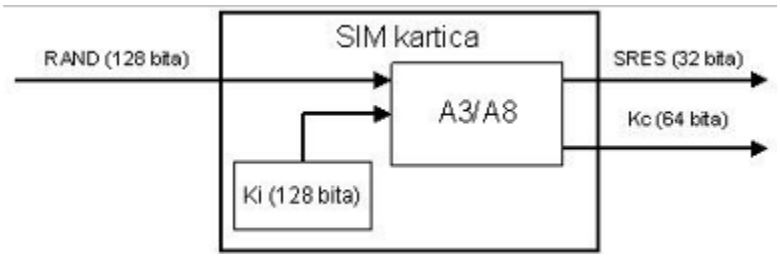
izdaju. Bitna je da bi se utvrdilo koji korisnik ima dozvolu za korišćenje mrežnih servisa. Ukoliko autentifikacija ne bi postojala, bilo koji korisnik bi mogao neovlašćeno koristiti korisnički račun bilo kog ovlašćenog korisnika i na taj način ga materijalno oštetiti. [3]

Autentif ikacija se mora vršiti na poseban način jer je medijum za prenos podataka vazduh, pa se pretpostavlja da bilo ko može da prisluškuje komunikaciju.

Postupak autentifikacije u GSM mrežama provjerava ispravnost SIM kartice pretplatnika, a zatim se odlučuje da li je mobilnoj stanici dozvoljen pristup mreži. Sve potrebne operacije tokom autentifikacije se odvijaju unutar SIM kartice, čime se postiže veći stepen sigurnosti. SIM kartica sadrži sve podatke potrebne za uspostavljanje pristupa određenom pretplatničkom računu. Potrebne su 2 informacije:

- IMSI - jedinstveni broj dodijeljen svakom korisniku mobilnog uređaja
- K_i - predstavlja početni ključ za generisanje svih ostalih ključeva i provjera tokom GSM komunikacije. Ključ K_i je visoko zaštićen i poznat je samo SIM kartici i mrežnom autentikacijskom centru (AUC).

Slika 2.2: Koncept autetifikacije na SIM kartici



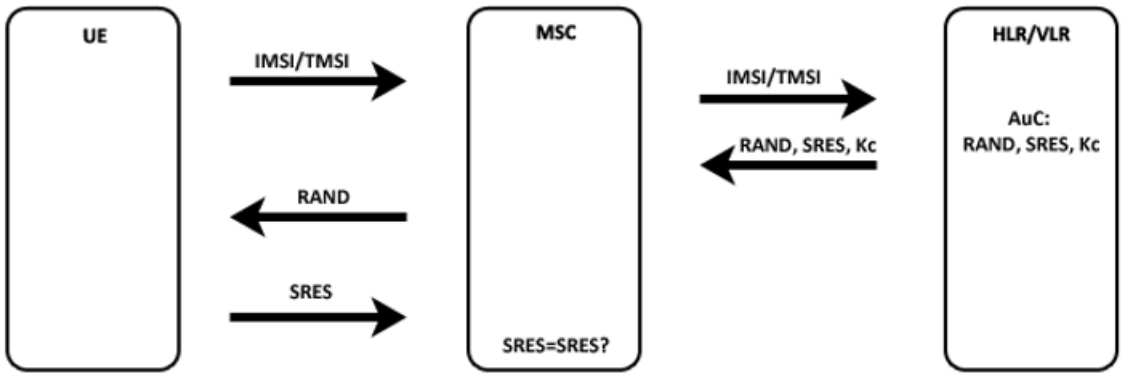
Najjednostavniji način autentifikacije bio bi slanje ključa K_i mobilnoj mreži kad ga mobilna mreža zatraži, što bi bilo nesigurno, jer bi ključ u tom slučaju bio ranjiv na

presretanje a samim tim i na otkrivanje. Da bi potvrdila vjerodostojnost pretplatnika mreža koristi metod izazov-odgovor (engl. *challenge-response method*).

Kako bi uspostavio poziv korisnik šalje baznoj stanici zahtjev za dobijanje kanala (engl. *channel request*) i kao odgovor dobija redni broj TDMA okvira i detalje kanala koji su dodijeljeni mobilnom telefonu. MS se podešava na dodijeljeni kanal i šalje svoj IMSI, i zahtjev za uslugu. Bazna stanica kao odgovor šalje RAND vrijednost i istovremeno podatke o pretplatniku šalje AUC-u. Na SIM kartici, kao i autentifikacijskom centru se realizuje A3 algoritam sa ulaznim parametrima K_i i RAND.

Dobijeni podaci se prosleđuju do MSC-a koji ukoliko se vrijednosti poklapaju signalizira da je autentifikacija uspješno završena. Sigurnosni model pruža povjerljivost i autentikaciju, ali ima ograničene mogućnosti autorizacije.

Slika 2.3: Proces autentifikacije u GSM mreži



Razvoj UMTS-a uvodi neobavezno modul USIM (eng. *Universal Subscriber Identity Module*) koji koristi duži autentikacijski ključ u svrhu pružanja bolje sigurnosti, kao i međusobnog autentifikovanja mreže i korisnika.

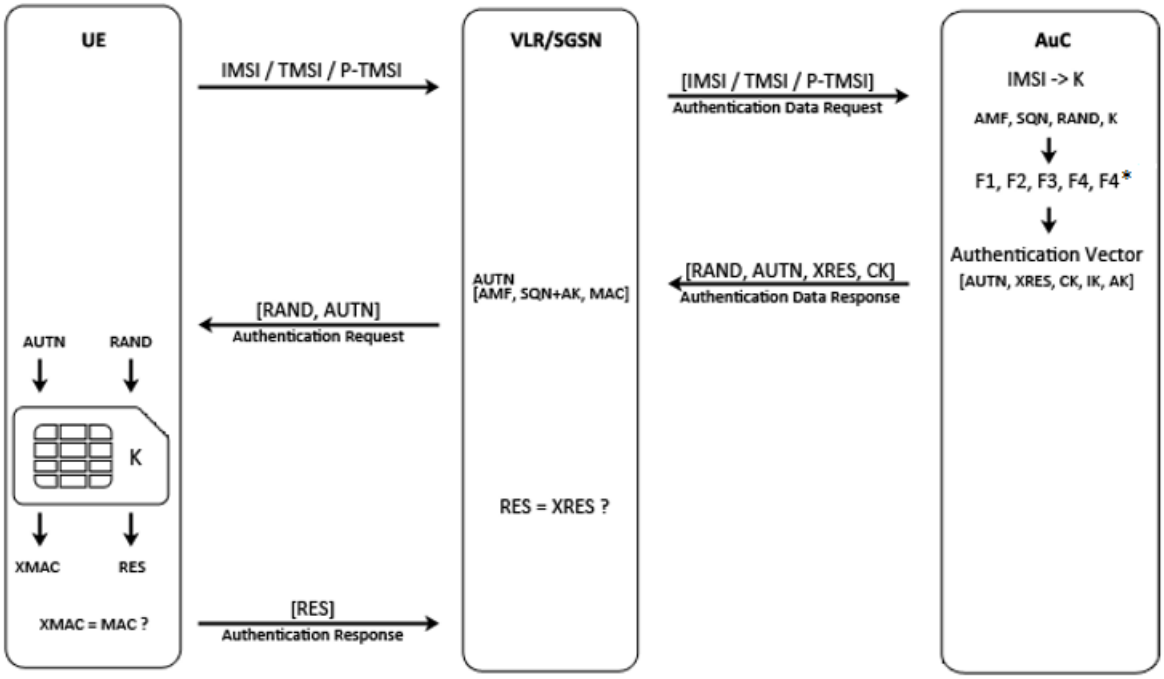
Principi autentifikacije kod GSM i UMTS mreža se bitno razlikuju. Prije svega zbog obostrane autentifikacije mreže i korisnika kod UMTS sistema i zbog korišćenja

dodatnih algoritama zaštite.

