TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto

Tutkintotyö

Toni Pesonen

SALAUSTEKNIIKAT LANGATTOMISSA JÄRJESTELMISSÄ

Tutkintotyö, joka on jätetty opinnäytteenä tarkastettavaksi insinöörin tutkintoa varten
Tampereella 20.4.2010.

Työn ohjaaja: Lehtori Jorma Peltoniemi
Tampere 2010

TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikka
Tietoliikennetekniikka
Toni Pesonen
Salaustekniikat langattomissa järjestelmissä
Tutkintotyö 32 sivua
Työn ohjaaja Lehtori Jorma Peltoniemi
Huhtikuu 2010

TIIVISTELMÄ

Tämän työn tavoitteena on esitellä erilaisia salaustekniikoita ja erityisesti tekniikoita, joita käytetään langattomissa järjestelmissä. Työssä perehdytään hieman salauksen historiaan sekä salauksen perusteisiin. Lisäksi käydään läpi tarkemmin muutamat langattomat sovellukset, WLAN, Bluetooth, GSM, 3G ja LTE-järjestelmät ja niissä käytetyt salaustekniikat.

Työn tarkoitus on antaa selkeä kuva erilaisista salaustekniikoista ja auttaa ymmärtämään, miten näitä on sovellettu nykypäivän käytetyimmissä langattomissa järjestelmissä. Juuri langattomuus tekee työstä mielenkiintoisen. Langattamuus ja langattomat järjestelmät ovat tärkeitä myös tulevaisuudessa. Työssä kuvattujen järjestelmien vain salauksen kannalta tärkeimmät kohdat on esitetty.

Avainsanat Langaton järjestelmä, salaus, GSM, WLAN, 3G, LTE

TAMK UNIVERSITY OF APPLIED SCIENCES

Computer Systems Engineering
Telecommunication Engineering
Toni Pesonen
Encryption techniques in wireless systems
Thesis 32 pages
Thesis supervisor Lecturer Jorma Peltoniemi
April 2010

ABSTRACT

The purpose of this paper is to introduce different kinds of encryption techniques and how they are used in a modern wireless network. This paper deals a little bit with the history of cryptology and the basic encryptions. The systems that are dealt with are WLAN, Bluetooth, GSM, 3G and LTE-systems.

It's the wireless side that makes this paper interesting. Keeping secrets has always been an issue in a wireless telecommunication and that is the case in the future too. Wireless systems will become more and more common in the future and it's important to get to know the security of these systems. In this paper the security aspects of the systems are described briefly and only the main points about the encryptions are shown for easy understanding.

Keywords Wireless systems, encryption, WLAN, GSM, 3G, LTE

ALKUSANAT

Tämä työ on tehty Tampereen ammattikorkeakoulun tietoliikennetekniikan linjan opinnäytetyönä.

Aiheen valinta oli aluksi hieman hankalaa kunnes mieleeni tulivat salaukset, joita käytetään esimerkiksi matkapuhelinjärjestelmissä. Kiinnostuin aiheesta siinä määrin, että päätin tehdä aiheesta opinnäytetyöni. Aiheeseen tutustuminen osoittautui erittäin mielenkiintoiseksi ja ajatuksia herättäväksi.

Haluan kiittää kaikkia opettajiani Tampereen ammattikorkeakoulussa, sillä heidän opastuksellaan ja opetuksiensa avulla pystyin tämän työn tekemään. Kiitän erityisesti Jorma Peltoniemeä työn ohjaamisesta. Erityiskiitokset myös vanhemmilleni, jotka ovat tukeneet minua monin tavoin koko opiskelujeni ajan.

