	УНИВЕРЗИТЕТ „УНИОН“ **РАЧУНАРСКИ ФАКУЛТЕТ** Кнез Михаилова 6/VI 11000 БЕОГРАД	Број: Датум:

UNIVERZITET UNION
RAČUNARSKI FAKULTET
BEOGRAD
RAČUNARSKE MREŽE I KOMUNIKACIJE

DIPLOMSKI RAD

Kandidat: Dušan Kilibarda
Broj indeksa: RM 10/09

Tema rada: Bezbednost mobilnih mreža najnovije generacije

Mentor rada: prof. dr Đorđe Babić

Beograd, 1.12.2014.

Ovih prvih par redova iskoristiću za kritički osvrt prema sebi samom za period od kada sam uzeo temu za diplomski rad, do današnjeg dana, kada je rad gotov.
Temu ovog diplomskog rada sam odabrao bez predstave u šta se upuštam. Put je bio dug i uzbudljiv, pa se napor nije previše osetio. U isto vreme sam dobio prvi posao, što je sigurno uticalo na prolongiranje pisanja diplomskog, ali verujem i na promenu načina mog razmišljanja, pa samim tim i na kvalitet diplomskog rada. Zbog toga je rad, na moju inicijativu, pretrpeo nekoliko kompletnih izmena pre konačne verzije.
Osim početnog problema sa nedostatkom literature, najveći problem sa kojim sam se susreo bio je taj što je trebalo odlučiti koje delove teme obraditi, a koje ne, šta izbaciti iz rada, odnosno šta uopšte ne ubaciti. Tema mi je u svakom trenutku bila interesantna, ali na žalost preobimna, pa sam tako imao veliki broj nedoumica šta ubaciti i šta je bitno, u čemu su mi uputstva profesora Babića veoma pomogla.

Ovom prilikom bih želeo da se zahvalim prof. dr Đorđu Babiću koji mi je pomogao u izradi ovog diplomskog rada, kao i svojoj porodici i prijateljima na strpljenju i podršci koju su mi pružili tokom studiranja. Ovim vam odgovaram na brojna postavljena pitanja "Kada?" i "Zašto?".

Dušan Kilibarda

SADRŽAJ

1. UVOD

Ljudska radoznalost i želja za nečim novim pokrenula je lančanu reakciju u kojoj se smenjuju i uzajamno dopunjuju tehnička unapređenja uzrokovana zahtevima i novi zahtevi uzrokovani tehničkim dostignućima. Ista pojava se primećuje i u razvoju mobilnih mreža i mreža uopšte. Čoveku nije bila dovoljna komunikacija između udaljenih fiksnih tačaka, već je postojala potreba za komunikacijom i u toku pokreta kao i komunikacijom sa nepristupačnih terena. Tim zahtevom je iniciran razvoj mobilnih mreža. Danas mobilne mreže koristi nekoliko milijardi korisnika. 2013. godine odnos broja mobilnih telefona i živog stanovništva Zemlje bio je 97%, dok se u 2014. očekuje da na Svetu bude više mobilnih telefona nego ljudi. Razvoj servisa i aplikacija koje koriste mobilne mreže beleži promene na dnevnom nivou i postavlja se pitanje da li su mobilne mreže dovoljno sigurne da izdrže ovaj nalet novih korisnika i obezbede im sigurnu uslugu.

2. RAZVOJ MOBILNIH MREŽA

Nastankom prvih bežičnih telefona početkom dvadesetog veka, nastaje potreba za povećanjem dometa, proširenjem oblasti u kojima bežični telefoni mogu da rade i povećanjem broja korisnika. Broj korisnika je predstavljao ozbiljan problem, jer se za komunikaciju između dva korisnika zauzimala cela frekvencija, a broj frekvencija koji se koristio, osim što je bio ograničen, u to vreme je bio i veoma mali. Pronalaskom bežičnih ćelijskih sistema i integracijom u postojeću mrežnu infrastrukturu, korisnicima bežičnih telefona se daje mogućnost kretanja kroz oblasti ćelijskog sistema bez gubitka veze – uređaji postaju mobilni. Ćelija podrazumeva oblast pokrivenu signalom jedne bazne stanice, dok ćelijski sistem obuhvata sve oblasti pokrivene signalima baznih stanica u jednom regionu.

Prednosti uspostavljanja ovakvog sistema ogledaju se u boljoj iskorišćenosti frekvencija i većoj mobilnosti korisnika mobilne mreže. U ćelijskim sistemima moguće je ponavljanje frekvencija u više različitih ćelija, a da pritom ne dođe do interferencije signala, odnosno sistem sa istim brojem frekvencija može da pokrije veću geografsku površinu i samim tim podrži veći broj korisnika. Osim toga, uvođenjem Time Division Multiple Access (TDMA), omogućuava se da isti kanal opslužuje veći broj korisnika istovremeno deljenjem iste frekvencije na vremenske slotove. U GSM sistemu, koji koristi TDMA, moguće je koristiti 124 frekvencije, od kojih se svaka deli na osam kanala, tako da sistem raspolaže sa ukupno 992 kanala.

Sledeći korak u razvoju mobilnih mreža je pitanje bezbednosti, odnosno kako obezbediti siguran prenos podataka, otporan na greške u toku prenosa, koji će biti „čitljiv“ prijemnoj strani, a uz to „nečitljiv“ posrednicima u prenosu ili trećim licima koja bi mogla da prisluškuju komunikaciju.

Dok kod prvih mobilnih analognih mreža (1G) šifrovanje signala nije postojalo, a za komunikaciju između dva korisnika se zauzimala cela frekvencija, koju je mogao da prisluškuje i ometa bilo ko, kod projektovanja digitalnih mobilnih mreža (2G, 3G) mnogo više truda se uložilo u razvijanje bezbednog prenosa podataka, zaštitu korisnika i povećanje kapaciteta, odnosno brzine saobraćaja.

2.1. 2G

Pretnje sa kojima se susreće mobilna mreža su vezane za zaštitu razgovora od ometanja i prisluškivanja, zaštitu korisnika od krađe korisničkih podataka i zaštitu sistema od kompromitovanja sistemskih parametara.

Global System for Mobile Communications (GSM) kao predstavnik mobilnih celularnih mreža druge generacije (2G), unapred je projektovan da reši probleme bezbednosti. Kao standard, GSM je dizajniran da bude siguran mobilni sistem sa autentifikacijom korisnika i šifrovanjem podataka u toku prenosa. Iako

sam model i algoritmi nikada nisu javno objavljeni, proučavani su od trenutka nastanka 1991. godine do danas i propusti u funkcionalnosti su ipak pronađeni, čime je zaključeno da bezbednost GSM sistema nije potpuna.

Kao što je pomenuto na početku, tehničke inovacije i ljudska želja su deo uzajamne lančane reakcije. U to vreme siguran GSM standard korisnicima nije pružao dovoljnu funkcionalnost, jer osim poziva i slanja kratkih tekstualnih poruka, nikakvu drugu funkcionalnost nije imao. U isto vreme internet se sve brže razvijao i korisnicima nudio sve raznovrsnije opcije.

Postojali su pokušaji da se funkcionalnost GSM-a poveća, pa je tako Short Message Service (SMS) korišćen za plaćanje računa, ali s obzirom na to da se SMS prenosi u obliku čistog teksta, ova usluga nije bila bezbedna.

2.2. 2.5G

Kao odgovor na zahtev korisnika za novim servisima, GSM standard je proširen uvođenjem prenosa podataka putem General Packet Radio Service (GPRS). Ovaj servis nudi prijem i slanje elekrtonske pošte i multimedijalnih poruka u vidu slika, brzinom od 115Kb/s. Kasnije je upotrebom Enchanced Data Rates for Global Evolution (EDGE) tehnologije brzina povećana na 348Kb/s.

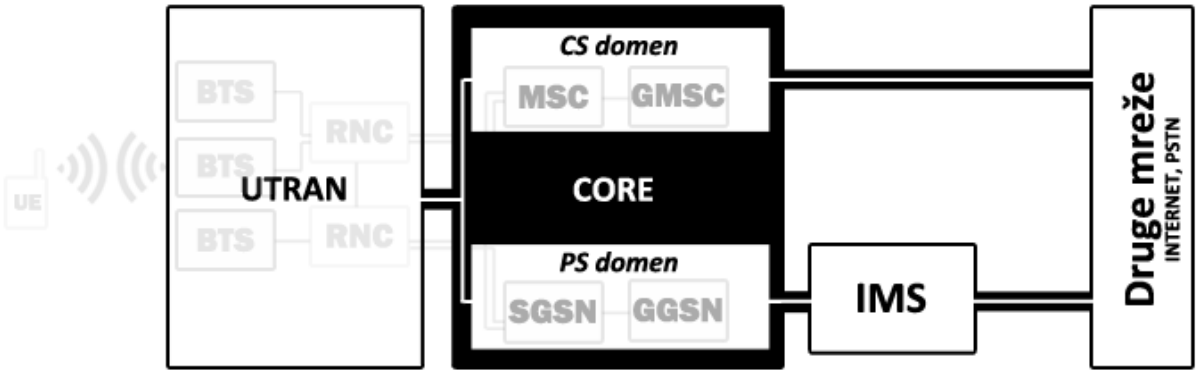
Uvođenjem paketskog prenosa podataka u osnovnu GSM komunikaciju, zvanično nastaju 2.5G mreže. CORE GSM mreže, koji je do tada obavljao funkciju komutiranja veza, morao je biti podeljen na dva domena, CS domen (Circuit-switched Domain) koji sadrži uređaje potrebne za komutaciju veza i PS domen (Packet-switched Domain) koji sadrži uređaje potrebne za komutaciju paketa (prenos podataka). Ova dodatna funkcionalnost je zapravo nadogradnja na postojeći GSM sistem koja utiče na pojavu novih vrsta napada na mobilne mreže jer postaje integralni deo mobilne mreže i koristi već postojeće elemente GSM mrežne infrastructure.

Do uvođenja GPRS, 2000. Godine, GSM mreže su korisnicima pružale relativno dovoljnu zaštitu, dok je sigurnost GSM/GPRS sistema okarakterisana kao umerena. Dodatna otežavajuća okolnost je što uvođenjem novih servisa koji koriste paketski prenos podataka, korisnici sve više ličnih podataka prenose kroz mrežu, pa se i cilj napada menja i usmerava ka krađi identiteta i podataka “trećih servisa”, koji mobilnu mrežu koriste samo kao medijum za prenos. Mobilnim mrežama se time nameće dodatna obaveza, da osim o komunikaciji krajnjih korisnika, čuvanju njihovih podataka, čuvanju podataka mreže, vode računa i o zaštiti podataka između korisnika i interneta.

2.3. 3G

Zbog velikog broja tehničkih propusta, nedovoljne zaštite GSM/GPRS mreža, i zahteva za dodatnim funkcionalnostima i većim brzinama prenosa podataka, u mobilne mreže se implementira nova tehnologija – Universal Mobile Telecommunication Systems (UMTS) – 3G. UMTS je, kao i GPRS, tehnologija koja je nadograđena na postojeću GSM infrastrukturu i osmišljena da bude kompatibilna sa postojećim GSM sistemom. Implementacijom UMTS-a, 2003. godine, ispravljene su greške koje su

dozvoljavale napade upotrebom lažne bazne stanice na nezaštićeni prenos kriptografskih ključeva i autentifikaciju u samoj mreži, kao i krađu korisničkog identiteta – o ovim napadima će biti više reči kasnije. Osim sigurnosnih poboljšanja, UMTS je korišćenjem naprednijih metoda multipleksiranja, Wideband Code Division Multiple Access (WCDMA), umesto dotadašnjeg TDMA povećao i brzinu prenosa podataka na 2Mb/s, čime je povećan i broj usluga koja je moguće ponuditi korisnicima, od kojih je najbitnija prenos multimedijalnog sadržaja (video pozivi, video "streaming"...). Prenos multimedijalnog sadržaja je veoma bitna funkcionalnost, zbog tendencije rasta broja multimedijalnih servisa na internetu. Zbog toga je bilo potrebno da se CORE mobilne mreže još jednom izmeni, odnosno proširi, pa je pored dotadašnjih PS i CS domena, dodata još jedna funkcionalna grupa – IMS (IP Multimedia Subsystem), koja povezuje PS i ostatak interneta.



Funkcionalne grupe UMTS mreže: *UTRAN (UMTS Terrestrial Radio Access Network) – Pristupna radio mreža, obuhvata kontrolere baznih stanica i bazne stanice; CS domen (Circuit-switched Domain) – Domen linijske komutacije, obuhvata uređaje čija je uloga u komutaciji linija, kanala, odnosno poziva; PS domen (Packet-switched Domain) – Domen paketske komutacije, obuhvata uređaje čija je uloga u komutaciji paketa, odnosno IP saobraćaja.*

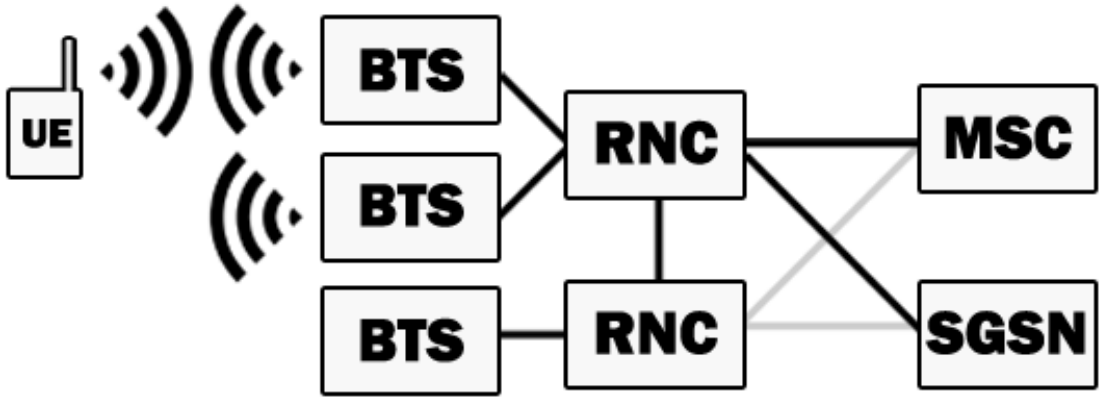
3. MOBILNI SISTEMI

Mobilni sistem, grubo govoreći, predstavlja sistem u kome korisnici mogu međusobno da kumuniciraju putem mobilne mreže, koristeći mobilne telefone. Preciznije, mobilni sistem se sastoji od korisnika koji eksploatišu i mobilne mreže koja je eksploatisana. Sistem se sastoji od četiri osnovna dela:

- Mobilnog uređaja (Mobile Station - MS),
- Sistema baznih stanica (Base Station System - BSS),
- Mrežnog i komutacijskog sistema (Network and Switching System - NSS),
- Sistema operativne podrške (Operation Support System - OSS).

