Fakultet elektrotehnike i računarstva
Zavod za elektroničke sustave i obradbu informacija

GSM: END - TO - END ENKRIPCIJA RAZGOVORA

Agata Šakić
0036404744

SADRŽAJ

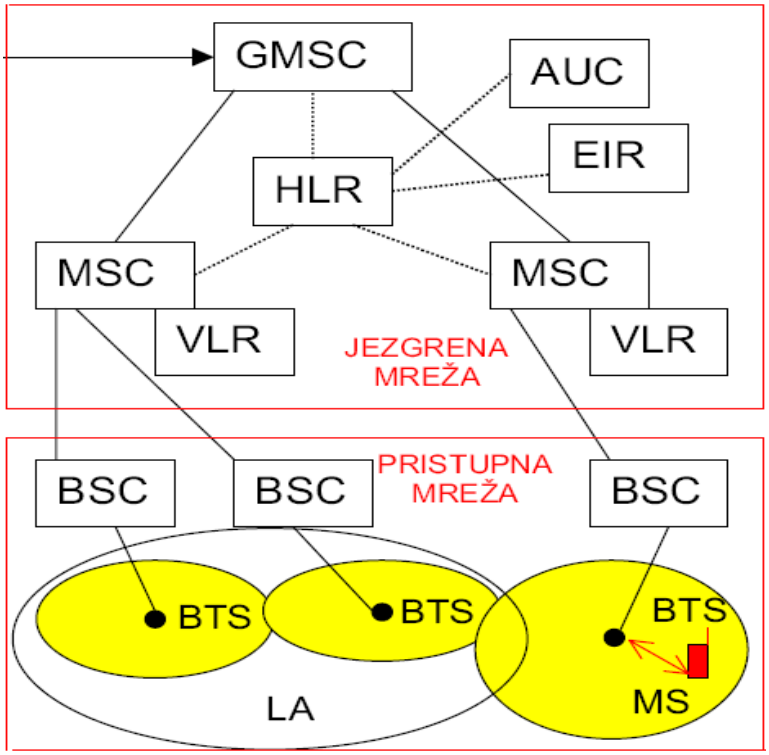
1 UVOD

Globalni sustav pokretnih komunikacija (Global System for Mobile communication - GSM) najraširenij je standard mobilnih komunikacija. On je standard druge, digitalne generacije mobilne tehnologije (2G). Koriste se standardi:

- GSM 900 (emitiranje na frekvencijskom rasponu od 900 MHz) – Europa, neka područja Azije i Tihog oceana
- GSM 1800 (emitiranje na frekvencijskom rasponu od 1800 MHz) – također se koristi u Europi i Aziji, ali nije tako široko prihvaćen kao GSM 900.
- GSM 1900 (emitiranje na frekvencijskom rasponu od 1900 MHz) – u obje Amerike i Kanadi.

Osnovne karakteristike GSM-a su ćelijska struktura, višestruki pristup u vremenskoj podjeli (Time Division Multiple Access – TDMA: 124 frekvencije x 8 kanala = 992 kanala) i postojanje prometnih i kontrolnih kanala (odvojene korisničke od upravljačkih informacija).

1.1 ARHITEKTURA MREŽE GSM



Sl.1. – Arhitektura GSM mreže

- MSC (Mobile Switching Centre) - mobilni servisni komutacijski centar kontrolira i upravlja cjelokupni sustav
- GMSC (Gateway MSC)
- HLR (Home Location Register) - baza podataka koja sadrži sve potrebne informacije o svim pretplatnicima koji su registrirani u odgovarajućoj GSM mreži
- VLR (Visitor Location Register) – zajedno s HLR – om i MSC - om vrši usluge usmjeravanja i preusmjeravanja poziva prema drugim mrežama te sadrži podatke o trenutnom položaju mobilne stanice u sustavu
- AUC (Authentication Centre) - zaštićena baza podataka koja sadrži kopiju tajnog koda (PIN broj) koji sadržava svaka pretplatnička SIM kartica
- EIR (Equipment Identification Register) - baza podataka koja sadrži listu mobilnih uređaja koji mogu pristupiti sustavu