Jedan od bitnijih principa mreža treće generacije je dvosmjerna autentifikacija koja povećava u velikoj mjeri bezbjednost mobilne mreže. I u UMTS mobilnim mrežama autentifikacija počinje isto kao u GSM mrežama. Bitna razlika je uvođenje vektora autentifikacije (AV) koji je dio mehanizma UMTS mreža koji služi za obostranu autentifikaciju korisnika i mreže.

Za generisanje parametara AV se koriste jednosmjerne funkcije. Jednosmjerne funkcije su funkcije koje za neki ulazni parameter daju izlazni, ali se na osnovu izlaznog parametra ne možkoristi se pet jednosmjernih funkcija: F1 za generisanje MAC vrijednosti, F2 za generisanje XRES vrijednosti, F3 za generisanje C_k ključa, F4, za generisanje I_k ključa, F5 za generisanje Ak (engl. *Anonymous Key*) ključa. Proces autentifikacije prikazan je na Slici 2.4.

Slika 2.4: Proces autentifikacije u UMTS mreži



Ovo prije svega onemogućava da se napadač predstavi kao bazna stanica i dodatno štiti korisnika od krađe identiteta, za razliku od GSM jednosmjerne autentifikacije.

2.2 A3/A8 algoritam

Uloga ovih algoritama je da na osnovu RAND vrijednosti i ključa K_i generišu SRES vrijednost (A3) koja se koristi za autentifikaciju i ključ Kc (A8), koji se koristi za šifrovanje komunikacije ukoliko je autentifikacija uspješna.

Algoritam za šifrovanje koji oni koriste je najčešće COMP128, pa su nedostaci A3/A8 algoritama zapravo nedostaci COMP128 algoritma. Nedostaci su ograničen broj vrijednosti koje se koriste za RAND i namjerna oslabljenost algoritma pri generisanju Kc ključa, koji umesto 64 bita zapravo ima 54 bita i 10 dodatnih bitova čija je vrijednost 0. Time se složenost ključa smanjuje za 1024 puta.

Sigurnost se bazira na pretpostavci o tajnosti algoritma što je velika mana. Princip rada nikada nije javno objavljen ali specifikacije su dospjele u javnost. Te je ovaj algoritam razbijen od strane Vagnera i Goldberga. Danas se koriste COMP128-3 i COMP128-4, koji nemaju pomenutih 10 praznih bitova u Kc, ali i dalje većina SIM kartica koristi izvorni COMP128. Razbijanjem ovog algoritma, Vagner i Goldberg dobili su vrijednost ključa K_i, čime su dokazali da mobilna komunikacija ipak nije dovoljno sigurna, te da je moguće klonirati SIM kartice. Za detaljnije opise algoritama pogledati [4].

2.2.1 Šifrovanje podataka - Algoritam A5

Mobilne komunikacije koriste simetrične algoritme za kriptovanje podataka, tj. algoritme koji za šifrovanje i dešifrovanje podataka koriste isti ključ. Glavni problem kod simetrične kriptografije je kako da se primalac i pošiljalac dogovore koji će ključ

koristiti bez straha od prisluškivanja. Međutim, prednost simetrične kriptografije je što je u većini slučajeva brža od asimetrične kriptografije.

Kako bi se zaštitili podaci koji se bežičnim putem šalju preko mreže, GSM šifruje podatke koristeći protočnu šifru poznatiju kao A5, tj. algoritam za šifrovanje podataka.

Nakon autentifikacije korisnika, i mreže u unaprijeđenim sistemima, mreža zahtijeva od korisnika da započne proces šifrovanja. U mobilnim komunikacijama šifrovanje podataka se odvija između mobilnih uređaja i bazne stanice.

Mobilni uredjaj (MS) generiše ključ K_c (engl. *session key*) koristeći A8 algoritam, implementiran na SIM kartici, sa ulaznim parametrima RAND i K_i. Na osnovu ključa K_c i poruke, na mobilnom uređaju se vrši šifrovanje date poruke pomoću algoritma A5. Dodatni faktor sigurnosti je mogućnost promjene ključa za šifrovanje koji se može takođe mijenjati u vremenskim intervalima. Tako šifrovani podaci se šalju baznoj stanici.

S druge strane, na osnovu informacija iz procesa autentifikacije, MSC presljeđuje baznoj stanici ključ K_c generisan algoritmom A8 u AUC-u. U baznoj stanici, na osnovu ključa K_c i šifrovanog teksta vrši se algoritmom A5 dekripcija. Bazna stanica istovremeno od MSC-a prima podatke i o primaocu, drugom mobilnom uređaju, i na osnovu njegovog ključa šifruje podatke i šalje mu ih bežičnom radio vezom. Primalac šifrovanje podatke dešifruje pomoću algoritma A5 i svog ključa za šifrovanje. A5 je implementiran u mobilnom telefonu, kako bi mogao da šifruje podatke neposredno pred prenos.

Postoje četiri različite varijante A5 algoritma:

- A5/0 algoritam koji ne šifruje podatke. Uglavnom se koristio u zemljama pod sankcijom Ujedinjenih Nacija i pojedinim zemljama trećeg svijeta.

- A5/1 je najjača verzija algoritma. Specificiran je sredinom 80-tih nakon rasprave o jačini algoritma koja se vodila između nekoliko članica NATO-a. Algoritam se koristio pretežno u Zapadnoj Evropi i Americi.

- A5/2 predstavlja oslabljenu verziju algoritma A5/1. Uglavnom se koristila u zemljama Azije.

- A5/3 je kasnije napravljen za korišćenje u 3G mreži i predstavlja novi algoritam zasnovan na blokovskoj šifri KASUMI. [5]