Mobilni uređaj je najčešće mobilni telefon, koji ima svoj jedinstveni petnaestocifreni International Mobile Station Equipment Identity (IMEI) broj i koristi Subscriber Identity Module (SIM) karticu na kojoj se nalazi jedinstveni petnaestocifreni International mobile Subscriber Identity (IMSI) broj i jedinstveni, tajni ključ Ki. U UMTS mrežama se koristi Universal Integrated Circuit Card (UICC) kartica, koja je slična SIM kartici, ali osim SIM aplikacije za GSM, sadrži i Universal Subscriber Identity Module (USIM) aplikaciju za UMTS i IP Multimedia Services Identity Module (ISIM) aplikaciju za IMS, pa može da koristi i GSM i UMTS i paketski prenos.

Sistem baznih stanica obuhvata sistem za prenos radio signala između kontrolera baznih stanica (Base Station Controllers - BSC) ili kontrolera radio signala (Radio Network Controllers - RNC) i primopredajnih baznih stanica (Base Transciever Stations - BTS). BSC je komutator u GSM mrežama, koji povezuje MSC (Mobile Services Switching Center) i BTS. Hijerarhijski gledano, jedan MSC kontroliše više BSC ili RNC, koji kontrolišu više BTS. BTS sadrži opremu za upravljanje radio signalima ka korisnicima unutar ćelija. RNC u UMTS mrežama ima sličnu ulogu kao BSC u GSM-u, da povezuje paketski komutiranu mrežu (Core mobilne mreže) i linijski komutiranu mrežu (deo mobilne mreže između korisničkog uređaja i RNC). RNC je povezan na MSC i SGSN (Serving GPRS support node) i osim što kontroliše bazne stanice, odnosno konekcije ka mobilnim uređajima i raspolaže radio resursima, vodi računa i o mobilnosti korisnika, odnosno obezbeđuje takozvani “soft handover”, prelazak korisnika sa jedne bazne stanice na drugu, ili čak sa jednog RNC na drugi bez prekida komunikacije.



Sistem baznih stanica: *UE – User Equipment, BTS – Base Transciever Station, RNC – Radio Network Controller, MSC - Mobile Switching Center, SGSN - Serving GPRS Support Node;*

Mrežni i komutacioni sistem obavlja funkcije komutiranja i upravljanja komunikacijom između mobilnih uređaja i javne komutirane telefonske mreže - PSTN, i komutiranja paketa između mobilnih uređaja i internet mreže. Komutacija paketa nije sastavni deo GSM sistema, već je implementirana pri uvođenju GPRS-a.

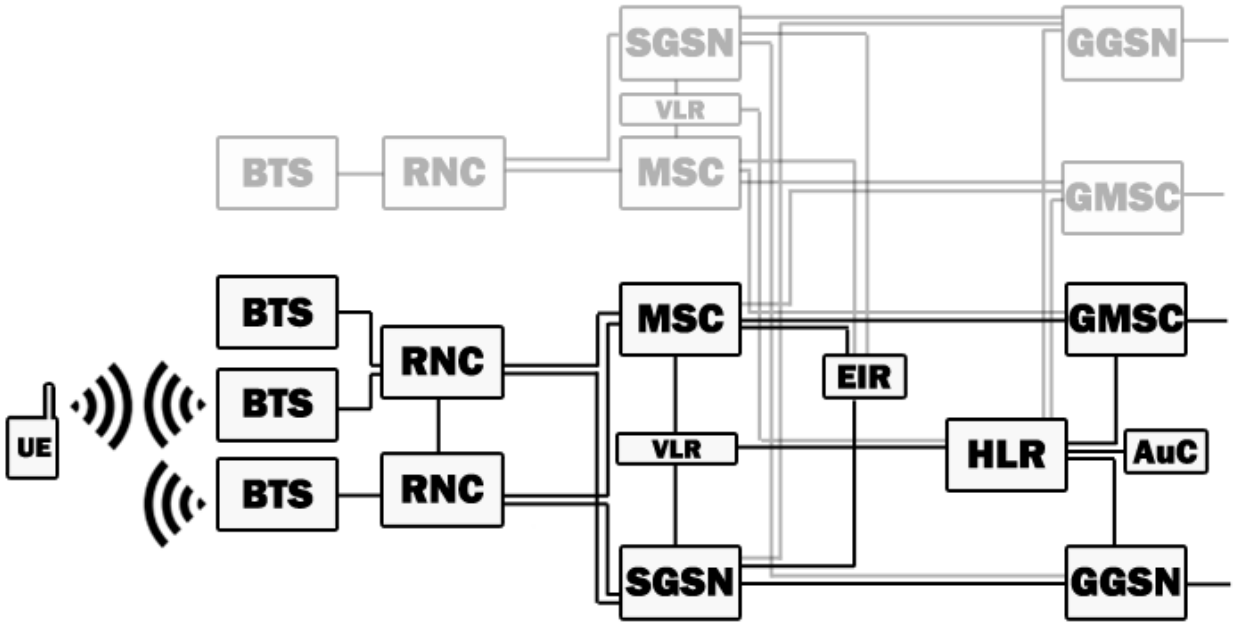
Delovi komutacionog sistema su:

- **MSC (Mobile Switching Center)** - Mobilni komutacioni centar je deo mobilne mrežne infrastrukture koji upravlja pozivima, signalizacijom unutar mreže između krajnjih korisnika, naplatom i evidencijom korisničkih računa u realnom vremenu i povezivanjem novih mobilnih uređaja.
- **GMSC (Gateway Mobile Switching Center)** - Deo mobilne mrežne infrastrukture koji služi za upravljanje pozivima između dve mobilne mreže.
- **HLR (Home Location Register)** - Registar vlastitih pretplatnika je centralna baza podataka koja sadrži podatke o korisnicima kojima je dozvoljeno da koriste mobilnu mrežu. Sadrži private i javne podatke o korisniku, uslugama koje mu se isporučuju, trenutnom položaju, kao i podešavanja za paketski prenos.
- **VLR (Visitor Location Register)** - Registar gostujućih pretplatnika je privremena baza podataka koja sadrži podatke o korisnicima koji privremeno gostuju u delu mreže koji kontroliše lokalni MSC. Kada se gostujući pretplatnik "javi" lokalnom MSC-u, VLR vezan za taj MSC prosleđuje MSC-u potrebne podatke ukoliko su mu poznati ili kontaktira HLR tog pretplatnika kako bi dobio podatke o korisniku. VLR u mreži nije obavezan i implementira se zbog smanjenja broja zahteva koji bi se inače slali HLR-u. Umesto da svaki MSC za svakog svog korisnika svaki put šalje zahteve HLR-u, slaće ih VLR-u i time rasteretiti ostatak mreže. VLR je povezan na najmanje jedan MSC, tako da je jedna BTS povezana na jedan VLR, tj. jedan korisnik može u jednom trenutku biti samo u jednoj VLR bazi.
- **AuC (Authentication Center)** - Centar za autentifikaciju je baza podataka pridružena HLR-u, koja sadrži podatke za autentifikaciju i proveru korisničkog identiteta - kopije tajnih ključeva korisnika i vektore autentifikacije, koje generiše.
- **EIR (Equipement Identity Register)** - Registar identiteta opreme je baza podataka koja sadrži informacije o IMEI brojevima svih mobilnih uređaja koji su zabranjeni u mreži, ili se

prate.

- **SGSN (Serving GPRS Support Node)** - Implementiran prvi put u 2,5G mrežama, kada je uveden paketski prenos podataka, a zadržan je kao sastavni deo UMTS mreža. Ima sličnu ulogu kao MSC, a razlika je u tome što umesto glasovnom komunikacijom, SGSN upravlja komutacijom i rutiranjem paketa podataka unutar mreže, autentifikacijom i sesijama paketskog prenosa. U mreži može postojati više SGSN nodova, koji međusobno mogu direktno da komuniciraju ukoliko se nalaze u istom PS domenu. Ukoliko se nalaze u različitim PS domenima, njihova komunikacija se vrši preko GGSN noda.
- **GGSN (Gateway GPRS Support Node)** - Kao i SGSN, implementiran prvi put u 2,5G mrežama. Ima ulogu u rutiranju paketa podataka između lokalne paketske komutirane mreže i drugih, spoljnih, paketskih komutiranih mreža, PS domena ili interneta.
- **MGW (Media Gateway)** – Deo mobilne mreže dodat u kasnijim revizijama UMTS-a, koji nasleđuje ulogu koju su do tada vršili MSC i GMSC – prenos korisničkog saobraćaja, dok MSC i GMSC nastavljaju da vrše ulogu prenosa kontrolnih podataka i signalizacije.

Sistem operativne podrške je spojen na svu opremu i omogućava mobilnom operateru centralizovan sistem nadzora i administracije mobilne mreže.



Osnovni elementi mobilne mreže: *UE – User Equipment, BTS – Base Transciever Station, RNC – Radio Network Controller, MSC - Mobile Switching Center, SGSN - Serving GPRS Support Node, VLR - Visitor Location Register, EIR - Equipement Identity Register, HLR - Home Location Register, AuC - Authentication Center, GMSC - Gateway Mobile Switching Center, GGSN - Gateway GPRS Support Node;*

3.1. DODATNE FUNKCIONALNOSTI

Osim osnovnih funkcionalnosti, mobilna mreža može imati i dodatne, pa samim tim i dodatne elemente koji bi te funkcionalnosti omogućili.

- Mobile Service Node (MSN)
- GSM Interwork Unit (GIWU)

MSN integriše usluge "inteligentne mreže" unutar mobilne GSM mreže, pružajući dodatne usluge. Primeri ovih usluga su: glasanje putem SMS-a, prebacivanje mobilnog broja u drugu mrežu, čuvanje glasovne pošte, poziv na čekanju, preusmeravanje poziva.

GIWU predstavlja hardversko i softversko rešenje za prebacivanje između glasovnog i paketskog prenosa u toku razgovora (primer: prelazak sa bazne stanice koja podržava 3g na baznu stanicu koja ne podržava). Takođe se implementira unutar MSC-a.

3.2. USPOSTAVLJANJE POZIVA U MOBILNOJ MREŽI

Uspostavljanje poziva se izvršava u nekoliko koraka:

Kada korisnik odabere broj, mobilni uređaj prvo traži kanal, onda se vrše identifikacija i autentifikacija kod AuC i EIR uz pomoć IMEI i IMSI broja. Zatim poziv ide redom preko BTS, BSC/RNC, MSC, GMSC, sve do GMSC-a druge mreže.
Nakon što poziv dođe do GMSC-a odredišne mreže, odredišni GMSC od svog HLR-a traži informacije o korisničkom MSC-u i BSC/RNC-u. HLR i VLR razmenjuju podatke o pozvanom korisniku. MSC preko BSC/RNC-a prenosi svim BTS-ima zahtev za pozivanje određenog korisnika. AuC i EIR proveravaju i autentifikuju pozvanog korisnika. Osigurava se kriptografska zaštita komunikacije i komunikacija može da počne.

3.3. IMS

IP Multimedia Subsystem (IMS) je deo mobilne mreže, koji povezuje PS domen lokalne mobilne mreže i globalnu internet mrežu. Iako je deo mobilne mreže, IMS nije svestan mobilnosti uređaja i služi samo za implementaciju servisa baziranih na IP. Pošto je u pitanju servis koji radi pre svega sa paketima internet protokola, CS domen nije direktno povezan na njega, ali IMS može da implementira funkcionalnost translacije IP paketa u pakete protokola CS domen, tako da pozivi u mobilnoj mreži koriste protokole CS domena, a van mreže internet protokol. Njegova uloga je da vodi računa o multimedijalnim servisima, raspolaže i prati IP adrese koje koriste te servise i IP adrese samih servisa, raspolaže portovima, kao i da vodi računa o kodecima koji se koriste, kvalitetu servisa, itd. Implementacija IMS-a je zahtevala izmenu

dotadašnjeg HLR-a, odnosno proširenje HLR-a sličnim servisom koji će sadržati podatke o korisnicima paketskog saobraćaja – HLR postaje Home Subscriber Server (HSS).

4. SIGURNOSNE PRETNJE

Ubrzan razvoj internet servisa nesumnjivo je uticao na razvoj mobilnih mreža, povećanje brzine podataka, razvoj mobilnih uređaja i servisa koji bi te mreže maksimalno iskoristili. Ovaj razvojni bum pokrenuo je lavinu pitanja o bezbednosti mreža, zaštiti korisnika i njihovih podataka.

Cilj zaštite mreže je zaštita sačuvanih podataka i podataka koje se prenose kroz mrežu. U mobilnoj mreži, to su privatni podaci korisnika, tehnički podaci korisnika, podaci o uslugama, tehničke informacije o mobilnoj mreži, komunikacija između korisnika, komunikacija između korisnika i mreže, komunikacija korisnika sa udaljenim servisima. Mobilni operateri su ti koji su odgovorni za uspostavljanje sigurnosti u svojoj mreži, što podrazumeva održavanje funkcionalnosti, ali i dodavanje dodatnih funkcionalnosti kao što su firewall, šifrovanje podataka, autentifikacija korisnika, VPN, novi protokoli za enkripciju… Iako su neki problemi mobilnih mreža unapred predviđeni prilikom projektovaja, neki su ispravljeni tek nakon eksploatacije od strane trećih lica, dok su neki još uvek nerešeni. Standardne sigurnosne usluge mobilne mreže su anonimnost i autentifikacija korisnika, zaštita signala u toku prenosa i zaštita korisničkih podataka i komunikacije.

Sigurnost mobilnih mreža se teško može podeliti na segmente, jer je svaki segment usko povezan sa još nekim, i napadi koji se izvršavaju, retko su fokusirani samo na jedan segment mobilne mreže. Ipak postoje celine koje se mogu zasebno razmatrati, ali je vrlo verovatno da će se opisom jedne, zaći u drugu i obrnuto. Stoga, ukoliko se neki od opisa budu ponovili, to je zato što su bitni za razumevanje rada sistema.
Grubo, bezbednost mobilnih mreža se može podeliti na segmente autentifikacije korisnika, zaštite anonimnosti korisnika i poverljivosti podataka i kontrolnih paketa.

Vrste napada koji se najčešće realizuju u mobilnoj mreži su:

- Prisluškivanje
- Lažno predstavljanje
- Oponašanje mreže
- Preuzimanje kontrole nad delom mreže (mrežnim čvorom ili vezom) i izmena
- Brisanje i slanje lažnih signala
- Krađa korisničkih podataka
- Krađa korisničke sesije

Da bi se neki od ovih napada uspešno realizovao, potrebno je razumevanje principa rada mobilnih mreža i kriptografije, kao i znanja iz bezbednosti mreža, programiranja, elektronike. Od opreme je najčešće potrebna bazna stanica ili pilagođen mobilni uređaj, kao i odgovarajući softver koji će potpuno ili samo delimično automatizovati sam napad. Dakle, napad na mobilnu mrežu nije jednostavan, zahteva puno znanja i vrlo je verovatno da će koštati više od benefita koji bi napadač eventualno imao.