- BSS (Base Station System)
- BSC (Base Station Controller) - upravljački dio bazne stanice
- BTS (Base Transceiver Station) - primopredajna bazna stanica
- MS (Mobile Station) – mobilna stanica
- LA (Location Area)

U HLR-u su sadržani:

- MSISDN (Mobile Station Integrated Services Digital Network) - broj koji identificira mobilnog telefonskog korisnika unutar javne telefonske mreže, tj. korisnički broj (dodjeljuje mrežni operator)
- IMSI (International Mobile Subscriber Identification) – sastoji se od vrijednost kôda zemlje za pokretne mreže (MCC), za Republiku Hrvatsku je 219, kôda pokretne mreže (MNC) koji ima dvije znamenke te je stoga moguće dodijeliti 100 MNC kôdova u rasponu od 00 do 99 i MSIN-a (Mobile Station Identification Number) (dodjeljuje mrežni operator)

U MS-u u SIM - u (Subscriber Identity Module):

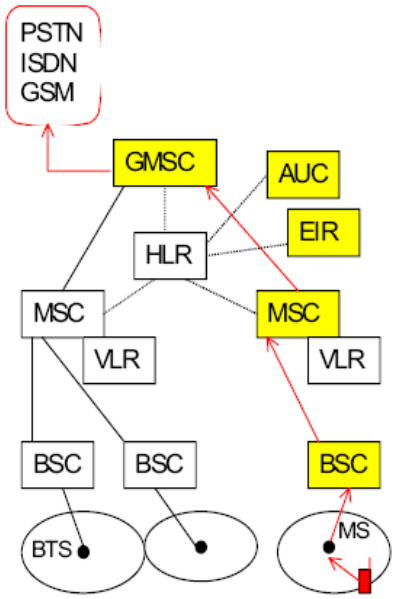
- MSISDN i IMSI
- Ki – jedinstveni 128-bitni broj koji osigurava komunikaciju na zračnom sučelju (MS - BTS). Ki se ne razmjenjuje kroz mrežu, već je izravno upisan u SIM i AUC, nije poznat niti korisniku jer je osnovica sigurnosti GSM mreže.

Prilikom uključivanja MS-a i registracije provjerava se autentičnost (AUC) i ispravnost opreme (EIR) te se lokacijska informacija dostavlja u HLR, tj. VLR. Prilikom promjene lokacije, kada MS mijenja ćeliju, podaci se obnavljaju. Omogućeno je prebacivanje poziva (handover) i komunikacija na drugim mrežama (roaming).

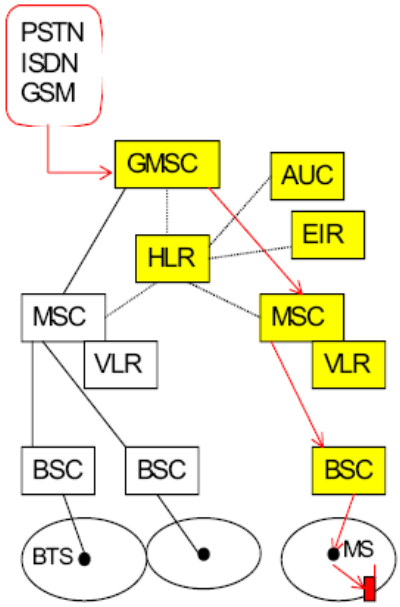
Za registraciju u vlastitoj mreži, MS šalje VLR-u zahtjev za registracijom, a on registracijsku poruku prosljeđuje HLR-u koji mu potom šalje pretplatničke podatke i registracija je uspješno obavljena. Za promjenu lokacije u vlastitoj mreži, postupak je jednak za novi VLR, uz to da HLR na kraju registracije starom VLR-u šalje deregistracijsku poruku koji mu odgovara s potvrdom deregistracije.

Za vrijeme obavljanja odlaznog poziva MS traži kanal, provjerava se autentičnost i identitet opreme i prospaja se poziv (BTS - BSC -MSC - GMSC - druga mreža). Tijekom

prijenosa podaci su kriptografski zaštićeni. Za vrijeme dolaznog poziva GMSC od HLR-a traži lokacijsku informaciju (LA) za MS te HLR i VLR izmjenjuju informacije o pozvanom MS-u. Provjerava se autentičnost i identitet opreme i prospaja se veza (kriptografska zaštita podataka).