Tampereella huhtikuussa 2010

Toni Pesonen

SISÄLLYSLUETTELO

LYHENNELUETTELO

3DES	3DES, paranneltu lohkosalain
3G	3rd Generation, kolmas sukupolvi
A3	A3, GSM-verkossa tilaajan tunnistukseen käytetty salausalgoritmi
A5	A5, GSM-verkossa radiotien salaamiseen käytetty algoritmi
A8	A8, GSM-verkon salausalgoritmi, jolla muodostetaan salausavain Kc.
AES	Advanced Encryption Standard, lohkosalausmenetelmä
AK	Anonymity Key, salausavain
AMF	Authentication management field, tunnistuksessä käytettävä arvo
AN	Access Network
AuC	Authentication Centre, tunnistuskeskus
AUTN	Authentication token, tunnistin
BS	Base Station, tukiasema
CCMP	Counter Mode Encryption, salausprotokolla
Ck	Cipher key, salausavain
DES	Data Encryption Standard, lohkosalain
E0	E0, jonosalain
EAP-TLS	Extensible Authentication Protocol- Transport Layer Security, käyttäjien tunnistusprotokolla
eNB	Enhanced nodeB, tukiasema
GMSK	Gaussian minimum shift keying, modulaatiomenetelmä
GSM	Global System for Mobile Communications, maailmanlaajuinen matkapuhelinverkko
GUTI	Globally Unique Temporary Identity, tilapäinen matkapuhelimen tunnus
HN	Home Network, kotiverkko
HSS	Home Subscriber Server, tilaajatietokanta
IBS	Input bit stream, sisääntuleva bittivirta

IEEE	Institute of Electrial and Electronics Engineers, standardointijärjestö
Ik	Integrity key, salausavain
IMEI	International Mobile Equipment Identity, kansainvälinen laitetunniste
IMSI	International Mobile Subscriber Number, kansainvälinen matkapuhelintilaajan tunnus
IP	Internet Protocol, internetprotokolla
IrDA	Infrared Data Association, infrapunajärjestelmä
IV	Initialization Vector, alustusvektori
Kc	64-bit ciphering key, salausavain
Ki	Authentication Key, salausavain
KS	Key Stream, avainjono
LTE	Long Term Evolution, matkapuhelinverkkojen neljäs sukupolvi
MAC-A	Message Authentication Code-A, vahvistusviesti
MME	Mobility Management Entity, hallintayksikkö
MSC	Mobile Switching Center, matkapuhelinkeskus
MT	Mobile Termination
OBS	Output Bit stream, ulostuleva bittivirta
PIN	Personal Identification Number, henkilökohtainen tunnistusavain
PMK	Pairwise Master Key, pääsalausavain
PTK	Pairwise Transient Key, salausavain
RAND	Random, satunnaisluku
RC4	Rivest Cipher 4, jonosalain
RNC	Radio Network Controller, radioverkko-ohjain
RSA	Rivest, Shamir, Adleman, salausmenetelmä
SAE	System Architecture Evolution, kytkentä tai pakettiverkko
Serving-GW	serving gateway, tarjoavana yhdyskäytävänä
SIM	Subscriber Identity Module, käyttäjän tunnistuskortti
SN	Serving Network, palveleva verkko
SQN	Sequence, lukujono

SRES	Signed Response, kirjattu vastaus
SSID	Service Set Identification, langattoman verkon nimi
TDMA	Time division multiple access, aikajakoisuus
TMSI	Temporary Mobile Subscriber Identity, tilapäinen matkapuhelimen tunnus
UE	User Equipment, käyttäjän laite
UMTS	Universal Mobile Telecommunications System, matkapuhelinjärjestelmän kolmas sukupolvi
USIM	User Service Identity Module, käyttäjän tunnistuskortti
WEP	Wired Equivalent Privacy, langattoman verkon salausmenetelmä
WLAN	Wireless Local Area Network, langaton lähiverkko
VLR	Visitor Location Register, vierailijarekisteri
WPA/2	Wireless Fidelity Protected Access, langattoman verkon salausmenetelmä
XOR	Exclusive or, looginen operaatio
XRES	Expected Response, odotettu vastaus

1 JOHDANTO

Ihmiset ovat kautta aikojen halunneet salata toisiltaan jotain, tämä kuuluu ihmisluontoon. Langattomuus taas näkyy tänä päivänä monessa kohtaa jokaisen elämässä, sillä lähes kaikilla ihmisillä on matkapuhelimet. Myöhemmin perehdytäänkin tarkemmin hyvin suositun GSM-järjestelmän salaukseen sekä otetaan kantaa myös uudempiin järjestelmiin, 3G ja LTE. Aluksi kuitenkin tutustutaan hieman salauksen historiaan sekä selvitellään, millasia salaukset yleisesti ovat.