2.2.2 Algoritam A5/2

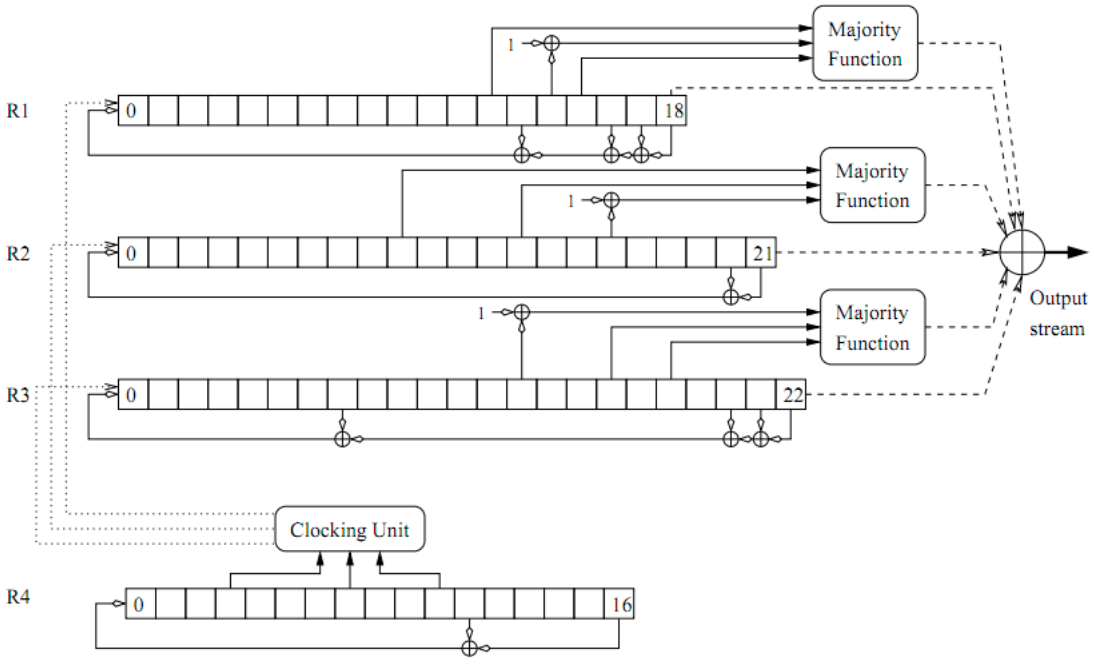
A5/2 predstavlja slabiju verziju algoritma A5/1. Razvijen je 1999. godine u skladu sa ograničenjima politike izvoza, izvan Evropske Unije jer u to vrijeme nije bio dozvoljen izvoz jakih šifara.

Šifrovanje radi po principu generisanja binarnih šifarskih blokova (maski) od strane A5 algoritma, koji se XOR funkcijom kombinuju sa podacima koji se prenose, što ovaj algoritam čini sekvencijalnim algoritmom. Na prijemu se nad kriptovanim podacima još jednom primenjuje XOR funkcija sa istim binarnim šifarskim blokovima koji su korišćeni pri kriptovanju i time se dobija početna informacija.

A5/2 je baziran na LFSR (engl. *Linear Feedback Shift Register*) blokovima nejednake dužine redom, 19, 22, 23 i 17 bita, čiji se izlazi sabiraju i daju izlazni rezultat. Istovremeno, određeni bitovi LFSR blokova se sabiraju i daju novi ulaz LFSR blokova.

Za stvaranje binarnih šifarskih blokova A5/2 algoritam koristi Kc ključ za šifrovanje. Kako bi sekvencijalni algoritam bio sigurniji, trebalo bi pored ključa za šifrovanje koristiti i dodatne vrednosti za generisanje binarnih šifarskih blokova (maski), tako da maska svaki put bude drugačija. Time bi se izbegao napad kriptoanalizom poređenjem više poruka šifrovanih istom maskom. A5/2 u tu svrhu koristi bitove LFSR

Slika 2.5: Struktura A5/2 algoritma



polja za kontrolu taktovanja.

Dok A5/1 algoritam koristi dodatnu promjenjivu COUNT. Vrijednost COUNT se zasniva na TDMA broju okvira, koji se sekvencijalno dodaju svakom GSM okviru (GSM okvir se generiše svakih 4.615ms). Tako će maska svaki put biti drugačija.

Na kraju svakog ciklusa je proizveden jedan izlazni bit. Jedinica za taktovanje (*Clocking Unit* registra izračunava većinsku funkciju nad bitovima, gdje se na osnovu izlaza te funkcije određuje koji registar će biti taktovan. Izlaz većinske funkcije se računa funkcijom *majority*, gdje su argumenti: tri bita registra određni svojim pozicijama, od kojih se vrijednost jednog bita komplementira. Funkcija je kvadratna i zapisuje se:

$$majority(a, b, c) = a \cdot b \oplus b \cdot c \oplus c \cdot a.$$

Prvih 99 bitova izlaza se odbacuju, što znači da se registri samo taktuju po prethodno definisanom pravilu, a sledećih 228 bitova izlaza se uzimaju kao izlazni niz ključa (engl. *keystream*).

Izlaz od 228 bita dijeli se na dva dijela. Prva polovina od 114 bita se koristi kao niz ključa za šifrovanje podataka na vezi od mreže ka telefonu, a druga polovina od 114 bita za šifrovanje podataka na vezi od telefona ka mreži. Šifrovanje se vrši bitskom operacijom XOR poruke podijeljene u okvire dužine 114 bita i niza ključa. [2]

2.3 Napadi na GSM mrežu

Cilj napada nije nužno dekriptovanje samo jedne šifrovane poruke, već sticanje informacija o ključu koji se koristi u datom sistemu, pri čemu se na taj način kompromituje prošla, a vjerovatno i buduća komunikacija. Neke od mana koje napadač može da iskoristi prilikom napada su:

- Mreža bira algoritam za šifrovanje. Telefon samo pruža spisak šifri koje podržava u okviru poruke koja se naziva *class-mark*. Moguće je da mreža ne koristi nijedan algoritam za šifrovanje.
- *Class-mark* poruka nije zaštićena, te napadač može da je promijeni.
- Lažne bazne stanice - Tokom autentifikacije samo telefon je autentifikovan od strane mreže, dok obrnuti mehanizam ne postoji.
- Ključ je uvijek isti i on zavisi samo od RAND, koji se bira od strane mreže, bez obzira koji algoritam (A5/1, A5/2, A5/3) se koristi za šifrovanje.
- Isti RAND je moguće koristiti više puta.

Najveći nedostatak u implementaciji GSM sistema je korišćenje jednosmjerne autentifikacije pri kojoj se mobilna mreža ne autentifikuje korisniku. To omogućava napadaču da postavi lažnu baznu stanicu sa identičnim kodom mobilne pretplatničke mreže. Pretplatnik bi tada bez znanja mogao obavljati razgovore i slati poruke preko te lažne bazne stanice omogućavajući napadaču da ih presrijeće, tkz. *man-in-the-middle*) napad.

Napadač može lako koristiti i nedostatke algoritama za šifrovanje podataka. A5/1 algoritam je baziran na moduo 2 sabiranjem 3 LFSR registra čiji se sinhronizacijski ulazi kontrolišu većinskom funkcijom određenih bita u samim LFSR-ima. Alex Biryukov, Adi Shamir i David Wagner su dokazali da se algoritam A5/1 može razbiti u samo jednoj sekundi koristeći PC i određene prije izračunate tablice. Napad iskorištava propust algoritma u trenutku spremanja tih tablica spajajući znanje od statističke analize koraka i iskorištavanja slabe 1-bitne kontrole sinhronizacije LFSR-a. A5/2 je namjerno oslabljen algoritam što ga čini još ranjivijim. U daljem tekstu je objašnjen napad koji se zasniva na manama protokola u komunikaciji između telefona i mreže.