Sl.2. Odlazni poziv



Sl.3. Dolazni poziv

1.2 SIGURNOSNE DOMENE

Sigurnost je sposobnost mreža, sustava, usluga i aplikacija da se suprotstave neočekivanim slučajnim događajima i zlonamjernim aktivnostima koje mogu narušiti i kompromitirati raspoloživost, vjerodostojnost, cjelovitost i povjerljivost informacije i komunikacije[1].

Kada zahtijevamo sigurnost, u 3 osnovne sigurnosne domene spadaju:

- **autentifikacija korisnika** (utvrđivanje i potvrda identiteta korisnika)
- **povjerljivost podatkovnih i signalnih informacija** (cjelovitost podataka - informacija poslana, primljena i pohranjena u izvornom obliku, povjerljivost - zaštita od neovlaštenih pristupa i neovlaštenog uvida, kontrolu pristupa, raspoloživost) te
- **povjerljivost korisnika** (zaštita IMSI-a)

Problemi do kojih može doći ako zahtjevi na sigurnost nisu ispunjeni:

- Presretanje i prisluškivanje podataka pri kojima se elektronička komunikacija presreće i preuzima se informacija čime je omogućena njihova neovlaštena uporaba i narušena privatnost. Ovaj slučaj je i zakonski reguliran.
- Prekidanje normalnog tijeka komunikacije, usluge ili aplikacije ili onemogućavanje iste namjernim izazivanjem opterećenja mreže ili umreženog sustava
- Promjena ili uništenje informacije ili kašnjenje informacije što ima potencijalno jednak učinak
- Ubacivanje zlonamjerne informacije.
- Lažno predstavljanje čime se preuzima identitet i uloga korisnika

[1] **Sigurnost mreža, usluga i aplikacija, Studijski primjer: pokretna mreža,** Poslijediplomski studij, Projektiranje telekomunikacijskih sustava**,** Ignac Lovrek

2 RAZRADA TEME

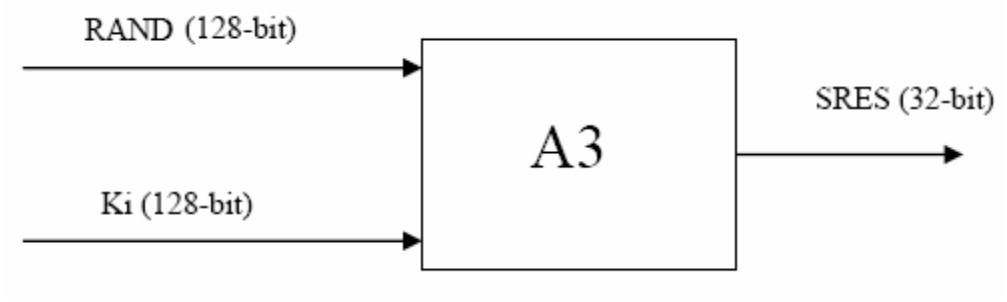
2.1 AUTENTIFIKACIJA KORISNIKA

Autentifikacija je potrebna da bi sustav bio zaštićen od neovlaštenih pristupa. U protivnom je omogućena registracija korisnika koji nije pretplatnik dane mreže, njegovo lažno predstavljanje i preuzimanje tuđeg računa, što bi, osim narušavanja privatnosti, značilo i potencijalno stvaranje troška na račun drugog korisnika.

Mobilni uređaj sam po sebi nema utvrđenu komunikaciju s određenom mrežom, za to je zadužena SIM kartica. Stoga ona mora posjedovati sve potrebno za pristup određenom računu (account-u): IMSI - jedinstven za svakog korisnika na svijetu, može mu se pristupiti lokalno uz poznavanje SIM PIN-a, i Ki - ključ za enkripciju poznat samo SIM-u i AUC-u. Mobilni uređaj sam po sebi nikad ne „nauči“ Ki, on mora biti maksimalno zaštićen. Sve dobivene podatke prosljeđuje SIM-u koji potom obavlja zahtjeve kao što su autentifikacija ili generacija ključa za šifriranje podataka (Kc - ciphering key).