Hyvin monilla yleisillä paikoilla sekä ihmisten kodeissa on nykyään käytössä WLAN (Wireless local area network), eli langaton lähiverkko. Tästä syystä on tärkeä huomata ottaa käyttöön salaus näissä järjestelmissä. Seuraavaksi kuitenkin lähempi katsaus salauksen historiaan ja erilaisiin salausmenetelmiin, jonka jälkeen tutustutaan salaukseen muutamissa erilaisissa langattomissa järjestelmissä.

2 Salaus yleisesti

Salauksella tarkoitetaan perinteisesti tapaa tehdä, koodata, viesti suojatuksi niin, että vain vastaanottaja tai vastaanottajat voivat sen avata ja ymmärtää. Nykyisin voidaan saavuttaa jo lähes murtumaton suoja ja viestin eheys. Salaukseen liittyvät läheisesti termit salaus ja purkaminen, jotka ovat toistensa vastatoimia. Salain taas on algoritmipari, jolla saavutetaan salaus. Salausavain säätelee algoritmien toimintaa. /2, s. 19 - 20/

Salausta on käytetty jo pitkään. Aikoinaan jo Julius Caesar käytti salausta, joka tosin oli vain aakkosten siirtoa eteenpäin. Tämä äärimmäisen yksinkertaista tapa oli silti siihen aikaan toimiva. Salaukset ovat kehittyneet huomattavasti 1900-luvulla. Voidaan kuitenkin sanoa, että suurin yksittäinen tekijä salaustekniikan kehittämisessä eteenpäin oli toinen maailmansota. /2, s. 19 - 21/

Saksalaisten kehittämällä Enigma-salauskoneella oli merkittävä vaikutus sodan kulkuun. Enigma oli kirjoituskonetta muistuttava laite, jonka näppäimistölle syötetyt merkit kulkivat sähköisesti kolmen roottorin läpi, myöhemmin laitteeseen myös lisättiin roottoreita salauksen parantamiseksi. Jokaisessa roottorissa oli paikka 26 aakkoselle, yhden merkin koodauksen jälkeen roottori pyörähti eteenpäin. Jotta Enigmaa voitiin tulkita, molemmilla osapuolilla tarvitsi olla koodikirja, josta luettiin päivittäin vaihtuvat alkuasetukset. Enigman lopullinen murtuminen tapahtui oikeastaan vasta englantilaisten onnistuttua kaappaamaan käytössä olleen koodikirjan. Enigman tapaisia mekaanisia salauskoneita käytettiin joissain maissa jopa 1990-luvulle asti. /2, s. 21 - 24/

Siirryttäessä historiassa eteenpäin saavutaan radioliikenteen ja tietoverkkojen aikaan. Alussa ei ollut muuta keinoa salata oma viestintä, kuin hankkia oma radiolähetin ja sopia vastaanottajan kanssa, milloin lähetetään viestejä. Suurin murros tapahtui kuitenkin 1970-luvulla, jolloin

kansallinen rahaliikenne oli siirtymässä sähköiseen muotoon ja tarvittiin turvallista tapaa hoitaa rahaliikennettä pankkien välillä. Tässä tapauksessa mukaan tuli IBM, joka kehitti DES-salauksen ja antoi sen pankkien käyttöön. DESin toimintaa käsitellään tarkemmin luvussa 2.1.1990-luvun puolivälissä tapahtui salauksen lopullinen läpimurto, internetin ja langattoman matkaviestinnän ansiosta. /2, s. 24 - 25/

2.1 Symmetrinen salaus

Tietotekniikan yleistyessä ja maailman muuttuessa ykkösiksi ja nolliksi tarvittiin varma keino luottamuksen saavuttamiseksi, tässä tapauksessa käyttöön otettiin salaustekniikat. Symmetrisellä salauksella tarkoitetaan tekniikkaa, jossa bitit sekoitetaan. Pääperiaattteena on sotkenta ja hajoitus, joka tunnetaan myös Claude Shannonin ajatuksena hyvästä salaimesta. Salaimen täytyy siis sotkea teksti niin, ettei siitä saa selvää eikä näe yhteyttä alkuperäiseen tekstiin. Lisäksi salaimen täytyy hajoittaa selvätekstissä esiintyvät toistot niin ettei niistä huomata säännönmukaisuutta. Symmetriset salaimet voidaan vielä jakaa lohko- ja jonosalaimiksi. /2, s. 77 - 78/