Takođe, tajno prisluškivanje omogućuje jedan drugi propust u GSM sistemu i malo politike. Naime, zakoni o komunikacijama nisu u svim zemljama jednaki. U mnogim zemljama Istočne Evrope i Bliskog Istoka, na zahtjev tajnih službi, nije dozvoljena upotreba jakog A5/1 algoritma, nego slabijeg A5/2, što predstavlja mnogo manje tehničkih i vremenskih zahtjeva za njihovo razbijanje. U nekim zemljama nije dozvoljen uvoz nikakve kriptografske opreme, pa su samim time i komunikacije potpuno nezaštićene. Treba napraviti baznu stanicu, koja bi mobilnom telefonu poslala informaciju da je u Iraku, čime bi on automatski isključio kripto-zaštitu te omogućio prisluškivanje. Projektanti nisu na vrijeme predviđali tu mogunost, te mogućnost prepravke bi na sistemu širom svijeta koštale milione dolara.

2.3.1 Napad na A5/2 sa poznavanjem samo šifrata

Napad sa poznavanjem samo šifrata predložili su i implementirali Barkan, Biham i Keller. Fokus u ovom napadu je na kanalu SACCH (engl. *Slow Associated Control CHannel*). U sistemima poput GSM-a, gdje se podaci prenose radio talasima, pojava greške je uobičajena, što ukazuje na potrebu korekcije greške.

Tokom komunikacije, poruka se prvo podvrgne kodiranju za ispravljanje greške, što dovodi do znatnog povećanja dužine poruke. U kanalu SACCH, poruka koju je potrebno kodirati je fiksne dužine od 184 bita. Nakon što se izvrši korekcija greške, poruka je dužine 456 bita, čiji su biti ispremještani i podijeljeni u četiri dijela. Ova poruka se šifruje i šalje dalje. Obično, u nekim sigurnijim sistemima, prvo se radi šifrovanje poruke, što znači da se svaki bit od 184 bita poruke prvo šifruje, pa se onda radi dodavanje redudantnih bitova informacija, sa kojim originalna poruka predstavlja poruku dužine 456 bita. Na osnovu redudantnih bitova moguće je postaviti napad. Inicijalna unutrašnja stanja registara tretiraju se kao varijable i svaki bit šifrata je napisan kao kvadratna funkcija tih varijabli. Potrebno je napraviti sistem linearno nezavisnih jednačina. Potrebne su barem dvije poruke dužine 456 bita, kako bi se dobilo 450 jednačina za rješavanje. Nakon što se riješi sistem Gausovim sistemom eliminacije za odgovorajuće $R4_1$, traži se K_c pokretanjem algoritma za određivanje ključa. Za detaljniji opis napada pogledati [8].

Glava 3

Kriptografski algoritmi za UMTS/LTE mreže

3GPP je dizajnirao UMTS sistem kako bi riješio neke od sigurnosnih problema originalnog GSM. UMTS je koristio GSM sistem kao osnovu za izgradnju kako bi se omogućila lakša migracija mreža i obezbijedila kompatibilnost unazad.

Naprednije generacije mobilnih mreža nude korisnicima širok spektar usluga, bežični pristup internetu i svjetski rasprostranjen roming. Međutim, ovo uključuje ozbiljne bezbjednosne ranjivosti što dodatno otežava uspostavljanje sigurne komunikacije. Neki od termina su se takođe promijenili kako bi naznačili nadograđenu tehnologiju naprednijih mobilnih telefona. Za razliku od GSM sistema gdje su algoritmi čuvani u tajnosti, 3GPP otvoreno poziva naučnu zajednicu da dizajnira njihove kriptografske sisteme. 3GPP objavljuje sve svoje nacrte, dizajn, i sigurnosne algoritme široj javnosti. To im je omogućilo da izaberu najbolje algoritme za autentifikaciju i enkripciju.

Glavni problemi GSM mreže su bili ranjivost na napad lažne bazne stanice, nedostatak sistema integriteta poruka i kratka dužina ključa A5 algoritma. A5 algoritam

koristi 64-bitni ključ koji se u to vrijeme smatrao sigurnim, ali sa pojavom jačih računara algoritam postaje ranjiv. Napad lažne bazne stanice je bio moguć jer su 2G sistemi samo potvrđivali korisnika, a ne i mrežu. 3GPP je želio da kreira sistem gdje su oba korisnika i mreža bili autentifikovani. Sistem provjere integriteta poruka bio je neophodan kako bi se osiguralo da nije bilo nikakvih problema sa komunikacijom između mreže i pretplatnika. Uz ove tri ideje, 3GPP je dizajnirao UMTS kriptografski sistem. HSDPA/HSPA+/LTE mreže su zasnovane na UMTS-u i stoga koriste isti algoritam za šifrovanje i autentifikaciju.

3.1 Integritet podataka: $f9$

Integritet podataka predstavlja svojstvo podataka koje garantuje da podaci nisu mijenjani od momenta njihovog nastanka. Kako bi osigurale integritet podataka UMTS mreže poruci dodaju 32-bitnu MAC-I vrijednost jedinstvenu za određenu mobilnu stanicu. Po prijemu poruke primalac računa očekivani kod integriteta XMAC-I, na isti način kao pošiljalac. Ukoliko bi u toku prenosa došlo do izmjene bilo koje od ulaznih vrijednosti ili same poruke, ove dvije vrijednosti bi bile različite i primalac bi znao da se poruka mijenjala u toku slanja.

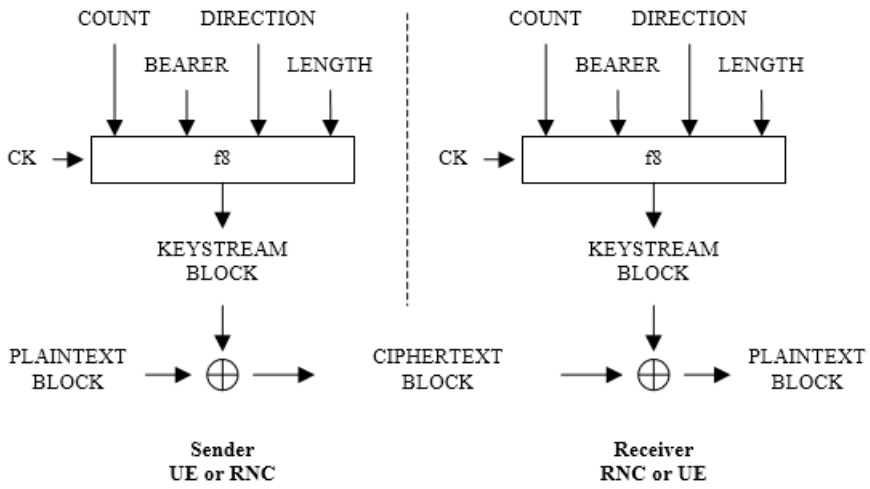
U svrhu izračunavanja ovih vrijednosti, UMTS mreže koriste $f9$ algoritam pod ključem integriteta IK.

Za jednostavnost primjene, $f9$ algoritam se u osnovi zasniva na istoj blok šifri $KASUMI$, kojeg također koristi i algoritam povjerljivosti $f8$. Ulazne vrijednosti za algoritam $f9$ su:

Izlaz za $f9$ algoritam je:

$$MAC-I \text{ (32-bita) Kod integriteta poruke } MAC-I[0]...MAC-I[31]$$

Slika 3.1: Izračunavanje koda integriteta poruke MAC-I i očekivanog koda XMAC-I



$COUNT-I$	(32 bita) Broj sekvence poruke $COUNT-I[0]...COUNT-I[31]$
$FRESH$	(1 bit) Slučajan broj generisan od strane mreže $FRESH[0]...FRESH[31]$
$DIRECTION$	(1 bit) Smjer komunikacije *uplink* ili *downlink* $DIRECTION[0]$
IK	(128 bita) Ključ integriteta $IK[0]...IK[127]$
$MESSAGE$	($LENGHT$ bita) Ulazni niz bita

S obzirom da $KASUMI$ algoritam proizvodi 64-bitni izlaz, za $MAC-I$ se uzima prvih 32 bita.