Osim napada sa mreže koji mogu da uzrokuju štetu, postoje i fizički napadi, od kojih se mrežni segmenti takođe moraju zaštititi. Fizička zaštita podrazumeva osiguravanje fizičkih položaja mobilne mreže, praćenje pristupa mrežnim segmentima, postavljanje video nadzora, postavljanje alarma, pa čak i proveru prošlosti zaposlenih koji rade za mobilne operatere.

5. OSNOVNI PRINCIPI ZAŠTITE

Zaštita u mobilnoj mreži se bazira na autentifikaciji i anonimnosti korisnika i šifrovanju podataka koji se prenose.

Šifrovanje se vrši kako bi se onemogućilo napadaču da razume komunikaciju između korisnika. Naravno, nije moguće sprečiti napadača da prisluškuje, ali je šifrovanjem moguće sprečiti da napadač razume podatke koje je prikupio.

Anonimnost se ogleda u tome da korisnik mreži nikada ne šalje lične podatke, već ekvivalent u vidu jedinstvenih brojeva. Razlog za to je da se napadaču oteža da identifikuje korisnike koji učestvuju u komunikaciji. SMART kartica u mobilnom uređaju sadrži jedinstveni International Mobile Subscriber Identity (IMSI) broj, koji služi za identifikaciju korisnika. IMSI broj se sastoji od delova koji predstavljaju broj pretplatnika, ime, mrežu i kod države kod koje je pretplaćen. Prilikom uključenja mobilnog uređaja, mobilni uređaj šalje IMSI ili Temporary Mobile Subscriber Identities (TMSI) broj, ukoliko je korisnik prethodno već koristio mrežu, na osnovu kog mreža utvrđuje identitet korisnika. Ukoliko korisnik prethodno nije koristio mobilnu mrežu, prosleđuje IMSI, a dodeljuje mu se TMSI broj , kojim se osigurava da identitet korisnika mobilne mreže ubuduće ostane zaštićen.

Osim IMSI broja, na SMART kartici se nalazi i tajni ključ Kc, koji nikada ne napušta SMART karticu, a nije poznat čak ni mobilnom uređaju. Ovaj ključ je predefinisan i poznat je samo HLR-u i SMART kartici, na koju se upisuje u procesu proizvodnje, osnosno personalizacije. Koristi se samo za autentifikaciju i za generisanje drugih, privremenih ključeva, koji se dalje koriste za autorizaciju, zaštitu integriteta podataka, enkripciju, itd.

Autentifikaciju za glasovne usluge u mobilnoj mreži obavlja MSC, a za podatke SGSN. Kako bi se osiguralo da samo autorizovani korisnici imaju pristup, i koriste servise na koje su pretplaćeni, koristi se autorizacija korisnika putem “challenge-response” mehanizama. Da bi korisnik i mobilna mreža bili sigurni da podaci dolaze od suprotne strane koja je prethodno autentifikovana i da u toku prenosa nisu menjani, mora se obezbediti integritet podataka. Integritet se obezbeđuje heš (hash) algoritmima koji za poruku bilo koje dužine daju string fiksne dužine. Strana koja šalje poruku, uz poruku šalje i heš vrednost poruke, a strana koja primi poruku na osnovu te poruke izračunava heš vrednost i upoređuje je sa heš vrednošću koju je primila uz poruku. Ukoliko su ove vrednosti iste, poruka nije menjana.

Potpuna zaštita bilo koje mreže, pa i mobilne, nije moguća. Zbog ograničenosti resursa (procesorske moći i propusnog opsega), zaštita i funkcionalnost mreže su obrnuto srazmerni, tako da što je mreža zaštićenija, to ima manje prostora za funkcionalnost, što dovodi do problema. Zato su projektanti mreža u obavezi da naprave optimalan balans između funkcionalnosti i zaštite, kako bi mreža bila funkcionalna, ali i dovoljno bezbedna. Dovoljna bezbednost se ogleda u tome da trud i resursi koje napadač uloži budu veći od benefita koje će dobiti ukoliko napad na mrežu bude uspešan, ili da vreme koje bi potrošio za napad bude toliko da informacije koje jednog dana dešifruje u tom trenutku više ne budu validne,

odnosno da nemaju primenu. Time se napadač demotiviše da uopšte pokuša napad.

Bezbednosni algoritmi i procedure koji obezbeđuju sve gore navedene funkcionalnosti biće obrađeni u sledećim poglavljima

5.1. AUTENTIFIKACIJA

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.

U procesu autentifikacije se koriste korisnički podaci (IMEI, IMSI i K), koji su poznati samo mobilnom uređaju, odnosno SMART kartici i HLR-u mobilne mreže. Osnovni princip autentifikacije i anonimnosti je da se ovi podaci nikada ne prenose nezaštićeni kroz mrežu i da se, uopšte, jako retko ili nikada ne prenose.

IMEI broj je prvi stepen autentifikacije mobilnog korisnika i koristi se za identifikaciju, odnosno predstavljanje mobilnoj mreži. To je petnaestocifreni broj koji poseduje svaki mobilni uređaj. Broj se sastoji od tri dela, TAC, SNR i CD.

- TAC je osmocifreni broj koji identifikuje proizvođača mobilnog uređaja i zemlju porekla.
- SNR je šestocifreni serijski broj uređaja, a
- CD je jednocifreni kontrolni broj, koji se koristi za proveru ispravnosti IMEI-a.

U slučaju krađe, operater IMEI broj stavlja u EIR bazu, koja bi trebalo da bude povezana na CEIR (Central EIR), tako da ukradeni mobilni uređaj bude odbijen pri pokušaju autentifikacije u bilo kojoj mobilnoj mreži povezanoj na CEIR.

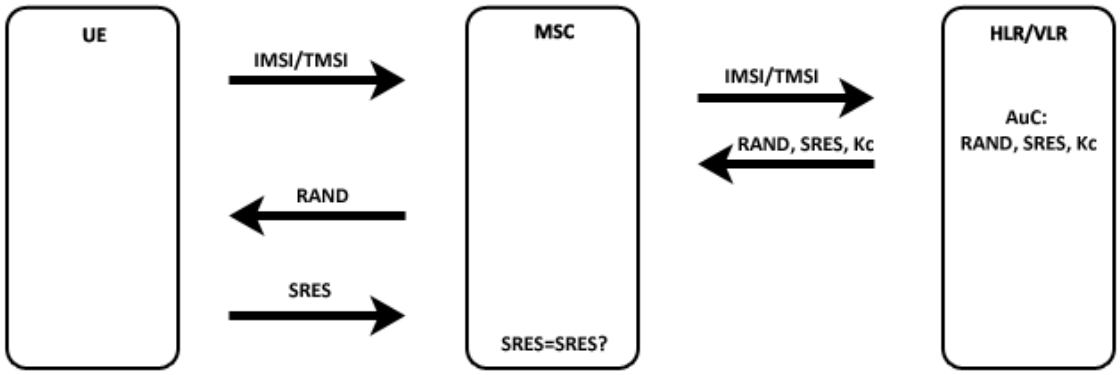
Drugi stepen autentifikacije je SMART kartica koja u sebi sadrži jedinstveni petnaestocifreni IMSI broj. IMSI sadrži informacije o matičnoj mreži pretplatnika i državi u kojoj se matična mreža nalazi. Osim IMSI broja, na SMART kartici je zapisan i jedinstveni ključ K. Kao što je prethodno navedeno, ovaj ključ se na SMART karticu upisuje u procesu personalizacije i koristi se za autentifikaciju i generisanje drugih potrebnih ključeva. K se, kao ni IMSI, ne pamti u telefonu, već se nalazi na SMART kartici i nikada je ne napušta. SMART kartica u sebi ima mikroprocesor koji generiše ključeve za autentifikaciju i kriptovanje. Iako K vrednosti ne može da se pristupi sa mobilnog uređaja, pronađen je način da se ova vrednost kompromituje, što može dovesti do ozbiljnog narušavanja bezbednosti korisnika. Većina napada na mobilnu mrežu ima za cilj upravo krađu podataka za autentifikaciju.

5.1.1. PRINCIPI AUTENTIFIKACIJE U MOBILNIM MREŽAMA

5.1.1.1. PRINCIPI AUTENTIFIKACIJE U GSM

Autentifikacija mobilnog uređaja u mobilnoj mreži mora da se vrši na poseban način jer je medijum za prenos podataka vazduh, pa se pretpostavlja da bilo ko može da prisluškuje komunikaciju. Jednostavno slanje IMSI ili K vrednosti baznoj stanici nije bezbedno i zbog toga je još za mreže druge generacije, GSM, osmišljen poseban princip autentifikacije koji koristi A3 i A8 algoritme.

Autentifikacija započinje tako što mobilni uređaj inicira zahtev za registraciju slanjem TMSI ili IMSI broja. Mobilna mreža, odnosno MSC mu odgovara Authentication Request porukom, koja sadrži 128-bitni RAND broj. Mobilni uređaj kombinuje RAND sa svojim K ključem i A3/A8 algoritmom generiše 32-bitni Signed Response (SRES) broj koji šalje nazad MSC-u. MSC obavlja isti postupak koristeći isti algoritam, korisnički ključ K iz HLR baze i RAND broj prethodno poslat korisniku. Dobijenu vrednost zatim uporedjuje sa SRES brojem dobijenim od korisnika. Ukoliko je rezultat isti, mobilni uređaj je uspešno autentifikovan. Zatim i MSC i mobilni uređaj drugim algoritmom na osnovu RAND broja i ključa K generišu kriptografski ključ Kc, koji se koristi za šifrovanje dalje komunikacije. Ukoliko mreža iz nekog razloga zahteva promenu ovog ključa, ceo proces autentifikacije mora da se ponovi.



Proces autentifikacije u GSM mreži: *UE (User Equipment) – korisnički uređaj, MSC (Mobile Switching Center) – centar za upravljanje pozivima, signalizacijom i povezivanjem novih uređaja, HRL/VLR – centar u čijem sklopu se nalazi AuC (Authentication Center) koji generiše podatke koji se koriste za autentifikaciju korisnika*

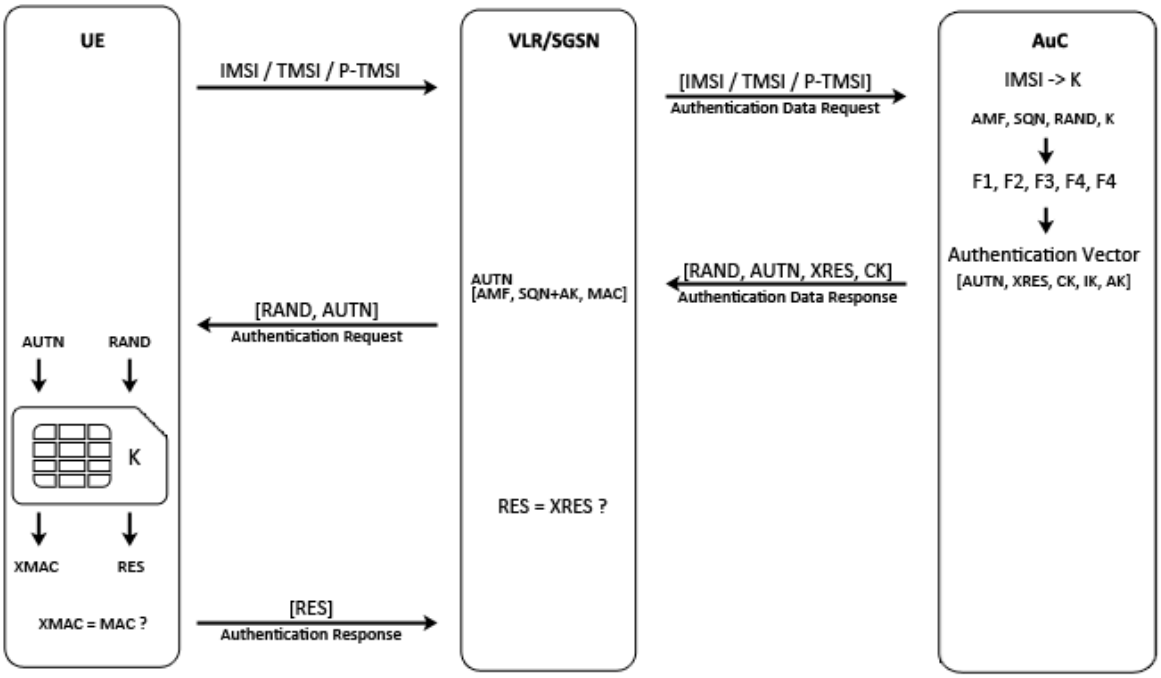
5.1.1.2. PRINCIPI AUTENTIFIKACIJE U UMTS

Principi autentifikacije kod GSM i UMTS mreža se bitno razlikuju. Pre svega zbog obostrane autentifikacije mreže i korisnika kod UMTS sistema i zbog korišćenja dodatnih algoritama zaštite.

Dvosmerna autentifikacija je jedan od bitnijih principa UMTS-a koji značajno povećava bezbednost mobilne mreže, pre svega onemogućava napad lažnom baznom stanicom i dodatno štiti korisnika od krađe identiteta, za razliku od GSM jednosmerne autentifikacije.

I u UMTS mobilnim mrežama autentifikacija počinje tako što se korisnik identifikuje mreži slanjem IMSI, TMSI ili P-TMSI (Packet TMSI) VLR-u ili SGSN-u. VLR/SGSN potom šalje Authentication Data Request AuC-u matične mreže korisnika. Authentication Data Request sadrži primljeni korisnički identitet

(IMSI/TMSI/P-TMSI). Kada AuC primi korisničke podatke, generiše vektor autentifikacije (AV) i šalje ga unutar Authentication Data Response nazad, VLR/SGSN-u. VLR/SGSN zatim šalje korisniku RAND i AUTN. AUTN je deo AV koji služi da se mreža autentifikuje korisniku. Korisnički uređaj prosleđuje podatke USIM kartici. USIM kartica na osnovu dobijenih podataka i ključa K generiše RES i XMAC. Ukoliko se MAC i XMAC ne poklapaju, korisnik šalje Authentication Reject i prekida process autentifikacije. Ukoliko se poklapaju nastavlja se process autentifikacije i korisnik odgovara VLR/SGSN-u tako što šalje RES kao Authentication Response. VLR/SGSN upoređuje RES primljen od korisnika i XRES iz AV. Ukoliko su ove vrednosti iste, korisnik je autentifikovan.