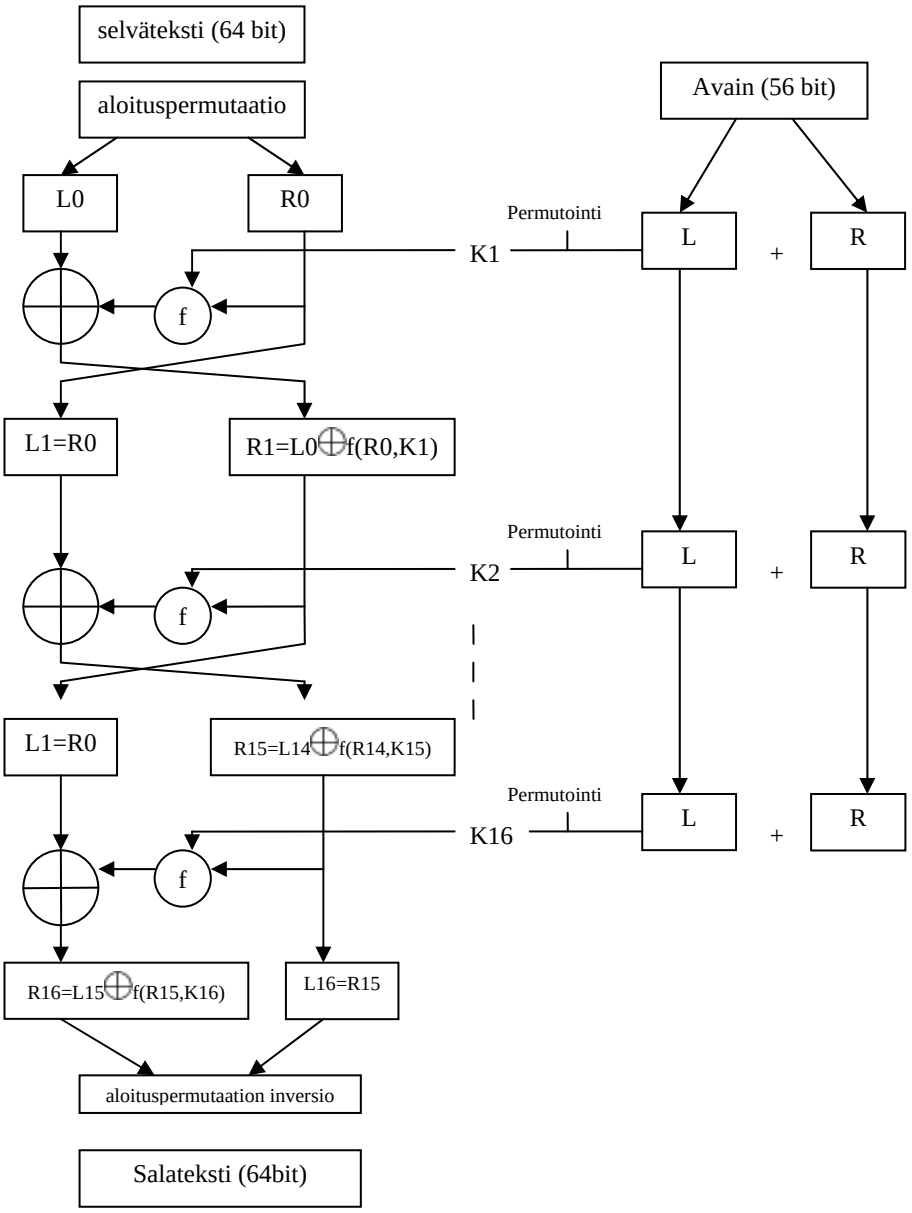
Lohkosalain (block cipher) käsittelee tekstiä lohkoina, joiden tyypilliset koot ovat 64 ja 128 bittiä. Lohkosalain käyttää samaa avainta lohkojen salaukseen. /2, s. 77 - 78/

Jonosalain (Stream cipher) taas käsittelee tekstiä yksiköissä, bitti tai merkki kerrallaan, vaihtaen samalla avainta jokaisen salausoperaation jälkeen. Itse salaus tapahtuu XOR-operaatiolla yhdistämällä käytetty avain ja selväteksti. Saadaan siis avainjono, jonka tuottamiseen tarvitaan jokin algoritmi, joka taas täytyy alustaa käyttäjien valitsemalla avaimella. Jonosalainta voidaan sanoa synkroniseksi, jos se tuottaa avainjonoa itsenäisesti, eli salateksti tai selväteksti eivät vaikuta siihen.