Inicijalizacija $f9$ algoritma počinje definisanjem dva 64-bitna registra A i B i postavljanjem oba na nulu. Modifikator ključa (*key modifier*) KM se definiše kao:

$$KM = AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$$

Ulazni parametri $COUNT$, $FRESH$, $MESSAGE$, i $DIRECTION$ su takođe nadovezani. Tada:

$$PS = COUNT[0]...COUNT[31]FRESH[0]...FRESH[31]MESSAGE[0]...$$
$$MESSAGE[LENGTH-1]DIRECTION[0]10^*$$

gdje 0^* označava između 0 i 63 '0' bite. Algoritam $f9$ je sada inicijalizovan.

Računanje $MAC-I$ počinje rastavljanje postavljenog PS stringa na 64-bitne blokove PS_i gdje:

$$PS = PS_0 \,||\, PS_1 \,||\, PS_2 \,||\, ... \,||\, PS_{BLOCKS-1}$$

Tada za svaki cio broj n sa svojstvom $0 \leq n \leq BLOCKS - 1$:

$$A = KASUMI\,[A \oplus PS_n]]_{IK}$$
$$B = B \oplus A$$

Konačno, izvodi se još jedna primjena $KASUMI$ algoritma sa modifikovanim ključem integriteta IK:

$$B = KASUMI\,[B]_{IK \oplus KM}$$

32-bitni $MAC-I$ sastoji se od prve polovine bita dobijenog rezultata.

$$MAC - I = \text{lijeva polovina}[B]$$

Tako za svaki cijeli broj i pri čemu je $0 \leq i \leq 31$ definišemo:

$$MAC - I\,[i] = B\,[i]$$

Biti $B\,[32]\,...B\,[63]$ su odbačeni. [6]

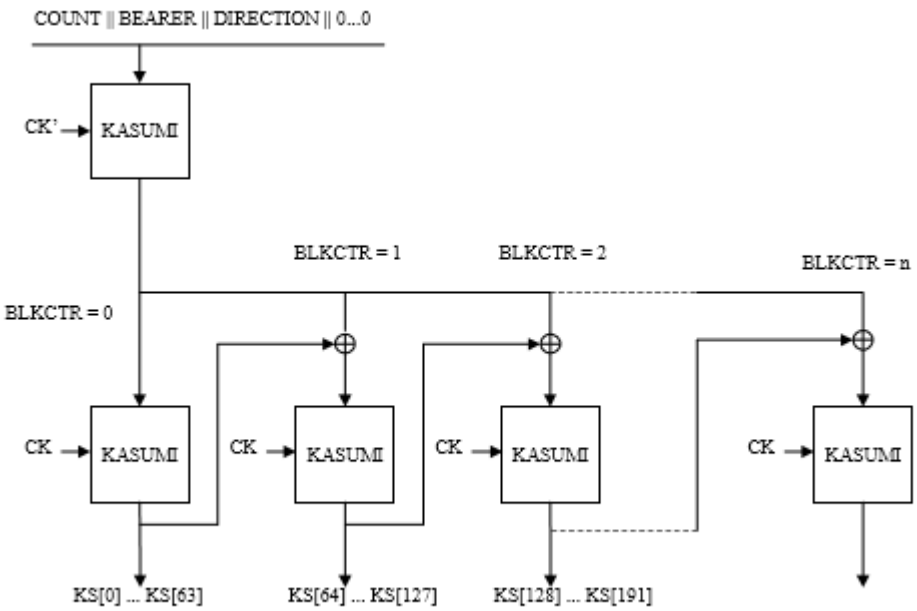
3.2 Algoritam za šifrovanje komunikacije - $f8$

Mobilne mreže novijih generacija preliminarno su definisale koncept IP multimedijalnih mreža, te je i njihova arhitektura znatno složenija. Kako su nadograđene na GSM sisteme, enkripcija i dekripcija se na sličan način vrše između korisnika i pristupne servisne tačke (RNC). Algoritam koji obezbjeđuje sigurnu komunikaciju zove se $f8$ algoritam i radi na sljedeći način:

Prvo koristeći ključ za šifrovanje Ck i druge parametre, u korisničkoj opremi izračunava izlazni niz bita. Drugo, izlazni niz bita se XOR-uje sa ulaznim nizom podataka u cilju dobijanja šifrovanog bloka podataka, tj. šifrata. Dalje se šifrat šalje na mrežu preko radio interfejsa. $f8$ algoritam na RNC-u koristi iste ulaze kao i korisnička oprema, uključujući i dijeljeni ključ Ck kako bi generisao isti izlazni niz bita kao i u korisničkoj opremi. Konačno, izlazni niz bita se XOR-uje sa šifratom kao bi se dobio originalni tekst. Na sličan način kao i u mrežama druge generacije se odvija dalja komunikacija sa primaocem.

$f8$ je sekvencijalni algoritam koji se koristi za enkripciju/dekripciju blokova podataka koristeći ključ povjerljivosti C_k i dodatne parametre: $DIRECTION$, $COUNTC$, $BEARER$, $LENGTH$. Sekvencijalni algoritam UMTS mreža koristi zbog njegove brzine i mogućnosti da se maska generiše prije nego što su podaci poznati.

Slika 3.2: Princip rada f8 algoritma



Jezgro $f8$ algoritma je KASUMI koji je šifra bloka. Algoritam $f8$ se sastoji od n KASUMI blokova, gde je $n = LENGTH$, od kojih svaki generiše po 64 bita, na osnovu ulaznih parametara iz registra A, brojača bloka podataka $BLKCNT$ i izlaznih bita prethodnog bloka.

Inicijalizacija generatora niza ključa počinje postavljanjem 64-bitnog registra A konkatenacijom:

$A = COUNT||BEARER||DIRECTION||0...0$

$A = COUNT[0]...COUNT[32]BEARER[0]...BEARER[4]DIRECTION[0]0...0$

gdje su poslednjih 26 bita postavljeni na 0. $BLKCNT$ je inicijalizovan na 0 i definišemo 128-bitni modifikator ključa KM kao binarni oktet 01010101 ponovljen 16 puta. Izmjena ulaznih podataka vrši se kako bi se smanjila predvidljivost izlaza $f8$ algoritma na osnovu ulaza. Zahvaljujući ovoj funkcionalnosti, skoro je nemoguće odrediti koji će izlazni blok biti generisan ukoliko nam je ulazni blok poznat.
Definišimo $KASUMI\,[x]_K$ kao izlaz KASUMI algoritma sa ulaznom vrijednošću x i ključem K.Dakle, inicijalizacija $f8$ algoritma vrši se jednom operacijom KASUMI algoritma na registar A sa modifikovanim ključem $CK \oplus KM$:

$$A = KASUMI\,[A]_{CK \oplus KM}$$

Pošto se tekst kojeg treba šifrovati sastoji od $LENGHT$ bita(1 - 20000) i generator niza ključa generiše bite u grupama od 64 bita, između 0 i 63 najmanje značajnih bita se izbacuju iz poslednjeg bloka u zavisnosti od ukupnog broja bita koje zahtijeva $LENGHT$. Promjenljiva $BLOCK$ jednaka broju $LENGHT/64$ zaokruženom na najbliži cio broj. Ako je $LENGHT = 192$ tada $BLOCKS = 3$. Ako je $LENGHT = 193$ tada je $BLOCKS = 4$. Za svaki cio broj n, pri čemu $1 \leq n \leq BLOCKS$ i $BLKCNT = n - 1$ možemo definisati keystream(?definisala sam na početku šta mi je keystream, mogu li ovako u nastavku da ga koristim ?) blok (KSB) definišući:

$$KSB_n = KASUMI[A \oplus BLKCNT \oplus KSB_{n-1}]_{CK}$$

Individualni biti keystream-a se izvlače od KSB_1 do KSB_{BLOCKS} u redosljedu tako da najznačajniji bit ide prvi. Za $n = 1$ do $BLOCKS$ i za svaki cijeli broj i, pri čemu $1 \leq i \leq 63$ definišimo:

$$KS[((n-1) * 64) + 1] = KSB_n[i]$$

gdje je $KS[i]$ i-ti bit keystream-a proizveden pomoći keystream generatora.

Jednom kada se keystream proizvede, šifrovanje teksta može se izvesti XOR-ovanjem ulaznih podataka sa generisanim keystream-om (KS). [4] Za svaki cio broj i, pri čemu $0 \leq i \leq LENGTH - 1$, definišimo izlaz za $f8$:

$$OBS[i] = IBS[i] \oplus KS[i]$$

Razlog za čak pet različitih ulaznih vrijednosti je smanjenje mogućnosti da se ista maska ponovi dva puta, što bi, ukoliko bi se desilo, dodatno olakšalo napade kriptoanalizom. Na primjer, ukoliko se dvije poruke šifruju istom maskom, binarni zbir šifrovanih poruka biće isti kao binarni zbir nešifrovanih, što znači da uporednom analizom određenih grupa bitova i upoređivanjem značenja dešifrovanog teksta možemo mnogo lakše da pretpostavimo koji će biti sledeći bit, što u velikoj mjeri skraćuje i olakšava napad. Ukoliko je cio niz poruka šifrovan istom vrijednošću, napad na takve poruke je još lakši, a jednom otkrivena maska, ukoliko nije mijenjana, napadaču može poslužiti da razumije cijelu komunikaciju. Zbog toga je bitno da se u toku komunikacije maska ne ponovi.

3.3 Kasumi algoritam

Poznati japanski naučnik i kriptograf Mitsuru Matsui, proučavanjem diferencijalne kriptoanalize dobio je ideju za novu tehniku testiranja kriptografskih blok algoritama

- linearnu kriptoanalizu. Matsui je osmislio dva nova 64-bitna blok algoritam koji koriste 128-bitni ključ, a koji su bili otporni na napade diferencijalnom i linearnom kriptoanalizom - MISTY1 i MISTY2.

U to vrijeme takođe je započet proces definisanja novog mobilnog standarda - UMTS, za koji su bile potrebne sekvencijalne funkcije za garanciju pouzdanosti i integriteta podataka kao i blok algoritam za šifrovanje, koji će se nalaziti u osnovi tih funkcija. Od svih tada poznatih blok algoritama MISTY1 je imao najveće šanse da bude iskorišćen, jer je bio najpogodniji za softversku i hardversku implementaciju u UMTS sistemu. Osim blok algoritama, ni sekvencijalni algoritmi nisu bili dovoljno dobri za implementaciju, pa je ideja bila da se osmisle posebne sekvencijalne funkcije koje će u osnovi imati MISTY1. Još jedan razlog zašto je MISTY1 odabran je ograničeno vrijeme za koje je bilo potrebno definisati algoritme za UMTS, a modifikovanje postojećeg algoritma bi oduzelo manje vremena od definisanja novog, čime bi se skratilo vrijeme potrebno za definisanje UMTS standarda. Osim toga, MISTY1 je više puta bio proučavan i dokazano je da je otporan na linearnu i diferencijalnu kriptoanalizu. Više timova je radilo na prepravkama MISTY1 i definisanju novih sekvencijalnih funkcija i konačno novembra 1999. stvorili su KASUMI algoritam, funkcija $f8$ za sekvencijalno šifrovanje i $f9$ za potvrdu integriteta podataka. Nakon toga su uslijedili testovi bezbjednosti KASUMI algoritma, a testovi su bili definisani tako da upoređuju ulazne i izlazne parametre funkcija na osnovu kojih se donose određeni zaključci. [3] Nijedan napad na KASUMI algoritam u sklopu mobilne UMTS mreže nije bio uspješan.

3.3.1 Struktura Kasumi algoritma

Iako baziran na MISTY1, KASUMI je modifikovan u tom pogledu da se što više olakša hardverska implementacija, a povećanje vremena izvršavanja, kompenzovano je

izbacivanjem pojedinih funkcija koje nisu značajno uticale na bezbjednost algoritma. Smanjenje bezbjednosti kompenzovano je dodavanjem još jedne iteracije S7 funkcije, što je značajno povećalo bezbjednost algoritma.

Mreža algoritma je zasnovana na Feistelovoj strukturi sa ukrštenim vezama i rekurzivnim ugnježdenim petljama sa različitim brojem iteracija. Ovakva struktura povećava veličinu bloka podataka i otpornost šifrovanog teksta. Sam algoritam se u osnovi sastoji od osam iteracija FO i FL funkcija, čiji se redosljed mijenja u svakoj iteraciji, i čiji su ulazni parametri dužine 32 bita. FO funkcija je takođe zasnovana na Feistelovoj strukturi u tri iteracije, u kojima se izvršava FI funkcija sa ulaznim parametrima dužine 16 bita. FI funkcija je kao i prethodne dvije zasnovana na Feistelovoj strukturi, sa dvije iteracije u kojima se izvršavaju S funkcije, takozvani S-BOX-ovi (S9 i S7).