Proces autentifikacije u UMTS mreži: *UE (User Equipment) – korisnički uređaj, AuC (Authentication Center) – centar za autentifikaciju matične mreže korisnika, VLR/SGSN – centar za upravljanje paketima, signalizacijom i autentifikacijom korisnika, IMSI/TMSI/P-TMSI – korisnički identiteti, K – jedinstveni ključ korisnika, AMF (Authentication Management Field), SQN (Sequence Number), RAND (Random Number), F1-5 – jednosmerne funkcije za generisanje vektora autentifikacije, AUTN (Authentication Token) – skup podataka za autentifikaciju mobilne mreže korisniku, MAC/XMAC – vrednosti koje se koriste za autentifikaciju mobilne mreže, RES/XRES – vrednosti koje se koriste za autentifikaciju korisnika*

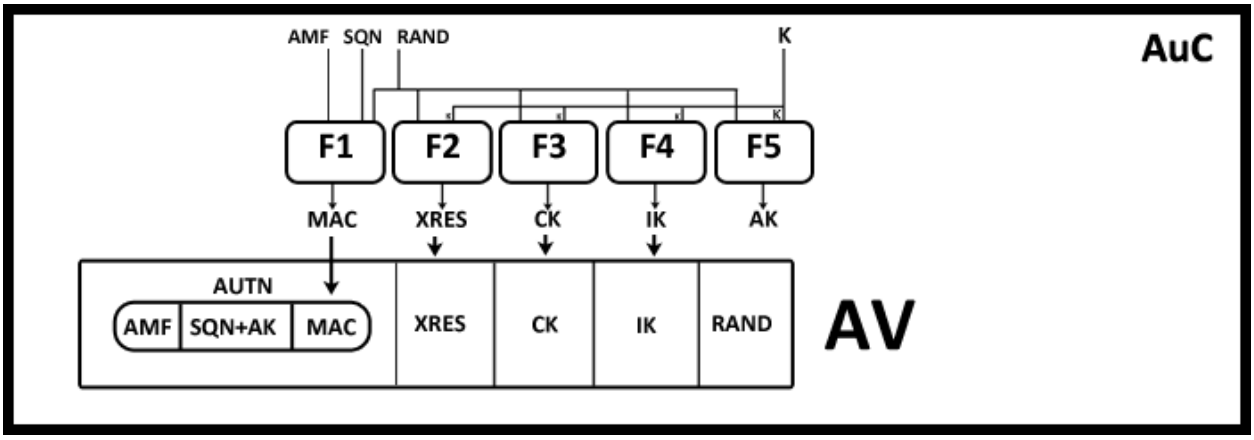
5.1.2. GENERISANJE VEKTORA AUTENTIFIKACIJE

Vektor autentifikacije (AV) je deo mehanizma UMTS mreža koji služi za obostranu autentifikaciju korisnika i mreže. Koristi se kako bi se izbeglo nezaštićeno slanje IMSI vrednosti putem mreže i može se generisati unapred, ili tek nakon zahteva korisnika za autentifikacijom.

Za generisanje parametara AV se koriste jednosmerne funkcije. To su funkcije koje za neki ulazni parameter daju izlazni, ali praktično ne postoji način da se na osnovu izlaznog parametra nađe parameter korišćen na ulazu funkcije. AuC pri generisanju AV koristi pet ovakvih funkcija, F1 za generisanje MAC vrednosti, F2 za generisanje XRES vrednosti, F3 za generisanje Ck ključa, F4, za generisanje Ik ključa, F5 za generisanje Ak (Anonymous Key) ključa. Osim F1, sve ostale imaju iste ulazne parametre, ali zbog specifičnisti svake od njih, za iste parametre daju drugačije izlazne vrednosti. Vrednosti koje oni generišu

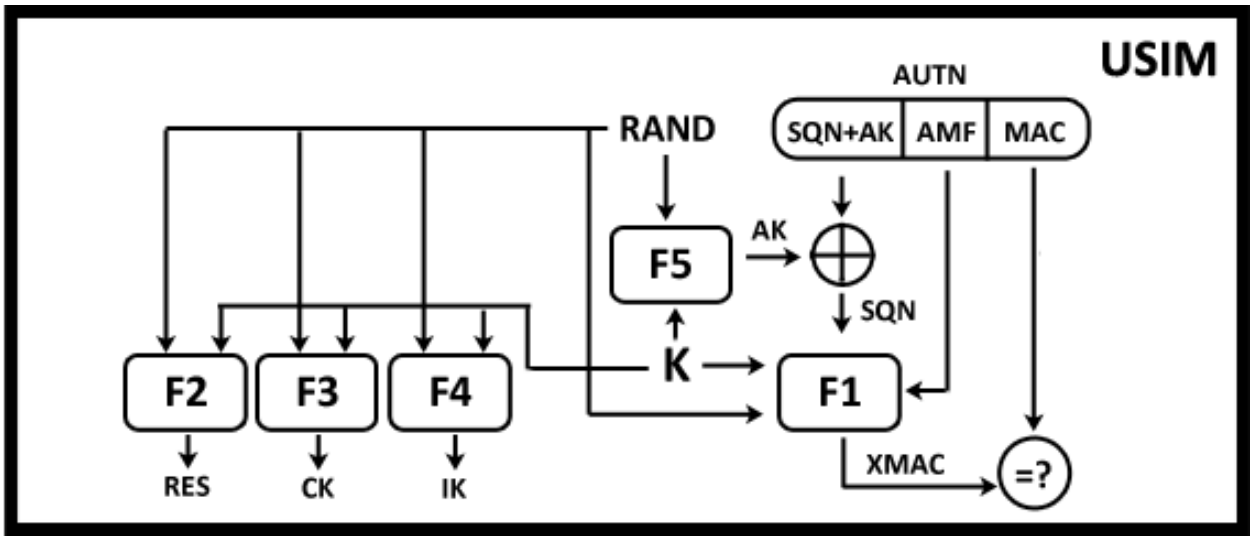
su, respektivno, MAC (64 bita), XRES (32-128 bita), Ck (128 bita), Ik (128 bita), Ak(64 bita).

Da bi se vektor autentičnosti generisao, potrebno je prvo da AuC generiše SQN (broj sekvence dužine 48 bita) i RAND broj (pseudo slučajni broj dužine 28 bita). SQN je bitan za sinhronizaciju autentifikacijskih poruka i sastoji se od SEQ i IND (indeks člana niza u vektoru autentičnosti). F1 algoritam na osnovu K, RAND, SQN i AMF (Authentication token) generiše MAC. Korišćenjem RAND vrednosti i ključa K, F2-5 algoritmi generišu XRES, Ck, Ik, Ak vrednosti. SQN se kriptuje Ak ključem pre prenosa i zajedno sa MAC i AMF vrednostima prenosi se u sklopu AUTN. AUTN se zatim smešta u AV, sa RAND, Ik, Ck i XRES vrednostima. Tako generisan autentifikacijski vektor se prenosi korisniku.



Generisanje Authentication Vector-a: *AuC (Authentication Center) – centar za autentifikaciju, K – tajni ključ korisnika, AMF (Authentication Management Field), SQN (Sequence Number), RAND (Random Number), MAC (Message Authentication Code) – vrednost kojom se mreža autentifikuje korisniku, XRES (Expected Response) – vrednost koja se poredi sa odgovorom korisnika in a osnovu koje se određuje da li je korisnik taj za koga se izdaje, CK (Cipher Key) – privremeni ključ kojim se šifruju poruke u daljoj komunikaciji, IK (Integrity Key), AK (Anonymity Key) – privremeni ključ kojim se šifruje SQN pre slanja AUTN*

Kod korisnika u USIM kartici se izvršavaju isti algoritmi, ali ne istim redom kao u AuC. Nakon što korisnik primi RAND i AUTN, nisu mu poznati ulazni podaci za sve F algoritme koje treba da izvrši. Potrebno je prvo da izvrši F5, kako bi na osnovu RAND i K vrednosti koje su mu poznate generisao ključ AK. AK binarno sabira sa binarnim proizvodom SQN i AK, koji se nalazi u AUTN, čime dobija SQN. Zatim se izvršava F1, kako bi se generisama XMAC vrednost, koja se upoređuje sa MAC vrednošću iz AUTN, čime se mreža autentifikuje korisniku. Nakon toga se izvršavaju F2-4, autentifikacija se nastavlja i ukoliko je uspešna, ključevi CK i IK počinju da se koriste.

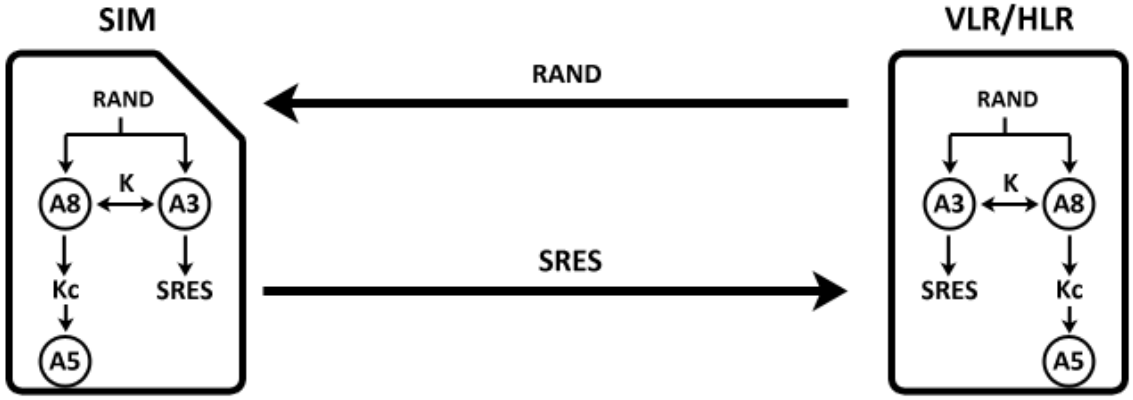


Princip autentifikacije u USIM kartici: *prvo se izvršavaju algoritmi za autentifikaciju mobilne mreže, nakon toga algoritmi za generisanje ključeva*

Svaki autentifikacijski vektor se može koristiti samo jednom kako bi se izbeglo da napadač koji prisluškuje nečiju autentifikaciju može ponovnim korišćenjem istog AV da se identifikuje kao regularan korisnik.

5.1.3. A3/A8 ALGORITAM

Iako se algoritmi A3 i A8 koriste u opisu principa autentifikacije i kriptovanja podataka, ovi algoritmi nisu algoritmi za šifrovanje. Njihova uloga je da na osnovu RAND vrednosti i ključa K generišu SRES vrednost (A3) koja se koristi za autentifikaciju i ključ Kc (A8), koji se koristi za šifrovanje komunikacije ukoliko je autentifikacija uspešna. Oba algoritma se u procesu autentifikacije gotovo istovremeno izvršavaju i nije moguće nezavisno izvršavanje bilo kog od njih, pa ukoliko mreža zatraži od korisnika promenu ključa Kc, potrebno je proći kroz ceo process autentifikacije, iako je korisnik već autentifikovan.



Princip rada A3/A8 algoritama: *SIM – SMART kartica u korisničkom uređaju u kojij se nalazi jedinstveni ključ K, VLR/HLR – baza korisničkih podataka u mreži, RAND – pseudoslučajna sekvenca koja se koristi za za dobijanje SRES vrednosti koja služi za autentifikaciju korisnika, A8 – algoritam za generisanje ključa Kc za šifrovanje podataka, A3 – algoritam za generisanje SRES vrednosti, A5 – algoritam za šifrovanje podataka komunikacije*

Algoritam za šifrovanje koji oni koriste je najčešće COMP128, pa su nedostaci A3/A8 algoritama zapravo nedostaci COMP128 algoritma. Neki od nedostataka su ograničen broj vrednosti koje se koriste za RAND i namerna oslabljenost algoritma pri generisanju Kc ključa, koji umesto 64 bita zapravo ima 54 bita i 10 dodatnih bitova čija je vrednost 0. Time se složenost ključa smanjuje za 2^10, odnosno 1024 puta.

Velika mana algoritama je što se sigurnost bazira na pretpostavci o tajnosti algoritma. Iako princip rada nikada javno nije objavljen, specifikacije su procurele u javnost i ovaj algoritam je razbijen od strane Vagnera i Goldberga. Zbog toga se danas 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 su dobili i Ki vrednost, čime su dokazali da mobilna komunikacija ipak nije dovoljno sigurna, te da je moguće klonirati SIM kartice.

Navedeni propusti omogućavaju neke od napada koji koriste ograničenja ovog algoritma za krađu identiteta korisnika i kasnije lažno predstavljanje.

5.1.3.1. PROBLEMI SA RAND VREDNOŠĆU

U toku autentifikacije mobilnog uređaja, napadač može da se umetne između korisnika i AuC i tako izmeni 128 bitnu RAND vrednost koja se šalje korisniku. Napadač time sprečava korisnika da se autentifikuje, a može da uzrokuje i DOS napad (napad odbijanjem servisa).

Osim toga, RAND vrednost nije sasvim slučajan broj i postoji ograničen broj vrednosti koje može da ima, što napadaču olakšava izvršenje “brute force” napad na RAND i nalaženje jedinstvenog ključa Ki.

5.1.3.2. KRAĐA IDENTITETA

Mobilni uređaji u GSM mrežama za autentifikaciju i identifikaciju koriste IMEI, IMSI i Ki vrednosti, pa je krađa identiteta upravo usmerena ka krađi ovih podataka.

Razlikuju se dve vrste krađe identiteta - aktivna i pasivna.

- Aktivna krađa identiteta podrazumeva da napadač ima prilagođenu baznu stanicu i podstiče korisnika da se poveže na tu baznu stanicu, a zatim od njega traži da se identifikuje slanjem IMSI broja.
- Pasivna krađa identiteta takodje podrazumeva da napadać ima prilagođenu baznu stanicu, ali ovaj put čeka pojavu nove registracije ili rušenje baze podataka, jer se u tim slučajevima od korisnika traži da svoje podatke pošalje u nešifrovanom tekstualnom obliku.

U UMTS mrežama umesto pomenutih vrednosti korisniku se šalju vektori autentifikacije, koji osim za autentifikaciju korisnika služe i za autentifikaciju mobilne mreže, čime se drastično smanjuje uspešnost napada baznim stanicama, a krađa identiteta na ovakav način postaje gotovo nemoguća. Ipak postoji mogućnost da napadač ometa komunikaciju između korisnika i bazne stanice, ali ništa više od toga.

5.1.3.3. LAŽNO PREDSTAVLJANJE KAO OBIČAN KORISNIK

Lažno predstavljanje kao običan korisnik je vrsta napada koja podrazumeva da se napadač predstavlja

mreži kao legitiman krisnik korišćenjem identiteta (podataka autentifikacije) drugog legitimnog korisnika kojeg je prethodno prisluškivao. Napad se može realizovati na nekoliko načina, upotrebom kompromitovanog autentifikacijskog vektora, prisluškivanjem postupka autentifikacije korisnika, otimanjem odlaznih i dolaznih poziva u mrežama bez enkripcije.