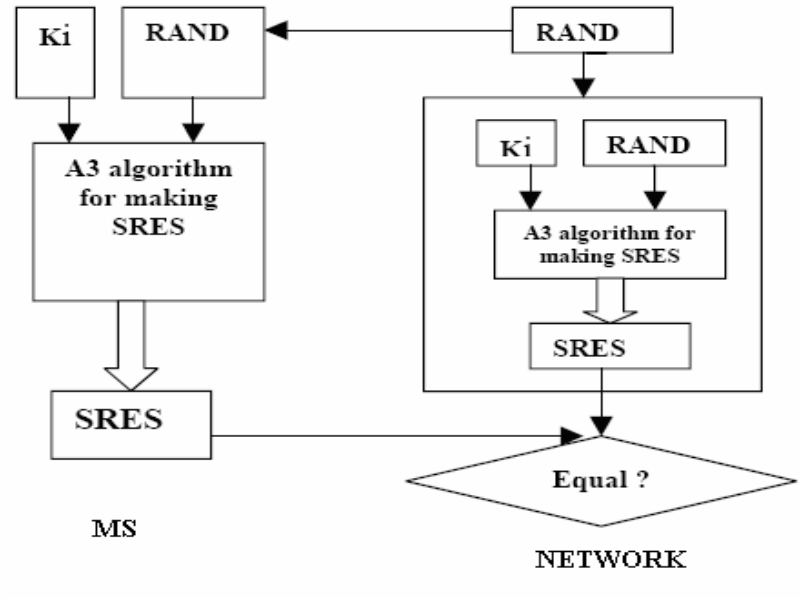
SIM je inteligentni uređaj (kartica) koji sadrži mikroprocesor u kojem se obrađuju podaci. Zaštićena je PIN kodom koji se unosi na tipkovnici mobilnog uređaja i prosljeđuje SIM kartici na verifikaciju. Za 3 bezuspješna unosa, SIM „zaključava“ PIN i traži unos PUK-a (PIN UnlocK-a). Nakon propalih pokušaja unosa PUK-a (obično se dopušta 10ak pokušaja), SIM onemogućava lokalni pristup i autentifikaciju čime SIM kartica postaje beskorisna.

Također treba utvrditi podudarnost tajnog Ki-a u AUC-u i onog u SIM-u. Naravno, to možemo jednostavno izvesti slanjem Ki-a putem mreže i njihovom usporedbom. Međutim, „puštanje“ Ki-a na mrežu je jako riskantno zbog mogućnosti presretanja ili prisluškivanja tajne informacije i nije preporučljivo. Umjesto toga, mreža generira 128-bitni broj – tzv. RAND. Generacijom je moguće dobiti bilo koji kombinaciju, a ima ih ($0 - 2^{128}-1$). RAND koristi A3 algoritam i Ki da bi matematički generirao 32-bitnu autentifikacijsku oznaku (authentication token) poznatu kao SRES (Signed RESult).



Sl.4. Algoritam A3

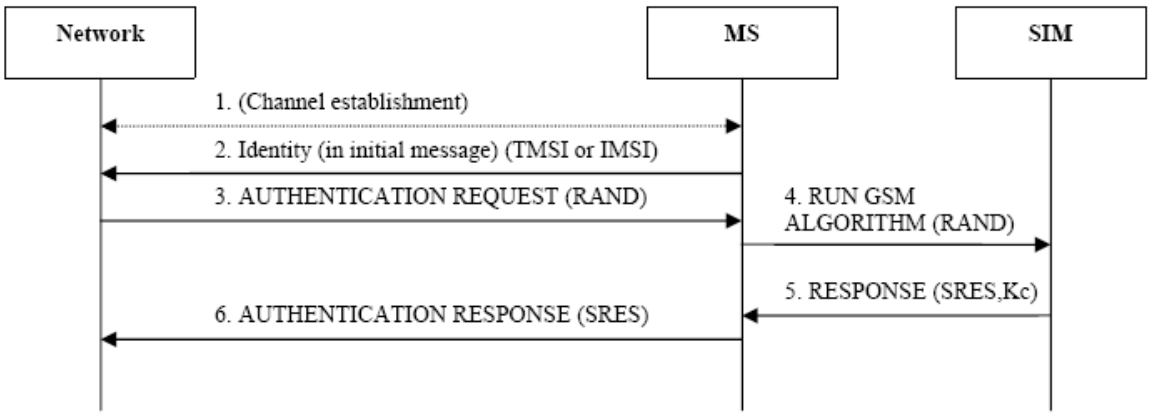
RAND se šalje i mobilnom uređaju koji također generira SRES i šalje ga mreži na usporedbu. Ako se primljeni SRES podudara sa SRES-om generiranim u mreži, Ki-ovi moraju biti jednaki po matematičkoj teoriji vjerojatnosti. 128-bitni RAND se svaki put nanovo generira. Naime, kada bi se uvijek slao isti RAND, „provalnik“ bi jednostavno mogao imitirati korisnika šaljući poznati SRES.