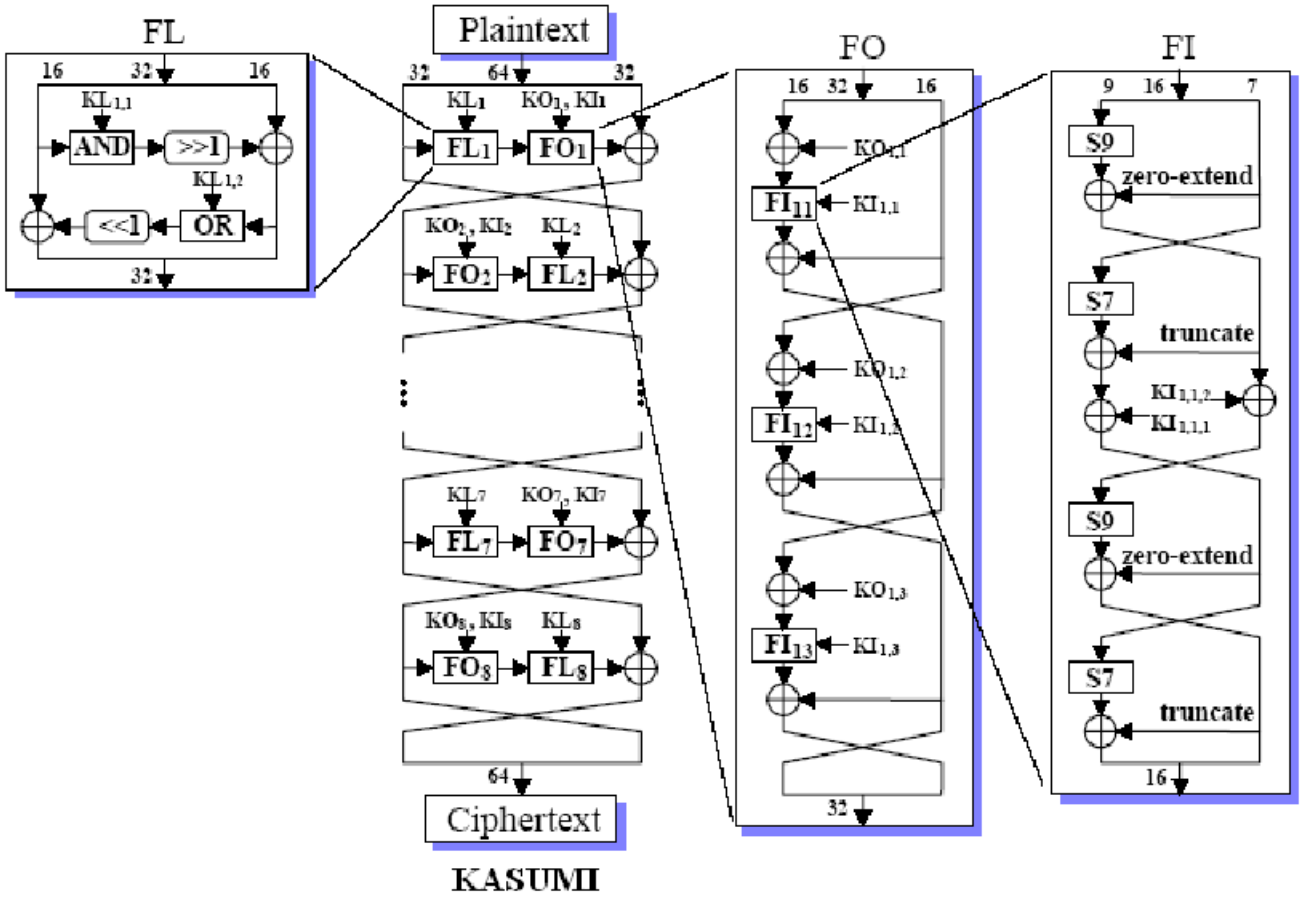
Segmentacijom na manje funkcije, implementacija algoritma je postala jednostavnija, a sam algoritam složeniji, jer su S7 i S9 funkcije relativno lake za hardversku implementaciju, a mrežne strukture oko ovih funkcija čine da algoritam bude kompletan. Iako nalikuje DES algoritmu, jer kao i DES koristi Feistelove strukture, KASUMI za razliku od DES algoritma ne koristi dekripciju, odnosno funkcija dekriptovanja je ista kao i funkcija enkriptovanja, što ima dodatnu prednost u implementaciji [7].

3.3.2 Princip rada Kasumi algoritma

KASUMI koristi 64-bitne blokove podataka i 128-bitne blokove ključa kako bi generisao 64-bitne izlazne (šifrovane) blokove podataka. Ulazni podaci se dijele na dva bloka po 32 bita, L_0 i R_0. Ti podaci se prosleđuju prvoj od osam iteracija u kojima se izvršava f-funkcija, koja objedinjuje FL i FO funkcije jedne iteracije.

Izlaz prve iteracije je:

Slika 3.3: Princip rada KASUMI algoritma



$$R1 = L0 \text{ i } L1 = R0 \oplus fi(L0, RK1),$$

gdje je $RK1$ skup ključeva KL, KO, KI, koji se koriste unutar FL, FO i FI funkcija. Tako će izlaz i-te iteracije biti:

$$Ri = Li - 1 \text{ i } Li = Ri - 1 \oplus fi(Li - 1, RKi),$$

odnosno izlaz algoritma se dobija konkatenacijom izlaznih blokova

$$R8 = L7 \text{ i } L8 = R7 \oplus f8(L7, RK8).$$

Funkcija f_i prima 32-bitni ulaz i daje 32-bitni izlaz uz pomoć RK_i ključa koji objedinjuje ključeve potrebne za FL i FO funkcije. f funkcija ima dvije različite

forme, parnu i neparnu. Razlika je u redosljedu izvršavanja FL i FO funkcija. U neparnim iteracijama se prvo izvršava FL funkcija, a u parnim FO funkcija. Shodno tome izlaz parne iteracije se razlikuje od izlaza neparne.
Pa će tako izlaz neparne iteracije biti:

$$f_i(I, RK_i) = FO_i((FL_i(I, KL_i), KO_i, KL_i)$$

Dok će izlaz parne biti malo drugačiji:

$$f_i(I, RK_i) = FL_i(FO_i(I, KO_i, KI_i), KL_i)$$

Funkcija FL

FL funkcija za 32-bitni ulaz, koristeći 32-bitni ključ KL daje 32-bitni izlaz. Kako se ulazni podaci dijele na dva jednaka 16-bitna bloka $I = L||R$, i ključ KL se dijeli na dva jednaka dijela

$$KL = KL_{i,1}||KL_{i,2}.$$

Izlaz jedne iteracije FL funkcije za lijevi odnosno desni dio funkcije bi bio:

$$L' = L \oplus ROL(R' \cup KL_{i,2})$$
$$R' = R \oplus ROL(L \cap KL_i, 1)$$

gdje je ROL lijevi ciklični pomjeraj bloka za jedan bit, $\cup$ logička operacija "ili", a $\cap$ logička operacija "i". Uloga FL funkcije u KASUMI algoritmu je da otežа praćenje pojedinačnih bitova kroz iteracije algoritma.

Funkcija FO

FO funkcija koristi 32-bitni ulaz podataka i dva 48-bitna ključa, KO i KI. Podaci sa ulaza se dijele na dva 16-bitna bloka, $I = L_0 \,||\, R_0$, dok se ključevi dijele na tri dijela:

$$KO_i = KO_{i,1} \,||\, KO_{i,2} \,||\, KO_{i,3}$$
$$KI_i = KI_{i,1} \,||\, KI_{i,2} \,||\, KI_{i,3}$$

Izlaz svake od tri iteracija bi bio za desni dio, odnosno lijevi dio:

$$Rj = FI(L_{j-1} \oplus KO_{i,j}, KI_{i,j}) \oplus R_{j-1}$$
$$L_j = R_{j-i}$$

gdje i označava i-ti blok FO funkcije, a j označava iteraciju unutar bloka. Izlaz FO funkcije je 32-bitna vrijednost $(L_3 \,||\, R_3)$.

Funkcija FI

FI funkcija kao ulaz ima 16-bitni blok podataka I i 16-bitni ključ $KI_{i,j}$. Ulazni podaci se dijele na dva nejednaka bloka, 9-bitna lijeva strana L_0 i 7-bitna desna strana R_0 gdje je $I = L_0 \,||\, R_0$. Na sličan način se i ključ $KI_{i,j}$ rastavlja na dva ključa od po 7 i 9 bita, gdje je $KI_{i,j} = KI_{i,1} \,||\, KI_{i,2}$, koji služe kao ulazni podaci S funkcija - $KI_{i,1}$ za $S7$, a $KI_{i,2}$ za $S9$.