5.1.4. NEDOSTACI AUTENTIFIKACIJE

Najveći nedostatak autentifikacije u GSM mrežama je to što ne postoji obostrana autentifikacija, već se samo korisnik autentifikuje mreži, dok se mreža nikada ne autentifikuje korisniku. Zbog toga su i mogući napadi lažnom baznom stanicom, prisluškivanje komunikaije, maskiranje u mobilnu mrežu i "man in the middle" napadi. Ovi napadi iniciraju prividnu nekompatibilnost algoritama za šifrovanje između korisnika i prave mobilne mreže, što za cilj ima nekorišćenje algoritama za šifrovanje.

Takođe je moguć i prekid autentifikacije između korisnika i mreže, tako što napadač koristeći kod prave mreže šalje RAND vrednost korisniku, na šta mu korisnik odgovara misleći da je dobio zahtev za reautentifikaciju od prave mobilne mreže ali napadač odbacuje sve odgovore korisnika i time prekida autentifikaciju korisnika i prave mreže.

TMSI i IMSI podaci o autentifikovanim korisnicima su povezani i čuvaju se u bazi u VLR-u. U slučaju pada baze i gubljenja podataka sa VLR-a, prekida se autentifikacija svih korisnika. Dodatni problem nastaje kada korisnici pokušaju ponovo da se autentifikuju, jer VLR nema nikakve podatke o njima, pa je potrebno da mu proslede IMSI broj u obliku čistog teksta, što predstavlja veliki sigurnosni rizik. Korišćenjem obostrane autentifikacije u UMTS mobilnim mrežama svi ovi nedostaci su ispravljeni.

Više o napadima na ovaj sigurnosni propust nalazi se u odeljku "Maskiranje u mobilnu mrežu".

5.2. ANONIMNOST

Anonimnost korisnika u mobilnoj mreži podrazumeva da se identitet korisnika nikada ne otkriva, odnosno da se nezaštićene i nešifrovane korisničke informacije što ređe ili nikada ne šalju kroz mrežu. Razvijeni su razni mehanizmi za zaštitu anonimnosti.

Umesto da se između mreže i korisnika šalje nekriptovani IMSI, šalje se TMSI broj, koji je jedinstven za mobilni uređaj u jednom području. Mobilna mreža mobilnom uređaju dodeljuje TMSI. Promenom lokacije, moguće je promeniti i TMSI. Prilikom promene, TMSI broj se šifrovan šalje mobilnom uređaju. TMSI se čuva u telefonu, ili na SMART kartici, ali za razliku od IMSI broja, nije fabrički dodeljen SMART kartici.

U slučaju promene lokacije, kada mobilni korisnik pređe sa jednog VLR-a na novi VLR, novi VLR traži informacije o korisniku od HLR-a korisnikove matične mreže, njegov K i IMSI. Prilikom prenosa ovih informacija kroz mrežu, a posebno ukoliko je mobilni uređaj u romingu, postoji izvestan rizik od presretanja. Takođe, može doći do preopterećenja HLR-a ukoliko se pri svakoj autentifikaciji od njega traže podaci o korisniku. Zbog toga se umesto IMSI i K u UMTS mrežama između starog i novog VLR-a za svaki traženi IMSI prosleđuju autentifikacijski vektori.

Dodatni doprinos sigurnosti ima i često menjanje frekvencija prilikom prenosa (Frequency Hopping). U GSM mreži, frekvencija se menja 217 puta u sekundi, odnosno na svakih 4.615 ms. Promena frekvencija

zavisi od HSN (Hopping Sequence Number) i MAIO (Mobile Allocation Index Offset) parametara. HSN određuje da li se frekvencije menjaju ciklično ili ne, dok MAIO određuje inicijalnu frekvenciju koja se koristi za frekvencijsko skakanje.

Frekvencijsko skakanje ne samo da otežava napadaču da prisluškuje komunikaciju, jer se komunikacija vrši na više od jednog kanala, nego i smanjuje eventualnu interferenciju i utiče na odnos signala i šuma u prenosu. Ukoliko se na nekoj frekvenciji pojavi šum ili postoji interferencija sa istim kanalom, koristiće se druga frekvencija. Takođe, ako napadač želi da prisluškuje, morao bi da prisluškuje ceo spektar kanala.

U slučaju kada bi napadač mogao da razume poruke koje se šalju, mogao bi iz tih poruka da pročita koja će se sledeća frekvencija koristiti. Ovaj eventualni propust se rešava korišćenjem inicijalnog kriptovanog kanala pri određivanju kanala za prenos govora ili podataka. Ograničavajuća okolnost je da bazne stanice imaju ograničen broj frekvencija koje koriste.

5.3. ZAŠTITA PODATAKA

Poverljivost podataka zauzima važno mesto u mobilnim komunikacijama i mobilnom sistema. Stoga je šifrovanje podataka veoma bitno zbog zaštite podataka i signalizacionih poruka koje se prenose. U GSM i UMTS sistemima se koristi simetrična kripcija, odnosno 128-bitni simetrični ključevi, Kc vrednosti, koji su poznati samo SMART kartici i HLR u mobilnoj mreži. Bitno je da se ovi ključevi ne prenose putem mreže, kako bi podaci u slučaju da se komunikacija presretne, bili nečitljivi za napadača. Kao što je već rečeno, u slučaju da je Kc kompromitovan, mora se generisati novi ključ, a s obzirom na to da se algoritmi A3 (generisanje SRES vrednosti) i A8 (generisanje Kc) istovremeno izvršavaju na SIM kartici, ceo proces autentifikacije bi morao da se odradi ponovo.

5.3.1. ALGORITMI ZA KRIPTOVANJE KOMUNIKACIJE - A5

Algoritam A5 služi za šifrovanje komunikacije između korisnika i mreže u realnom vremenu. Postoji nekoliko verzija algoritma A5 koji se koriste u mobilnim mrežama, zavisno od zahtevnosti, generacije mobilne mreže ili tržišta na kome se primenjuje, ali se koriste samo oni koji su podržani od strane mobilnih uređaja. Dva osnovna algoritma su A5/1 i A5/2, koji su definisani GSM standardom, GAE3, koji je uveden za GPRS kripciju i A5/3 predviđen za 3G (UMTS). A5/1 se koristi u Americi, a A5/2 je namerno oslabljena verzija A5 algoritma namenjena manje razvijenim regionima. A5/3 je najnovija verzija razvijena od strane 3GPP (The 3rd Generation Partnership Project) i kao i GAE3, baziran je na Kasumi algoritmu. Mobilna mreža može koristiti do 7 algoritama za šifrovanje komunikacije, ali ne mora ni jedan.

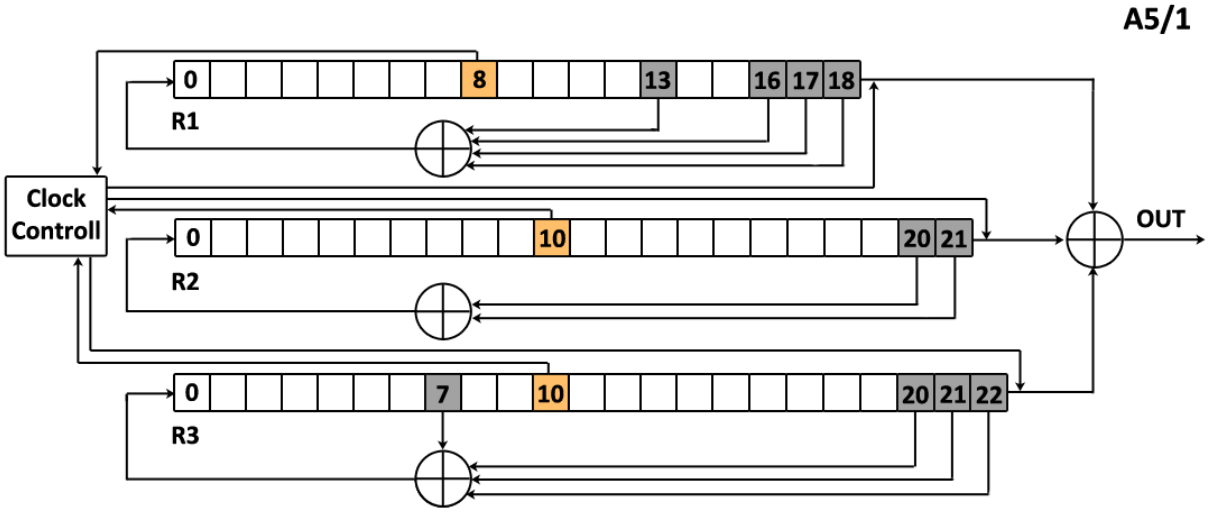
Nakon autentifikacije, mobilna mreža može da inicira šifrovanje podataka i šalje korisnicima podržane algoritme šifrovanja. Na ovu poruku korisnici odgovaraju “classmark” porukom, kojom se definišu mogućnosti mobilnog uređaja i podržani algoritmi šifrovanja.

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.

A5/1 je baziran na LFSR (Linear Feedback Shift Register) blokovima nejednake dužine, 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 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. A5/1 u tu svrhu koristi bitove LFSR polja za kontrolu kloka. Klok bitovi u ovom slučaju određuju koji će se od registara koristiti za generisanje izlaza.



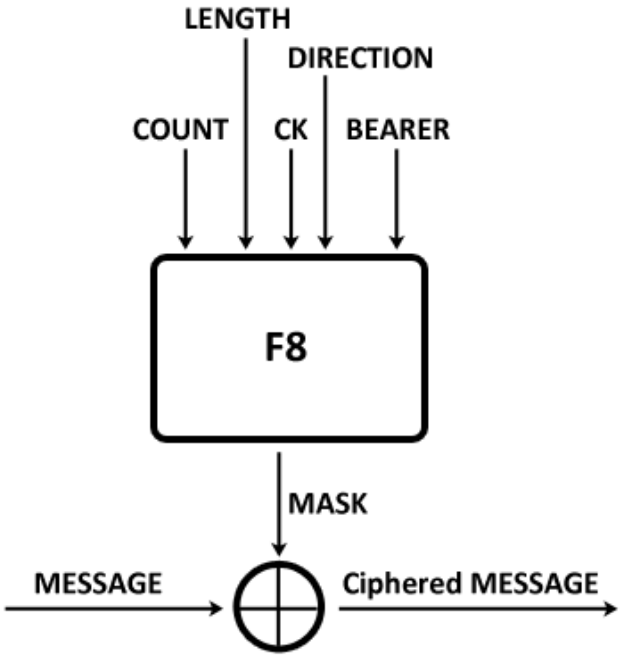
A5/1: *Sekvencijalni lgoritam za šifrovanje komunikacije u GSM mrežama, radi po principu generisanja maske, kojom se XOR funkcijom šifruju podaci koji se šalju . R1, R2, R3 su LFSR registri nejednakih dužina. Klok bitovi određuju koji od registrar će učestvovati u generisanju izlaza i-tog koraka. Kontrola kloka se vrši po principu većine – ukoliko dva registra imaju iste klok bitove, ta dva registra će učestvovati u generisanju izlaza. Ukoliko sva tri registra imaju iste bitove kloka, sva tri registra učestvuju u generisanju izlaza.*

A5/3 je još unapređeniji, pa osim bitova LFSR blokova, za generisanje ulaza, odnosno izlaza kao dodatnu sekvencu koristi klok TDMA okvira. TDMA okvir je promenjivi ulazni parameter koji u ovom slučaju odlučuje koji će od LFSR blokova učestvovati u izračunavanju izlaza i dodatno povećava bezbednost algoritma. A5/3 je inače baziran na KASUMI algoritmu.

5.3.2. ALGORITMI ZA KRIPTOVANJE KOMUNIKACIJE - F8

UMTS za šifrovanje podataka koristi sekvencijalni algoritam zbog njegove brzine i mogućnosti da masku kojom se podaci šifruju generiše pre nego što su podaci poznati. Osnova algoritma za šifrovanje je F8 funkcija, koja osim 128 bitnog ključa za šifrovanje CK koristi i dodatne parametre: DIRECTION, COUNT-C, BEARER, LENGTH.

Maska koju F8 generiše se XOR funkcijom dodaje bloku podataka koji se šifruje i tako šifrovani podaci se šalju drugoj strani. Algoritam za šifrovanje je baziran na KASUMI algoritmu.



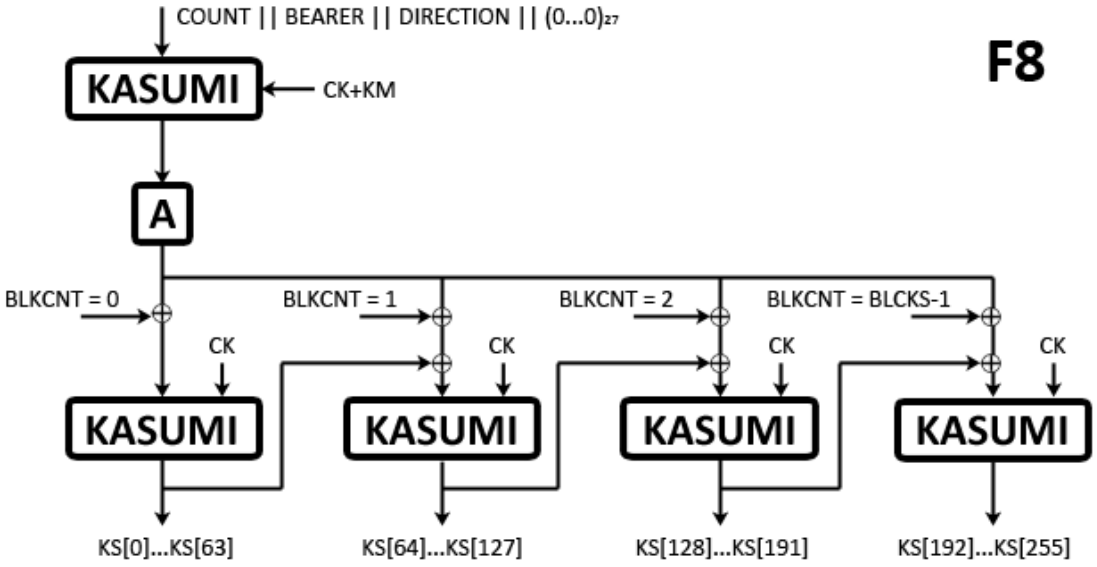
Princip rada sekvencijalnog F8 algoritma: *F8 na ulazu ima više različitih elemenata kako bi se što više smanjila mogućnost da se dva puta ponove iste ulazne vrednosti, što bi uzrokovalo generisanje iste maske više od jednog puta, što je ozbiljan bezbednosni propust.*

Razlog za čak pet različitih ulaznih vrednosti je smanjenje mogućnosti da se ista maska ponovi dva puta, što bi, ukoliko bi se desilo, dodatno olakšalo napade kriptoanalizom. Za primer, ukoliko se dve 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 meri skraćuje i olakšava napad. Ukoliko je ceo niz poruka šifrovan istom vrednošću, utoliko je napad na takve poruke još lakši, a jednom otkrivena maska, ukoliko nije menjana, napadaču bi poslužila da razume celokupnu komunikaciju. Zato je bitno da se u toku komunikacije maska ne ponovi, i za to služe navedene ulazne vrednosti:

- **CK:** Jedinstveni 128-bitni ključ za šifrovanje generisan u procesu autentifikacije
- **COUNT:** 32-bitni broj sekvence poruke koja se šalje, svaka strana povećava count za 2 svaki put kada se poruka pošalje. Sastoji se najčešće od lokalnog i globalnog brojača. Kada lokalni brojač obrne ceo krug, globalni se poveća za jedan. Zbog broja poruka koje se prenose, može se desiti da i globalni brojač istroši sve vrednosti, pa se zbog toga vrednosti svih brojača setuju na 0 svaki put kada se generiše ključ CK.
- **BEARER:** 5-bitni broj kojim je obeležen svaki nosilac radio komunikacije u mobilnoj mreži. Svaki bearer ima zasebne COUNT vrednosti.
- **DIRECTION:** Bit kojim se označava smer komunikacije, uplink ili downlink.
- **LENGTH:** Broj koji označava dužinu poruke koja se kriptuje. Ovaj broj utiče samo na dužinu maske koja će biti generisana.