Sl.5. Proces autentifikacije

Algoritam autentifikacije:

1) AUC unaprijed generira RAND i proračunava SRES
2) Registriran je pokušaj uspostave komunikacije MS-a i mreže.
3) MS šalje mreži početnu poruku koja mora sadržavati korisničke podatke (identity field). Po mogućnosti se izbjegava slanje IMSI-a. Umjesto njega se šalje TMSI (Temporary Mobile Subscriber Identity) . MS se prijavljuje VLR-u koji traži podatke za MS od HLR-a, koji ih dobiva iz AUC-a.
4) AUC šalje BTS-u zahtjev za autentifikaciju (**authentication request**) koji sadrži RAND i SRES, a BTS prosljeđuje RAND MS-u.
5) MS prima RAND i prosljeđuje ga SIM-u
6) SIM izvrši A3 algoritam i vraća SRES MS-u
7) SIM šalje autentifikacijski odgovor (authentication response) tako da pošalje SRES BTS-u
8) VLR provjerava jednakost dvaju SRES-ova i ako oni jesu jednaki, autentifikacija je uspješno sprovedena



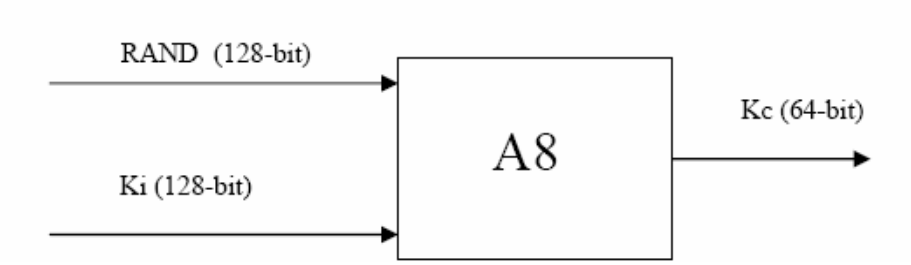
Sl.6. Komunikacija SIM-a, MS-a i mreže

Ako autentifikacija nije uspješno provedena, a korišten je TMSI, mreža može pri ponovnom pokušaju autentifikacije zatražiti IMSI.

A3 algoritam se ne odnosi na specifičan algoritam. Svaki operator odabire svoj A3 algoritam. Napravljen je kao „jednosmjerna“ funkcija (trap door function) da bi omogućio lako generiranje SRES-a iz RAND-a i Ki-a, ali jako kompleksno dobivanje Ki-a iz RAND-a i SRES-a. Prvi A3 algoritam je COMP128 (poznat kao i COMP128-1), a zbog poboljšanja se najviše koriste COMP128-2 i COMP128-3. COMP128 ima funkciju i A8 algoritma (algoritam za generiranje ključa za šifriranje).