Razlog za ovakvu podjelu bitova je taj što bijektivne funkcije neparne dimenzije imaju manju linearnu predvidljivost, što ih čini otpornijim na linearnu kriptoanalizu. Ove funkcije za ulazni podatak od 7 bita (funkcija $S7$) daju izlaz od 7 bita. Isto tako i za 9-bitni ulaz, $S9$ funkcija daje 9 - bitni izlaz. Pošto se podaci unutar FI funkcije ne dijele na blokove iste dužine, to malo komplikuje manipulaciju podacima, pa je potrebno definisati ZE i TR funkcije, koje vode računa o dužini ulaznih blokova. Tako definišemo:

ZE od 7-bitnog bloka daje 9-bitni dodavanjem dvije nule sa lijeve strane,

TR od 9-bitnog bloka daje 7-bitni odsijecanjem dva skroz lijeva bita.

Izlaz FI funkcije po unutrašnjim iteracijama je sledeći:

$$
\begin{array}{ll}
L_1 = R_0 & R_1 = S9[L_0] \oplus ZE(R_0) \\
L_2 = R_1 \oplus KI_{i,j,2} & R_2 = S7[L-1] \oplus TR(R-1) \oplus KI_{i,j,1} \\
L_3 = R_2 & R_3 = S9[L-2] \oplus ZE(R_2) \\
L_4 = S7[L_3] \oplus TR(R_3) & R_4 = R_3
\end{array}
$$

Derivacija ključa

Kasumi algoritam poštuje osnovne postulate bezbjednosti i u svakoj iteraciji koristi drugačiji 128-bitni ključ. Svaki taj ključ stvoren je korišćenjem jedinstvenog K ključa. Prije nego što se generišu ključevi funkcija KI, KO i KL, generišu se dva niza od po osam 16-bitnih vrijednosti, K_i i K'_i. Niz K_i je generisan segmentacijom ključa K na 16-bitne blokove:

$$K = K1 \,||\, K2 \,||\, K3 \,||\, K4 \,||\, K5 \,||\, K6 \,||\, K7 \,||\, K8$$

Dok je niz K'_i izveden iz niza K_i, primjenjujući za svako i, pri čemu važi $1 \leq i \leq 8$:

$$K'_i = K_i \oplus C_i$$

Konstanta C je zapravo niz konstanti od osam vrijednosti - po jedna za svaku od osam iteracija KASUMI algoritma.

$$
\begin{array}{ll}
C1 = \text{0x0123} & C2 = \text{0x4567} \\
C3 = \text{0x89AB} & C4 = \text{0xCDEF} \\
C5 = \text{0xFEDC} & C6 = \text{0xBA98} \\
C7 = \text{0x7654} & C8 = \text{0x3210}
\end{array}
$$

Nakon generisanja K_i i K'_i ključeva, slijedi derivacija KL, KO i KI ključeva. Za opis postupka derivacije ključeva KL, KO i KL pogledati [7]. Na ovaj način svaka iteracija svake od funkcija će imati jedinstven ključ, što predstavlja jedan od osnovnih principa bezbjednosti [7].

3.4 Sigurnosni nedostaci mreža novije generacije

Mreže treće generacije postigle su priličan nivo zaštite podataka. Takođe, sigurnosne mjere se mogu lako mijenjati i unaprjeđivati u skladu sa uočenim potrebama.

Mnogi od napada i dalje nisu spriječeni kao što su odbijanje servisa, napad koji je do sada posebno napadao veb sajtove. Napadač može lako zagušiti mrežu lažnim zahtjevima. Nemogućnost ostvarivanja konekcije jeste bezbjednija po pitanju zaštite podataka od kompromitovanja konekcije, ali korisnik ne može obavljati željene poslove, čime sama zaštita gubi smisao.

Na mnogim područjima i dalje se koriste GSM sistemi. Uslijed nedostupnosti 3G ili 4G mreža mobilni uređaj prelazi na korišćenje 2G sistema, što lako omogućava napadaču prisluškivanje i ometanje poziva pomoću danas jeftinih i dostupnih uređaja.

Teorijske napade predstavio je K. Kotapati u svom radu [9]. Identifikuje pet glavnih napada na komunikacione entitete u mreži: presretanje, ometanje, umetanje, modifikacija i odbijanje servisa. U knjizi su predstavljeni teorijski napadi na 3G i 4G sisteme od kojih su neki kasnije uspješno realizovani. Za detalje opise napada na algoritam kritovanja KASUMI pogledati [9].

Glava 4

Zaključak

U počecima stvaranja 2G i 3G mreža sigurnost je bila jedan od glavnih ciljeva, mada su se u praktičnoj implementaciji pokazali i određeni nedostaci.

Kod analognih sistava je relativno jednostavno bilo zaštititi korisnika i vezu, jer se radilo samo o govornim pozivima. Pojavom digitalnog doba i novog načina prenosa podataka, te novim uslugama, nije samo porastao broj usluga , već i broj potencijalno različitih napada na korisnike, mrežu i usluge.

U novim implementacijama kao što su LTE mreže i 5G mreže funkcije za zaštitu podataka su poboljšane iako i one sadrže određene propuste.

Procijenjeno je da se računarska snaga udvostručuje svake dvije-tri godine što obezbjeđuje napadačima da razvijaju nove napade na postojeće sisteme. Ne može se pobjeći od činjenice da ništa nije 100% sigurno, te da i pored zaštite postoje propusti i nove mogućnosti za napade na sigurnost. Njih mogu iskoristiti isključivo stručni napadači ili organizacije kao što su vlada i vojska što im može omogućiti presretanje poziva i prosluškivanje.

U našoj državi je aktuelna 4G mreža, pri čemu mobilni uređaji često prelaze na 2G i 3G sisteme. Te prisluškivati korisnika često može i pojedinac za osnovnim znanjem funkcionisanja mreža i jeftinim uređajima za prisluškivanje.

Bibliografija

[1] Keith M. Martin, "Everyday Cryptography: Fundamental Principles and Applications", Second Edition

[2] Marin Hofer, "Kriptoanaliza A5/2", Univerzitet u Beogradu, Matematički fakultet, 2016

[3] Dušan Kilibarda, "Bezbednost mobilnih mreža najnovije generacije", 2014

[4] David Royer Lewis , "Mobile phone security specializing in GSM, UMTS, and LTE networks", Faculty of San Diego State University, 2014

[5] Valtteri Niemi, Kaisa Nyberg, "UMTS Security", Nokia Research Center, Finland, 2003

[6] G. T. 33.909, 3G security; Report on the evaluation of 3GPP standard confidentiality and integrity algorithms, technical report, 3GPP, 2001.

[7] G. T. 35.202, Specification of the 3GPP confidentiality and integrity algorithms; document 2: Kasumi, technical report, 3GPP, 2012.

[8] Dan Boneh, "Advances in Cryptology – CRYPTO 2003: 23rd Annual International Cryptology Conference", USA, 2003

[9] K. Kotapati, P. Liu, Y. Sun, i T. F. L. Porta, "A Taxonomy of Cyber Attacks on 3G Networks", ISI, 2005