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 bitova prethodnog bloka (osim prvog bloka za koji prethodni blok ne postoji). Registar A kao ulazne vrednosti dobija inicijalni vektor koji je sastavljen konkatenacijom vrednosti COUNT, BEARER, DIRECTION i sekvence od 28 bitova 0, enkriptovan KASUMI algoritmom koji kao ključ koristi ključ CK izmenjen modifikatorom ključa

KM, koji je zapravo binarni oktet 01010101 ponovljen 16 puta. Ova izmena ulaznih podataka vrši se kako bi se smanjila predvidivost 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, jer se ulazni podaci menjaju pre generisanja izlaza.

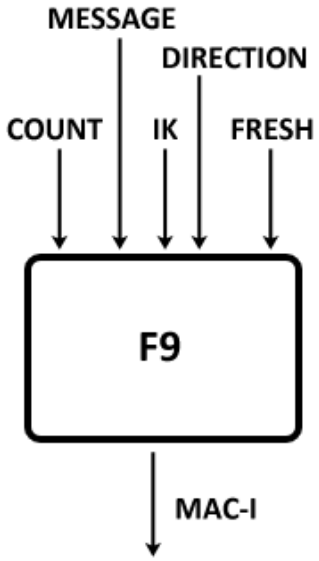


Dijagram F8 algoritma: *COUNT – broj sekvence poruke; BEARER – broj nosioca komunikacije; DIRECTION – smer komunikacije; CK – ključ za šifrovanje podataka; KM – modifikator ključa za šifrovanje dobijen ponavljanjem sekvence 01010101 šesnaest puta; BLCKNT – brojač bloka; BLCKS – ukupan broj blokova; A – registar za čuvanje*

5.3.3. ALGORITMI ZA ZAŠTITU INTEGRITETA PODATAKA

UMTS mreže dodatno osiguravaju integritet paketa potpisujući ih jednom vrstom digitalnog potpisa, odnosno dodavanjem 32-bitnog I-MAC jedinstvenog za određenu mobilnu stanicu. To je zapravo heš vrednost generisana na osnovu poruke i drugih ulaznih vrednosti. Ukoliko bi u toku prenosa došlo do izmene bilo koje od ulaznih vrednosti ili same poruke, I-MAC takve poruke se ne bi poklapao sa I-MAC-om početne poruke i primalc bi znao da je poruka menjana u toku izmene.

Za generisanje digitalnog potpisa za integritet paketa u UMTS mrežama se koristi F9 algoritam. Ulazne vrednosti su IK ključ identiteta, koji se generiše kada i CK i prenosi zajedno sa njim, DIRECTION oznaka smera komunikacije, COUNT-I broj sekvence poruke, FRESH slučajni broj jedinstven za svaku pojedinačnu konekciju i poruka koja se šalje. FRESH se koristi za kontrolu slanja paketa za vreme konekcije na samo tu konekciju. U paru sa COUNT vrednošću ograničava slanje kontrolnih paketa na jednu konekciju i to samo u poretku tako da COUNT vrednost bude inkrementalna. Dakle COUNT vrednost sprečava slanje poruka van redosleda, a FRESH sprečava ponovno slanje istih poruka u nekoj drugoj konekciji, čime se sprečava napad prisluškivanjem i ponovnim slanjem kontrolnih poruka.



Algoritam za za zaštitu integriteta podataka: *Služi za generisanje heša koji se zajedno sa porukom šalje drugoj strani. Druga strana na osnovu istih ulaznih podataka i poruke izvršava isti algoritam i upoređuje dobijeni sa primljenim hešom. Ukoliko su isti, poruka nije menjana u toku prenosa, što je garancija da je pošiljalac poznat.*

5.3.4. PROBLEMI SA ALGORITMIMA ZA KRIPTOVANJE

Algoritmi A5/1 i A5/2 su kompromitovani vrlo brzo nakon implementacije, dok je oslabljena verzija A5/3 sa 5 umesto 8 iteracija KASUMI algoritma i bez FL funkcija u laboratorijskim uslovima kompromitovan pre nego što je A5/3 implementiran. Potpun A5/3 algoritam, ipak, nikada nije kompromitovan van laboratorije. 2003. je prvi put objavljeno da su A5/1 i A5/2 algoritmi kompromitovani, a napad je izvršen tako što je telefonima kao algoritam za šifrovanje predložen slabiji A5/2, za koji se koristi isti ključ kao i za A5/1, pa je faktički razbijanjem A5/2 razbijen i A5/1 algoritam.

2007. je započet prvi komercijalni projekat pravljenja tabela za razbijanje A5/1 kripcije, COPACOBANA. Nakon toga su usledili novi projekti i najnoviji je projekat sa rainbow tabelama veličine 2TB, koje mogu da se preuzmu i sa interneta, preko torenta.

Još jedan nedostatak algoritama za kriptovanje u GSM mobilnim mrežama je što se kriptovanje vrši tek nakon dodavanja Forward Error Correction (FEC) bitova za kontrolu greške, čime se olakšava kriptoanaliza podataka, jer su FEC bitovi poznati napadaču. Ovaj propust je u UMTS mobilnim mrežama ispravljen, pa se šifrovanje podataka vrši pre dodavanja FEC bitova.

5.3.4.1. MASKIRANJE U MOBILNU MREŽU

Jedna od mogućih vrsta napada na algoritme za šifrovanje, je podsticanje mreže i korisnika na nekorišćenje ovih algoritama. Realizuje se tako što se napadač korisniku predstavlja kao mobilna mreža na koju bi trebalo da se poveže, ili je napadač samo posrednik koji navodi mrežu i korisnika da koriste različite algoritme za šifrovanje, što dovodi do prekida šifrovanja saobraćaja između mreže i korisnika.

U prvom slučaju, korišćenjem lažne bazne stanice, napadač podstiče korisnika da se prijavi na tu lažnu mrežu i nudi mu algoritme za šifrovanje koje korisnik ne podržava, pa se komunikacija nastavlja bez korišćenja šifrovanja.

Drugi slučaj ima sličan scenario, koji se razlikuje u tome da napadač pravi nesporazum između mreže i korisnika, uzrokujući prividnu nekompatibilnost u algoritmima za šifrovanje, što kao posledicu ima nekorišćenje enkripcije.

Maskiranje u mobilnu mrežu takođe može da se iskoristi i za krađu korisničkog identiteta i lažno predstavljanje.

Napadač bi mogao da sazna IMSI korisnika time što bi se maskirao u baznu stanicu i čekao da korisnik pošalje svoj IMSI broj mreži. Drugi način je da korisniku pošalje “Identity Request” poruku, čime bi ga podstakao da se identifikuje lažnoj mreži i pošalje IMSI u tekstualnom obliku. Kada sazna korisnikov IMSI, napadač može da poveže svoj IMSI sa korisničkim TMSI brojem u pravoj mreži i neovlašćeno koristi usluge pravog korisnika.

Dalje, napadač može korisniku da pošalje “Authentification Request” poruku i RAND vrednost, na šta mu korisnik odgovara “Authentification Response” porukom sa SRES vrednošću. Napadač može ovaj korak da ponovi dovoljno puta da iz primljenih podataka, razbijanjem algoritma, dobije Ki vrednost korisnika. Time napadač dobija pun pristup svim komunikacijama mobilnog korisnika, odnosno, može da se autentifikuje i koristi mobilnu mrežu kao ovlašćeni korisnik, prisluškuje i razume mobilnu komunikaciju. U UMTS mrežama ovo nije moguće zbog korišćenja obostrane autentifikacije, pa ukoliko korisnik ne prepozna mrežu, prekida autentifikaciju.

5.3.5. PROBLEMI SA SMS SISTEMOM

SMS je usluga slanja kratkih tekstualnih poruka drugim korisnicima. Poruke koje se šalju se ne šifruju između krajnjih korisnika, već samo između mobilnog uređaja i bazne stanice A5 algoritmom, a kroz ostatak sistema se prenose u obliku čistog teksta, tako da svako ko ima pristup sistemu može da čita poruke korisnika.

Osim što je moguće prisluškivati ovaj način komunikacije, moguće je i menjati polja SMS zaglavlja. Tako napadač može da izmeni polje adrese inicijatora i da se predstavlja kao neki drugi korisnik.

Ono što zabrinjava je mobilno bankarstvo, koje je danas veoma zastupljeno u celom svetu. Prva ideja je bila da se SMS koristi isključivo u svrhe obaveštavanja korisnika i prenosa podataka koji nisu poverljivi, ali je kasnije servis evoluirao i počela je upotreba u verifikaciji transakcija.

Neke banke u Srbiji koriste USSD (Ustructured Supplementary Data) za prenos podataka. Za razliku od SMS, na ovaj način mobilni uređaj uspostavlja konekciju sa udaljenim serverom sa USSD podrškom i konekcija ostaje otvorena dok korisnik ne obavi transakciju. Korisnik, dakle, šalje svoj pin kod USSD serveru, u obliku čistog teksta, tako da mobilni operater ili bilo ko drugi ko je u mogućosti da prisluškuje komunikaciju, ima uvid u poverljive podatke korisnika, pin kod, stanje na računu, lične podatke.

Najveća mana ovog sistema je upravo to što prilikom projektovanja GSM arhitekture, nije predviđeno šifrovanje tekstualnih poruka koje se prenose putem mobilne mreže.

6. KASUMI ALGORITAM

6.1. NASTANAK KASUMI ALGORITMA

Poznati japanski naučnik i kriptograf Mitsuru Matsui, proučavanjem diferencijalne kriptoanalize dobio je ideju za novu tehniku testiranja kriptografskih blok algoritama - linearnu kriptoanalizu. Kako su mnogi algoritmi bili podložni napadima diferencijalnom i linearnom kriptoanalizom, Matsui je osmislio dva nova 64-bitna blok algoritam koji koriste 128-bitni ključ, a koji su bili otporni na ovakve napade - MISTY1 i MISTY2.

U to vreme 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 vreme za koje je bilo potrebno definisati algoritme za UMTS, a modifikovanje postojećeg algoritma bi oduzelo manje vremena od definisanja novog, čime bi se skratilo vreme 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. stvoreni su KASUMI algoritam, funkcija F8 za sekvencijalno šifrovanje i F9 za potvrdu integriteta podataka.
Nakon toga su usledili testovi bezbednosti KASUMI algoritma, a testovi su bili definisani tako da upoređuju ulazne i izlazne parametre funkcija na osnovu kojih se donose određeni zaključci. Ni jedan napad na KASUMI algoritam u sklopu mobilne UMTS mreže nije bio uspešan.

6.2. STRUKTURA KASUMI ALGORITMA

KASUMI u prevodu sa japanskog znači maglovit, nejasan (eng. FOGGY). Iako baziran na MISTY1, KASUMI je modifikovan u tom pogledu da se što više olakša hardverska implementacija, a povećanje vremena izvršavanja, odnosno smanjenje brzine algoritma, kompenzovano je izbacivanjem pojedinih funkcija koje nisu značajno uticale na bezbednost algoritma. Smanjenje bezbednosti, pak, kompenzovano je dodavanjem još jedne iteracije S7 funkcije, što je delimično povećalo hardver, ali značajno povećalo bezbednost 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 redosled

menja 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 dve zasnovana na Feistelovoj strukturi, sa dve 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.

6.3. 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 dele 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 $R_1=L_0$ i $L_1=R_0 \oplus f_i(L_0,RK_1)$, gde je RK_1 skup ključeva KL, KO, KI, koji se koriste unutar FL, FO i FI funkcija. Tako će izlaz i-te iteracije biti $R_i=L_{i-1}$ i $L_i=R_{i-1} \oplus f_i(L_{i-1},RK_i)$, odnosno izlaz algoritma se dobija konkatenacijom izlaznih blokova $R_8=L_7$ i $L_8=R_7 \oplus f_8(L_7,RK_8)$.