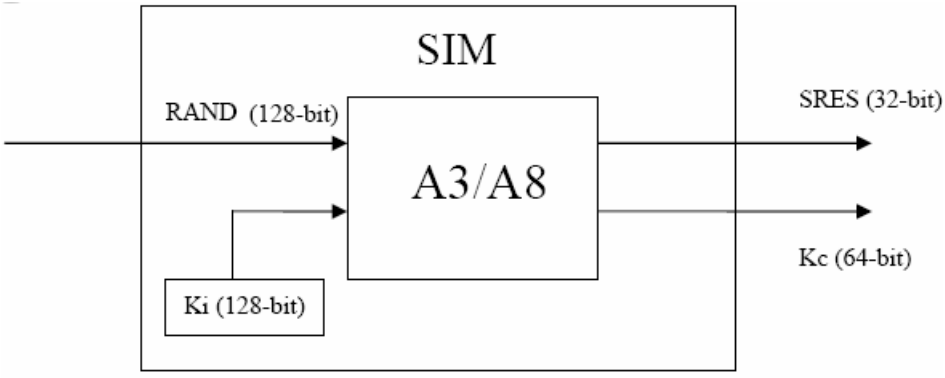
2.2 ŠIFRIRANJE

Šifriranje podataka najvažnija je zaštita prilikom prijenosa podatkovnih ili signalnih informacija. Koristi se tzv. simetrično šifriranje što znači da se podaci šifriraju i dešifriraju istim tajnim ključem. Uz pomoć Ki-a i RAND-a, osim SRES-a generira se i Kc – ključ za šifriranje. Za generaciju Kc-a upotrebljava se algoritam A8.



Sl.7. Algoritam A8

Kad god se pokrene A3 algoritam, pokreće se i A8. SIM pokreće oba u isto vrijeme:

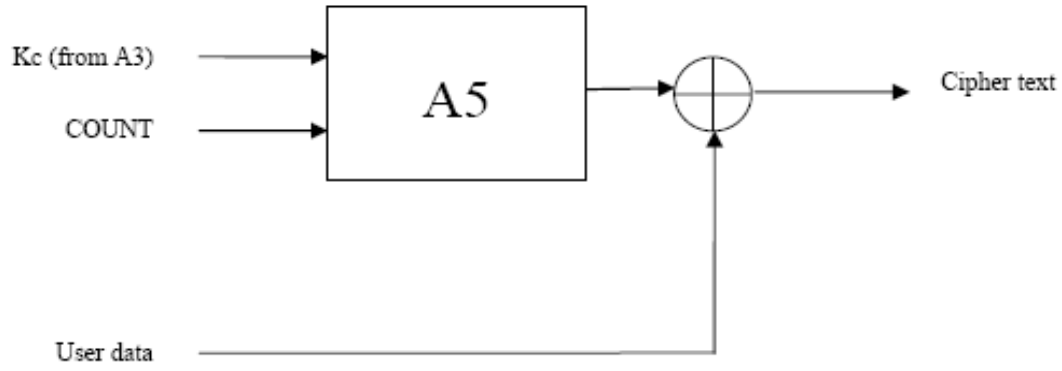


Sl.8. Implementacija A3/A8 u SIM

Kako se podaci šalju šifrirani, Kc mora biti poznat mreži i mobilnom uređaju. Za onoga tko prisluškuje podatke ili ih presreće, oni nemaju puno smisla. Kc se također mora često mijenjati da bi se povećala sigurnost.

Podaci koji se šalju GSM standardom podijeljeni su u snopove (burst), svaki po 114 bita odaslani u razmaku od 4.615ms. Šifriranje se provodi tako da se generira slučajna 114-bitna sekvenca uz pomoć A5 algoritma i sa 114-bitnim snopom podataka se vrši XOR

operacija. Ako ćemo A5 algoritam opisati kao crnu kutiju, ulazi su: Kc (64 bita) i poznati broj TDMA bloka podataka (22 bita) nazvanim COUNT , dok je izlaz 114-bitna sekvenca.



Sl.9. Algoritam A5

Trenutno su definirana tri A5 algoritma: A5/1, A5/2 i A5/3. A5/1 je korišten u SAD-u i u Europi dok se nesigurniji algoritam A5/2 koristi u zemljama nedovoljno pouzdanim za snažnije šifriranje. Pokazalo se da je bilo polemika da li bi GSM šifriranje trebalo biti jako ili ne. Nijemci su se zalagali za jaku enkripciju, dok su sve ostale zemlje bile protiv. Krajnji je algoritam francuskog podrijetla. Oba su dugo vremena bila čuvana u tajnosti dok ih nije „probio“ Marc Briceno iz GSM telephone-a 1999. godine.

A5/1 se bazira na trima linearnim posmačnim registrima s povratnom vezom i nepravilnim signalom takta duljine 32 bita, od kojih koristi samo 19 bitova u prvom, 21 bit u drugom te 23 bita u trećem registru. Ključ koji koristimo za šifriranje dug je 64 bita što je jednako zbroju efektivnih duljina posmačnih registara, što i jest cilj, jer se ključ u prvoj fazi algoritma upisuje u posmačne registre. Bajtovi ključa se upisuju redom u registre, oni s nižim indeksom na mjesta u registre s višim indeksom. Kako imamo različite duljine registara, neki će se bajtovi upisat dijelom u jedan, dijelom u drugi registar. Nakon toga, sve je spremno za proces šifriranja. U procesu se koristi pomoćni bajt. U njega se za svaki bajt podataka posebno zapisuju bitovi od kojih svaki ovisi o trenutnom stanju posmačnih registara. Između dobivenog pomoćnog bajta i bajta podataka vrši se XOR operacija kojom dobivamo šifrirani bajt. U pomoćni bajt zapisujemo bit po bit u 8 iteracija. U svakoj iteraciji bajt napravi posmak ulijevo. Time ostaje na njegovom najnižem bitu slobodno mjesto na koje možemo upisati novi bit. Da li će taj bit biti 0 ili 1 ovisi o trenutnim vrijednostima posmačnih registara što provjerava posebna procedura. U svakom registru točno je definiran poseban bit koji će se

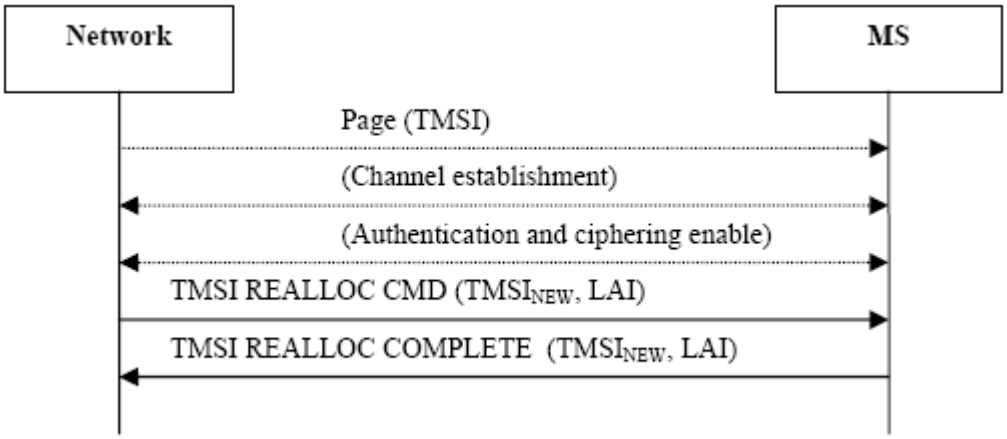
koristiti kod te procedure. U prvom registru je to deveti bit, a u ostala dva registra se radi o jedanaestom bitu. Najprije se provjerava kod sva tri bita ima li koji vrijednost 1. Nakon provjere, algoritam može razmatrati dva slučaja: prvi je slučaj da dva ili sva tri od spomenutih bitova imaju vrijednost 1 dok je drugi slučaj da samo jedan ili nijedan bit nema tu vrijednost. Osim kontrole navedenih bitova, promatraju se i još neki, za svaki registar posebno: za prvi registar su to 18., 17., 16. i 13 bit, u drugom registru se radi o 21., 20., 16. i 12. bitu dok se u trećem registru kontroliraju 22., 21., 18. i 17. bit. Zasebno se za svaki registar koristi još jedan pomoćni niz od 32 bita koji je rezultat operacije **XOR** između spomenutih bitova. Taj se niz naziva feedback. Konkretno, feedback ima vrijednost koja je rezultat te operacije između nekoliko 32- bitnih vrijednosti, ali mu je zato bit na najnižoj poziciji jednak toj operaciji između točno spomenutih bitova. Process dešifriranja ima identičnu proceduru kao i process šifriranja.