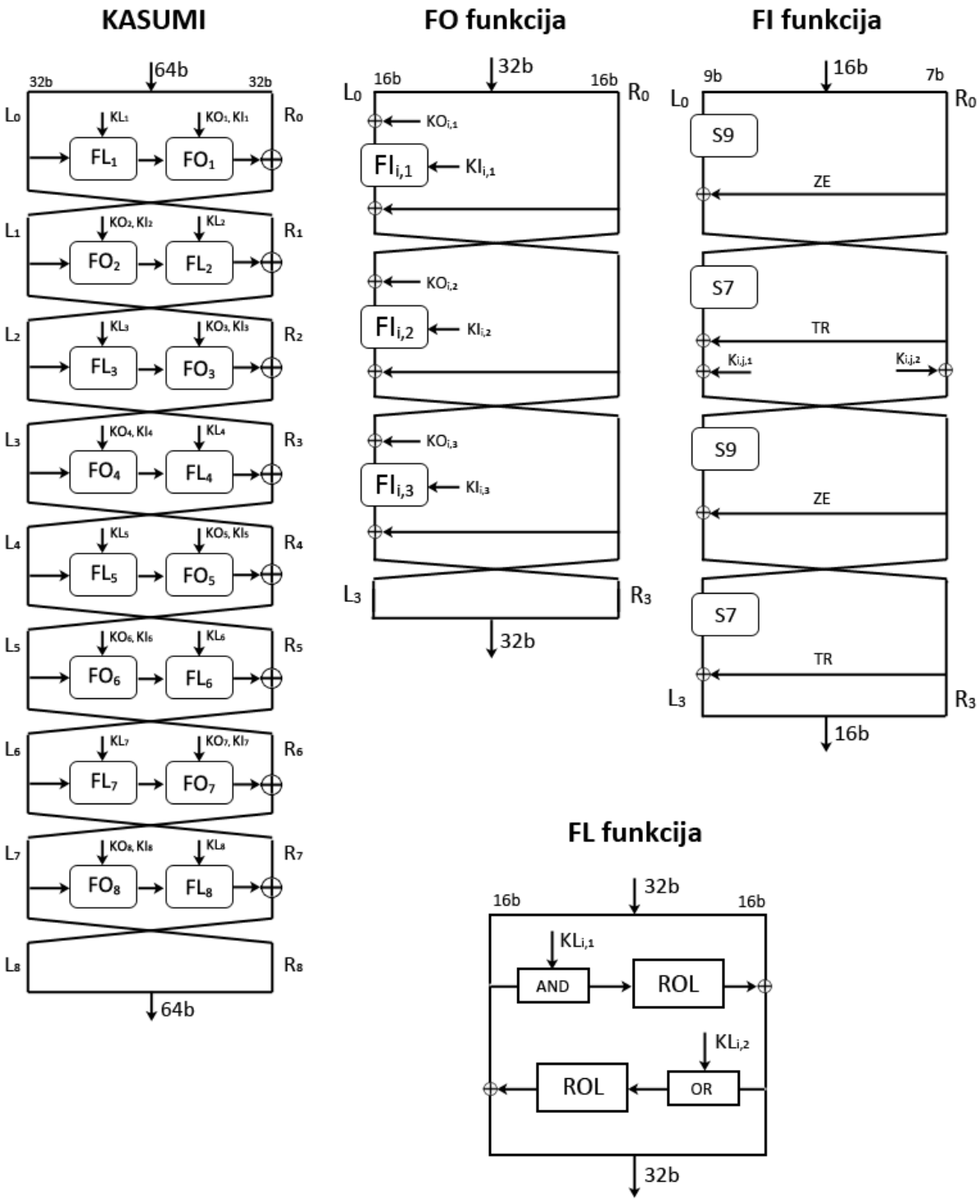
Funkcija f-i prima 32-bitni ulaz i daje 32-bitni izlaz uz pomoć RK_i ključa koji objedinjuje ključeve potrebne za FL i FO funkcije. F funkcija ima dve različite forme, parnu i neparnu. Razlika je u redosledu izvršavanja FL i FO funkcija. U neparnim iteracijama se prvo izvršava FL funkcija, a u parnim 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:

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


KASUMI
FO funkcija
FI funkcija
FL funkcija
64b
32b
FL1
FO1
FO2
FL2
FL3
FO3
FO4
FL4
FL5
FO5
FO6
FL6
FL7
FO7
FO8
FL8
16b
FIi,1
FIi,2
FIi,3
9b
7b
S9
S7
ZE
TR
AND
ROL
OR

6.3.1. FUNKCIJA FL

FL funkcija za 32-bitni ulaz, koristeći 32-bitni ključ KL daje 32-bitni izlaz. Kako se ulazni podaci dele na dva jednaka 16-bitna bloka I=L || R, i ključ KL deli na dva jednaka dela $KL=KL_{i,1} || KL_{i,2}$.

Izlaz jedne iteracije FL funkcije za levi deo funkcije bi bio:
$L'=L \oplus ROL(R' \cup KL_{i,2})$

dok bi desni deo bio:

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

gde je ROL levi ciklični pomeraj bloka za jedan bit, ∪ logička opetacija "ili", a ∩ logička operacija "i".

Uloga FL funkcije u KASUMI algoritmu je da oteža praćenje pojedinačnih bitova kroz iteracije algoritma

6.3.2. FUNKCIJA FO

FO funkcija koristi 32-bitni ulaz podataka i dva 48-bitna ključa, KO i KI. Podaci sa ulaza se dele na dva 16-bitna bloka, I=L0 || R0, dok se ključevi dele na tri dela:

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

i

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

Izlaz svake od tri iteracija bi bio:

$R_j=FI_{i,j}(L_{j-1} \oplus KO_{i,j}, KI_{i,j}) \oplus R_{j-1}$ za desni deo funkcije,

odnosno

$L_j=R_{j-i}$ za levi deo funkcije,

Gde i označava i-ti blok FO funkcije, a j označava iteraciju unutar bloka.

6.3.3. FUNKCIJA FI

FI funkcija kao ulaz ima 16-bitni blok podataka I i 16-bitni ključ $KI_{i,j}$. Ulazni podaci se dele na dva nejednaka bloka od 7 i 9 bitova, $KI_{i,i}=KI_{i,1} || KI_{i,2}$, koji služe kao ulazni podaci S funkcija - $KI_{i,1}$ za S7, a $KI_{i,2}$ za S9. Razlog za ovakvu podelu bitova je taj što bijektivne funkcije neparne dimenzije imaju manju linearnu predvidivost, 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 dele 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 ZE od 7-bitnog bloka daje 9-bitni dodavanjem dve nule sa leve strane, dok TR od 9-bitnog bloka daje 7-bitni odsecanjem dva skroz leva bita. Treba napomenuti da se bit najveće važnosti nalazi skroz levo.

Izlaz FI funkcije po unutrašnjim iteracijama je sledeći:

$L_1 = R_0$ $R_1 = S9[L_0] \oplus ZE(R_0)$

$L_2 = R_1 \oplus KI_{i,j,2}$ $R_2 = S7[L_1] \oplus TR(R_1) \oplus KI_{i,j,1}$

$L_3 = R_2$ $R_3 = S9[L_2] \oplus ZE(R_2)$

$L_4 = S7[L_3] \oplus TR(R_3)$ $R_4 = R_3$

6.3.4. S FUNKCIJE

Osnovne funkcije, takozvani S-BOX-ovi kao ulaz primaju sedam, odnosno devet bitova i po već opisanom principu se dužina izlaznih blokova obrađuje da bude ulaz sledećoj S funkciji.

6.3.4.1. FUNKCIJA S7

Funkcija S7 za 7-bitni ulaz daje 7-bitni izlaz, tako što se prvo ulazni blok podataka dužine sedam bita deli na sledeći način:

$x = x_6 \,||\, x_5 \,||\, x_4 \,||\, x_3 \,||\, x_2 \,||\, x_1 \,||\, x_0$

Logika kojom S7 funkcija daje izlaz y na osnovu ulaza x je sledeća:

$y_0 = x_1x_3 \oplus x_4 \oplus x_0x_1x_4 \oplus x_5 \oplus x_2x_5 \oplus x_3x_4x_5 \oplus x_6 \oplus x_0x_6 \oplus x_1x_6 \oplus x_3x_6 \oplus x_2x_4x_6 \oplus x_1x_5x_6 \oplus x_4x_5x_6$

$y_1 = x_0x_1 \oplus x_0x_4 \oplus x_2x_4 \oplus x_5 \oplus x_1x_2x_5 \oplus x_0x_3x_5 \oplus x_6 \oplus x_0x_2x_6 \oplus x_3x_6 \oplus x_4x_5x_6 \oplus 1$

$y_2 = x_0 \oplus x_0x_3 \oplus x_2x_3 \oplus x_1x_2x_4 \oplus x_0x_3x_4 \oplus x_1x_5 \oplus x_0x_2x_5 \oplus x_0x_6 \oplus x_0x_1x_6 \oplus x_2x_6 \oplus x_4x_6 \oplus 1$

$y_3 = x_1 \oplus x_0x_1x_2 \oplus x_1x_4 \oplus x_3x_4 \oplus x_0x_5 \oplus x_0x_1x_5 \oplus x_2x_3x_5 \oplus x_1x_4x_5 \oplus x_2x_6 \oplus x_1x_3x_6$

$y_4 = x_0x_2 \oplus x_3 \oplus x_1x_3 \oplus x_1x_4 \oplus x_0x_1x_4 \oplus x_2x_3x_4 \oplus x_0x_5 \oplus x_1x_3x_5 \oplus x_0x_4x_5 \oplus x_1x_6 \oplus x_3x_6 \oplus x_0x_3x_6 \oplus x_5x_6 \oplus 1$

$y_5 = x_2 \oplus x_0x_2 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_0x_2x_4 \oplus x_0x_5 \oplus x_2x_5 \oplus x_4x_5 \oplus x_1x_6 \oplus x_1x_2x_6 \oplus x_0x_3x_6 \oplus x_3x_4x_6 \oplus x_2x_5x_6 \oplus 1$

$y_6 = x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_4 \oplus x_1x_5 \oplus x_3x_5 \oplus x_6 \oplus x_0x_1x_6 \oplus x_2x_3x_6 \oplus x_1x_4x_6 \oplus x_0x_5x_6$

Izlaz funkcije je jednak:

$y = y_6 \,||\, y_5 \,||\, y_4 \,||\, y_3 \,||\, y_2 \,||\, y_1 \,||\, y_0$

Na ovaj način se formira tablica vrednosti S7 funkcije koja se sastoji od 128 pozicija (2^7=128). Svaki pozicija se može predstaviti u binarnom obliku sa sedam bitova - prva je 0 (0000000), a poslednja 127 (1111111).

Tablica vrednosti S7 funkcije za sve pozicije izgleda ovako:

54	50	62	56	22	34	94	96	38	6	63	93	2	18	123	33
55	113	39	114	21	67	65	12	47	73	46	27	25	111	124	81
53	9	121	79	52	60	58	48	101	127	40	120	104	70	71	43
20	122	72	61	23	109	13	100	77	1	16	7	82	10	105	98
117	116	76	11	89	106	0	125	118	99	94	77	30	57	118	95
112	51	17	5	95	14	90	84	91	8	35	103	32	97	28	66
102	31	26	45	75	4	85	92	37	74	88	57	68	29	123	36
64	107	108	24	110	83	36	78	42	19	15	41	88	119	59	3

Tablica vrednosti S7 funkcije

PRIMER:

U slučaju da S7 funkcija kao ulazni podatak dobije broj 44, čiji je binarni oblik 0101100, 7-bitni ulazni blok će biti podeljen po bitovima tako da je bit najveće važnosti skroz levo. Shodno tome, vrednosti niza ulaznih vrednosti x_i biće:

$x_0 = 0$ $x_1 = 0$ $x_2 = 1$ $x_3 = 1$ $x_4 = 0$ $x_5 = 1$ $x_6 = 0$

Nad ovim bitovima se primenjuje logika S7 funkcije, koja daje izlazni niz y_i:

$y_0 = 0$ $y_1 = 1$ $y_2 = 0$ $y_3 = 1$ $y_4 = 0$ $y_5 = 1$ $y_6 = 1$

Pošto pri deljenju ulaznog bloka na bitove važi da je bit najveće važnosti skroz levo, logično je da se i pri konstrukciji izlaza poštuje isto pravilo, pa će izlaz S7 funkcije biti 1101010, što u decimalnom obliku iznosi 106. Dakle za ulazni broj 44, izlaz funkcije je S7[44] = 106.

6.3.4.2 . FUNKCIJA F9

Funkcija F9 radi po istom principu kao F7, osim što je dužina ulaznih i izlaznih podataka 9 umesto 7 bita i logika unutar funkcije se razlikuje.

Ulazni blok podataka funkcije se sastoji od 9 bitova i deli se na devet delova, tako da je bit najveće važnosti sa leve strane.

$x = x_8 \,||\, x_7 \,||\, x_6 \,||\, x_5 \,||\, x_4 \,||\, x_3 \,||\, x_2 \,||\, x_1 \,||\, x_0$

Izlazni bitovi, koji se smeštaju u y_i niz se računaju po sledećoj logici:

$y_0 = x_0x_2 \oplus x_3 \oplus x_2x_5 \oplus x_5x_6 \oplus x_0x_7 \oplus x_1x_7 \oplus x_2x_7 \oplus x_4x_8 \oplus x_5x_8 \oplus x_4x_8 \oplus 1$

$y_1 = x_1 \oplus x_0x_1 \oplus x_2x_3 \oplus x_0x_4 \oplus x_1x_4 \oplus x_0x_5 \oplus x_3x_5 \oplus x_6 \oplus x_1x_7 \oplus x_2x_7 \oplus x_5x_8 \oplus 1$

$y_2 = x_1 \oplus x_0x_3 \oplus x_3x_4 \oplus x_0x_5 \oplus x_2x_6 \oplus x_3x_6 \oplus x_5x_6 \oplus x_4x_7 \oplus x_5x_7 \oplus x_6x_7 \oplus x_8 \oplus x_0x_8 \oplus 1$

$y_3 = x_0 \oplus x_1x_2 \oplus x_0x_3 \oplus x_2x_4 \oplus x_5 \oplus x_0x_6 \oplus x_1x_6 \oplus x_4x_7 \oplus x_0x_8 \oplus x_1x_8 \oplus x_7x_8$

$y_4 = x_0x_1 \oplus x_1x_3 \oplus x_4 \oplus x_0x_5 \oplus x_3x_6 \oplus x_0x_7 \oplus x_6x_7 \oplus x_1x_8 \oplus x_2x_8 \oplus x_3x_8$

$y_5 = x_2 \oplus x_1x_4 \oplus x_4x_5 \oplus x_0x_6 \oplus x_1x_6 \oplus x_3x_7 \oplus x_4x_7 \oplus x_6x_7 \oplus x_5x_8 \oplus x_6x_8 \oplus x_7x_8 \oplus 1$

$y_6 = x_0 \oplus x_2x_3 \oplus x_1x_5 \oplus x_2x_5 \oplus x_4x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_5x_6 \oplus x_7 \oplus x_1x_8 \oplus x_3x_8 \oplus x_5x_8 \oplus x_7x_8$

$y_7 = x_0x_1 \oplus x_0x_2 \oplus x_1x_2 \oplus x_3 \oplus x_0x_3 \oplus x_2x_3 \oplus x_4x_5 \oplus x_2x_6 \oplus x_3x_6 \oplus x_2x_7 \oplus x_5x_7 \oplus x_8 \oplus 1$

$y_8 = x_0x_1 \oplus x_2 \oplus x_1x_2 \oplus x_3x_4 \oplus x_1x_5 \oplus x_2x_5 \oplus x_1x_6 \oplus x_4x_6 \oplus x_7 \oplus x_2x_8 \oplus x_3x_8$

Izlaz funkcije S9 se, kao i izlaz funkcije S7, dobija konkatenacijom pojeidinačnih izlaznih bitova, tako da je bit najveće važnosti skroz levo:

$y = y_8 \,||\, y_7 \,||\, y_6 \,||\, y_5 \,||\, y_4 \,||\, y_3 \,||\, y_2 \,||\, y_1 \,||\, y_0$

Na ovaj način se dobija tablica vrednosti S9 funkcije, koja se sastoji od 512 pozicija, predstavljenih devetobitnim kodom (2^9=512), tako da je najniža pozicija 0 (000000000), a najviša 511 (111111111).

167	239	161	379	391	334	9	338	38	226	48	358	452	385	90	397
183	253	147	331	415	340	51	362	306	500	262	82	216	159	356	177
175	241	489	37	206	17	0	333	44	254	378	58	143	220	81	400
95	3	315	245	54	235	218	405	472	264	172	494	371	290	399	76
165	197	395	121	257	480	423	212	240	28	462	176	406	507	288	223
501	407	249	265	89	186	221	428	164	74	440	196	458	421	350	163
232	158	134	354	13	250	491	142	191	69	193	425	152	227	366	135
344	300	276	242	437	320	113	278	11	243	87	317	36	93	496	27
487	446	482	41	68	156	457	131	326	403	339	20	39	115	442	124
475	384	508	53	112	170	479	151	126	169	73	268	279	321	168	364
363	292	46	499	393	327	324	24	456	267	157	460	488	426	309	229
439	506	208	271	349	401	434	236	16	209	359	52	56	120	199	277
465	416	252	287	246	6	83	305	420	345	153	502	65	61	244	282
173	222	418	67	386	368	261	101	476	291	195	430	49	79	166	330
280	383	373	128	382	408	155	495	367	388	274	107	459	417	62	454
132	225	203	316	234	14	301	91	503	286	424	211	347	307	140	374
35	103	125	427	19	214	453	146	498	314	444	230	256	329	198	285
50	116	78	410	10	205	510	171	231	45	139	467	29	86	505	32
72	26	342	150	313	490	431	238	411	325	149	473	40	119	174	355
185	233	389	71	448	273	372	55	110	178	322	12	469	392	369	190
1	109	375	137	181	88	75	308	260	484	98	272	370	275	412	111
336	318	4	504	492	259	304	77	337	435	21	357	303	332	483	18
47	85	25	497	474	289	100	269	296	478	270	106	31	104	433	84
414	486	394	96	99	154	511	148	413	361	409	255	162	215	302	201
266	351	343	144	441	365	108	298	251	34	182	509	138	210	335	133
311	352	328	141	396	346	123	319	450	281	429	228	443	481	92	404
485	422	248	297	23	213	130	466	22	217	283	70	294	360	419	127
312	377	7	468	194	2	117	295	463	258	224	447	247	187	80	398
284	353	105	390	299	471	470	184	57	200	348	63	204	188	33	451

97	30	310	219	94	160	129	493	64	179	263	102	189	207	114	402
438	477	387	122	192	42	381	5	145	118	180	449	293	323	136	380
43	66	60	455	341	445	202	432	8	237	15	376	436	464	59	46

Tablica vrednosti S9 funkcije

PRIMER:

U slučaju da funkcija S9 kao ulazni parametar dobije broj 406, čiji je 9-bitni binarni ekvivalent 110010110, ulazni niz x_i će imati vrednosti:

$x_0 = 0 \quad x_1 = 1 \quad x_2 = 1 \quad x_3 = 0 \quad x_4 = 1 \quad x_5 = 0 \quad x_6 = 0 \quad x_7 = 1 \quad x_8 = 1$

dok će izlazni biti:

$x_0 = 1 \quad x_1 = 1 \quad x_2 = 0 \quad x_3 = 1 \quad x_4 = 1 \quad x_5 = 1 \quad x_6 = 1 \quad x_7 = 0 \quad x_8 = 0$

Primenom pravila da je bit najveće važnosti skroz levo i konkatenacijom pojedinačnih izlaznih bitova, dobija se 9-bitni binarni broj 001111011, čiji je decimalni oblik 123, što znači da funkcija S9 za ulazni boj 406 daje izlaz 123, odnosno:

S9[406] =123

Program korišćen za izračinavanje tabela S7 i S9 funkcija:

```
int main(){
   int p,q,broj=0;
   printf("S7\n");
   for(p=0;p<8;p++){
      for(q=0;q<16;q++){
         printf("%3d ",s7(broj++));
      }
      printf("\n");
   }
   broj=0;
   printf("\n\nS9\n");
   for(p=0;p<32;p++){
      for(q=0;q<16;q++){
         printf("%3d ",s9(broj++));
      }
      printf("\n");
   }
   return 0;
}

int s9(int ulaz){
   int x[9],i,t,y[9];
   for(i=0;i<9;i++){
      t=ulaz>>i;
      if(t&1){
         x[i]=1;
      }
      else{
         x[i]=0;
      }
   }
   y[0] = x[0] & x[2] ^ x[3] ^ x[2] & x[5] ^ x[5] & x[6] ^ x[0] & x[7] ^ x[1] & x[7] ^ x[2] & x[7] ^ x[4] & x[8] ^ x[5] & x[8] ^ x[7] & x[8]
^ 1;
   y[1] = x[1] ^ x[0] & x[1] ^ x[2] & x[3] ^ x[0] & x[4] ^ x[1] & x[4] ^ x[0] & x[5] ^ x[3] & x[5] ^ x[6] ^ x[1] & x[7] ^ x[2] & x[7] ^ x[5]
& x[8] ^ 1;
   y[2] = x[1] ^ x[0] & x[3] ^ x[3] & x[4] ^ x[0] & x[5] ^ x[2] & x[6] ^ x[3] & x[6] ^ x[5] & x[6] ^ x[4] & x[7] ^ x[5] & x[7] ^ x[6] & x[7]
^ x[8] ^ x[0] & x[8] ^ 1;
   y[3] = x[0] ^ x[1] & x[2] ^ x[0] & x[3] ^ x[2] & x[4] ^ x[5] ^ x[0] & x[6] ^ x[1] & x[6] ^ x[4] & x[7] ^ x[0] & x[8] ^ x[1] & x[8] ^ x[7]
& x[8];
   y[4] = x[0] & x[1] ^ x[1] & x[3] ^ x[4] ^ x[0] & x[5] ^ x[3] & x[6] ^ x[0] & x[7] ^ x[6] & x[7] ^ x[1] & x[8] ^ x[2] & x[8] ^ x[3] & x[8];
   y[5] = x[2] ^ x[1] & x[4] ^ x[4] & x[5] ^ x[0] & x[6] ^ x[1] & x[6] ^ x[3] & x[7] ^ x[4] & x[7] ^ x[6] & x[7] ^ x[5] & x[8] ^ x[6] & x[8]
^ x[7] & x[8] ^ 1;
   y[6] = x[0] ^ x[2] & x[3] ^ x[1] & x[5] ^ x[2] & x[5] ^ x[4] & x[5] ^ x[3] & x[6] ^ x[4] & x[6] ^ x[5] & x[6] ^ x[7] ^ x[1] & x[8] ^ x[3]
& x[8] ^ x[5] & x[8] ^ x[7] & x[8];
   y[7] = x[0] & x[1] ^ x[0] & x[2] ^ x[1] & x[2] ^ x[3] ^ x[0] & x[3] ^ x[2] & x[3] ^ x[4] & x[5] ^ x[2] & x[6] ^ x[3] & x[6] ^ x[2] & x[7]
^ x[5] & x[7] ^ x[8] ^ 1;
   y[8] = x[0] & x[1] ^ x[2] ^ x[1] & x[2] ^ x[3] & x[4] ^ x[1] & x[5] ^ x[2] & x[5] ^ x[1] & x[6] ^ x[4] & x[6] ^ x[7] ^ x[2] & x[8] ^ x[3]
& x[8];
   int izlaz=0;
   for(i=0;i<9;i++){
      izlaz+=y[i]*pow(2,i);
   }
   return izlaz;
}
int s7(int ulaz){
   int x[7],i,t,y[7];
   for(i=0;i<7;i++){
      t=ulaz>>i;
      if(t&1){
         x[i]=1;
      }
      else{
         x[i]=0;
```

```
      }
   }
   y[0] = x[1] & x[3] ^ x[4] ^ x[0] & x[1] & x[4] ^ x[5] ^ x[2] & x[5] ^ x[3] & x[4] & x[5] ^ x[6] ^ x[0] & x[6] ^ x[1] & x[6] ^ x[3] & x[6]
^ x[2] & x[4] & x[6] ^ x[1] & x[5] & x[6] ^ x[4] & x[5] & x[6];
   y[1] = x[0] & x[1] ^ x[0] & x[4] ^ x[2] & x[4] ^ x[5] ^ x[1] & x[2] & x[5] ^ x[0] & x[3] & x[5] ^ x[6] ^ x[0] & x[2] & x[6] ^ x[3] & x[6]
^ x[4] & x[5] & x[6] ^ 1;
   y[2] = x[0] ^ x[0] & x[3] ^ x[2] & x[3] ^ x[1] & x[2] & x[4] ^ x[0] & x[3] & x[4] ^ x[1] & x[5] ^ x[0] & x[2] & x[5] ^ x[0] & x[6] ^ x[0]
& x[1] & x[6] ^ x[2] & x[6] ^ x[4] & x[6] ^ 1;
   y[3] = x[1] ^ x[0] & x[1] & x[2] ^ x[1] & x[4] ^ x[3] & x[4] ^ x[0] & x[5] ^ x[0] & x[1] & x[5] ^ x[2] & x[3] & x[5] ^ x[1] & x[4] & x[5]
^ x[2] & x[6] ^ x[1] & x[3] & x[6];
   y[4] = x[0] & x[2] ^ x[3] ^ x[1] & x[3] ^ x[1] & x[4] ^ x[0] & x[1] & x[4] ^ x[2] & x[3] & x[4] ^ x[0] & x[5] ^ x[1] & x[3] & x[5] ^ x[0]
& x[4] & x[5] ^ x[1] & x[6] ^ x[3] & x[6] ^ x[0] & x[3] & x[6] ^ x[5] & x[6] ^ 1;
   y[5] = x[2] ^ x[0] & x[2] ^ x[0] & x[3] ^ x[1] & x[2] & x[3] ^ x[0] & x[2] & x[4] ^ x[0] & x[5] ^ x[2] & x[5] ^ x[4] & x[5] ^ x[1] & x[6]
^ x[1] & x[2] & x[6] ^ x[0] & x[3] & x[6] ^ x[3] & x[4] & x[6] ^ x[2] & x[5] & x[6] ^ 1;
   y[6] = x[1] & x[2] ^ x[0] & x[1] & x[3] ^ x[0] & x[4] ^ x[1] & x[5] ^ x[3] & x[5] ^ x[6] ^ x[0] & x[1] & x[6] ^ x[2] & x[3] & x[6] ^ x[1]
& x[4] & x[6] ^ x[0] & x[5] & x[6];
   int izlaz=0;
   for(i=0;i<7;i++){
      izlaz+=y[i]*pow(2,i);
   }
   return izlaz;
}
```

6.4. DERIVACIJA KLJUČEVA

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

$K= K_1 || K_2 || K_3 || K_4 || K_5 || K_6 || K_7$

Dok je K'_i generisan tako što je na postojeći ključ K_i XOR funkcijom dodata konstanta C_i.

$K'_i = K_i \oplus C_i$

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

C_1 = 0x0123 C_2 = 0x4567 C_3 = 0x89AB C_4 = 0xCDEF

C_5 = 0xFEDC C_6 = 0xBA98 C_7 = 0x7654 C_8 = 0x3210

Nakon generisanja K_i i K'_i ključeva, sledi derivacija KL, KO i KI ključeva, koja je prikazana u tabeli, gde <<N predstavlja ciklčnu rotaciju binarne sekvence za N mesta ulevo.

	K_i	K'_i	$KL_{i,1}$	$KL_{i,2}$	$KO_{i,1}$	$KO_{i,2}$	$KO_{i,3}$	$KI_{i,1}$	$KI_{i,2}$	$KI_{i,3}$
1	K_1	K'_1	K_1<<1	K'_3	K_2<<5	K_6<<8	K_7<<13	K'_5	K_4	K_8
2	K_2	K'_2	K_2<<1	K'_4	K_3<<5	K_7<<8	K_8<<13	K'_6	K_5	K_1
3	K_3	K'_3	K_3<<1	K'_5	K_4<<5	K_8<<8	K_1<<13	K'_7	K_6	K_2
4	K_4	K'_4	K_4<<1	K'_6	K_5<<5	K_1<<8	K_2<<13	K'_8	K_7	K_3
5	K_5	K'_5	K_5<<1	K'_7	K_6<<5	K_2<<8	K_3<<13	K'_1	K_8	K_4
6	K_6	K'_6	K_6<<1	K'_8	K_7<<5	K_3<<8	K_4<<13	K'_2	K_1	K_5
7	K_7	K'_7	K_7<<1	K'_1	K_8<<5	K_4<<8	K_5<<13	K'_3	K_2	K_6
8	K_8	K'_8	K_8<<1	K'_2	K_2<<5	K_5<<8	K_6<<13	K'_4	K_3	K_7

Tabela derivacije KL, KO i KI ključeva po iteracijama KASUMI algoritma.

Na ovaj način svaka iteracija svake od funkcija će imati jedinstven ključ, što predstavlja jedan od osnovnih principa bezbednosti.

7. ZAKLJUČAK

Mobilne mreže su projektovane da zadovolje trenutne zahteve korisnika po pitanju komunikacija i bezbednosti. Bezbednost GSM-a je bila zadovoljavajuća, ali nadogradnjom dodatnih funkcionalnosti pojavili su se veliki bezbednosni propusti. UMTS do određene mere rešava te bezbednosne propuste, ali sistem i dalje nije savršen. Ubrzani razvoj mobilne tehnologije ostavlja prostora napadačima da pronađu nove propuste i osmisle nove, sofisticiranije načine da ih iskoriste, čime postavljaju nove zadatke pred mobilne operatere i podstiču ih da se dodatno usavršavaju u pogledu bezbednosti. Ono što je sigurno je da i jedni i drugi napreduju i da ćemo sutra imati mnogo ozbiljnije pretnje nego što ih imamo danas. Zato je potrebno da i sami postanemo svesni pretnji koje nam donose nove tehnologije i da pre svega sami mislimo o bezbednosti svojih informacija. To možda neće u potpunosti zaštititi informacije, ali će dodatno olakšati posao ljudima koji se bave bezbednošću mobilnih mreža.

LITERATURA

[01] Valtteri Niemi, Kaisa Nyberg: UMTS Security, 2003

[02] Cornelia Cappler: UMTS Networks and Beyond, 2009

[03] Specification of 3GPP Confidentiality and Integrity Algorithms - Document 2: KASUMI Specification, 1999

[04] Ian Poole: UMTS / WCDMA Network Architecture
(http://www.radio-electronics.com/info/cellulartelecomms/umts/umts-wcdma-network-architecture.php)

[05] Nanić Dragan: Sigurnost u 3G mrežama, 2004
(http://www.telfor.rs/telfor2004/radovi/S-12-3.PDF)

[06] Hrvatska akademska i istraživačka mreža - Sigurnosni nedostaci u 3G mrežama
(http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-07-128.pdf)