A5/3 je dodan 2002. godine i temelji se na Kasumievom algoritmu definiranom za 3GPP (3rd Generation Partnership Project). Što se A8 algoritama tiče, važno je napomenuti da se prilikom generiranja Kc-a uvijek postavljalo 10 fiksnih nula što je od 64 generiranih bitova ustvari davalo slobodu samo za njih 54 čime je namjerno oslabljen A5. Kod nove generacije A8 algoritama (COMP128-3), generira se puni Kc sa svih 64 bita čime je dobivena pojačana sigurnost. To je ujedno i jedina razlika algoritama COMP128-2 i COMP128-3.

2.3 TMSI

(Temporary Mobile Subscriber Identity)

Kao što je već spomenuto, jedan od načina zaštite komunikacije jest izbjegavanje korištenja IMSI-a. To se ostvaruje upotrebom 32-bitnog TMSI-a. TMSI se obnavlja najmanje prilikom svake promjene lokacije (Location Area), a može biti u svakom trenutku promijenjen i od strane mreže i šifriran poslan natrag MS-u. Na taj način se onemogućava treća strana da prati trenutni TMSI, čime je ostvarena anonimnost korisnika. Uređaj mora pohranjivati TMSI u postojanu podatkovnu memoriju (non – volatile memory) da ostane sačuvan i prilikom gašenja mobilnog uređaja. Uobičajeno je da se čuva u SIM-u.



Sl.10. Komunikacija prilikom promjene TMSI-a

3 ZAKLJUČAK

Za svaki sustav sa simetričnim šifriranjem, sigurnost sustava vezan za zaštitu podataka počiva na tajnosti ključa za šifriranje (Kc-a). Svatko tko posjeduje potreban ključ može dešifrirati podatke i ugroziti pouzdanosti sistema. Ako to primijenimo na GSM, algoritam A8 i način generiranja Kc-a moraju biti visokog stupnja sigurnosti. Jako malo napada na sigurnost je bilo dok su algoritmi A5 držani u tajnosti. Međutim, kako su sva tri otkrivena i objavljena, bilo ih je mnogo. Spomenut ćemo nekoliko najpoznatijih: Biryukov, Wagner, Shamir – uz poznavanje 2s razgovora, potrebno je samo nekoliko minuta da se na osobnom računalu otkrije Kc kod algoritma A5/1, Berkleyev „little sister“ kod A5/2, kod A3/8 (COMP128) se uz fizički pristup SIM kartici može u nekoliko sati otkriti IMSI i Ki što omogućava „kloniranje“ kartice, Bihamov napad na A5/3 (KUSIMU), itd. Neki su algoritmi bili i namjerno oslabljeni kao što je bilo kod prvih dviju verzija COMP128, gdje se u generaciji Kc-a postavljalo deset fiksnih nula. Moguće je kupiti i gotove uređaje za prisluškivanje, tzv. „spy phones“, cijene jesu visoke, ali jesu li dovoljno visoke za narušavanje privatnosti koje omogućavaju? Sigurnost u GSM mrežama nije idealna, ima mnogo propusta i slabosti koji se polako otklanjaju, ali se i otkrivaju novi načini „probijanja“ i neovlaštenih pristupa podacima pa ostaje pitanje hoće li ikada mreža sa zračnim sučeljem, bez obzira na algoritme i načine šifriranja, biti otporna na napade.

4 LITERATURA

http://en.wikipedia.org/wiki/Global_System_for_Mobile_Communications

http://en.wikipedia.org/wiki/A5/1

http://www.gsm-security.net/gsm-security-papers.shtml

http://www.funet.fi/pub/crypt/cryptography/symmetric/a5/

http://cryptome.org/a51-crack.htm

spvp.zesoi.fer.hr/predavanja/slides/gsm

http://www.telfon.net/tehnologije/arhitektura.php

www.tel.fer.hr/files/poslijediplomski/pts/5.%20Post-PTS3_sig-lov.pdf