Epäsynkroninen se taas on, jos selväteksti vaikuttaa avainten luontiin. /2, s. 77 - 78/

Symmetrinen salaus käyttää esimerkiksi seuraavia algoritmeja: DES, 3DES, AES ja RC4. 1970-luvulla IBM alkoi kehittää DES-salausta tutkija Horst Feistellin aiempien töiden pohjalta. Koska haluttiin varmistaa, että salaus ei murru hetkessä, otti IBM yhteyttä tiedustelupalvelu NSA:han. Yhteistyön kautta syntyi vihdoin vuonna 1975 DES-salausjärjestelmä, josta tuli myös Yhdysvaltojen virallinen salaustandardi pari vuotta myöhemmin. DESin tehollinen avainpituus oli 56 bittiä, ja se käytti erilaisia lohkoja ja monenlaisia siirtoja ja kierroksia. Sen toimintaa kuvataan tarkemmin kuviossa 1. /2, s. 87 - 91/

Kuviosta 1. nähdään että selvätekstille tehdään aluksi aloituspermutaatio, jolla tarkoitetaan tapaa järjestää käsitellyt bitit uudestaan. Aloituspermutaation jälkeen tehdään 16 kierrosta, jonka jälkeen saadaan aikaiseksi salateksti. Ensimmäisellä kierroksella teksti jaetaan kahteen osaan, L ja R. Samaan aikaan saadaan myös silloin käytetystä avaimesta permutaation avulla luotua avain K1, jota käytetään yhdessä funktion f kanssa. Jokaisella kierroksella luodaan uusi avain K. Kullakin kierroksella R-lohkon sisältö menee funktiolle f kierrosavaimen kanssa. Tästä saatu tulos xorataan yhteen L-lohkon kanssa ja saatu tulos siirtyy seuraavan kierroksen R-lohkoksi. Ensimmäisen kierroksen R-lohko toimii seuraavan L-lohkona. Näin edetään kunnes 16-kierrosta on tehty, minkä jälkeen lohkot yhdistetään ja yksi kokonainen lohko on käsitelty. Funktio f sisältää kolme toimintoa: laajennus, S-laatikko ja permutointi. Näistä tärkein on S-laatikko, se nimensä mukaisesti korvaa sisään tulevan bittiyhdistelmä toisella, millä voidaan estää voidaan estää differentiaalinen kryptoanalyysi. /2, s. 87 - 91/



Kuvio 1: DES-salauksen toiminnan kuvaus. /2. s. 89/

Itse DES-algoritmi on hyvin suunniteltu eikä siitä ole löydetty varsinaisia heikkouksia. Ainoa tapa murtaa se on brute force -menetelmä. Tämä tarkoittaa tapaa kokeilla kaikkia mahdollisia avaimia kunnes oikea löytyy. DESin avainpituus on 56 bittiä, eli avainmahdollisuuksia on 2^{56}, joka tarkoittaa reilua 72 tuhatta biljoonaa. DESin olemassaolon aikana on kehitetty monia laitteita kokeilemaan tuota avainmäärää, ja nykyaikaisilla koneilla ja menetelmillä löydettäisiin avain muutamassa tunnissa. /2, s. 93 - 94/

Seuraava suuri askel symmetrisen salauksen historiassa oli hanke tehdä DESille seuraaja. Siitä järjestettiin avoin kilpailu, jonka voittajaksi selviytyi Rijndael-menetelmä. Näin sai alkunsa AES (Advanced Encryption Standard). Avainpituus AES:ssä voi olla mikä tahansa 32:n monikerta ja lohkon koko on 128 bittiä. DESistä poiketen AES käyttää vain yhtä 256 alkion S-laatikkoa ja on näin nopea ja elegantti. AESää käytetään nykyään hyvin monissa erilaisissa salausta vaativissa järjestelmissä. AES hyväksyttiin myös Yhdysvaltojen viralliseksi salaustandardiksi vuonna 2001. /2, s. 95 - 96/

2.2 Epäsymmetrinen salaus

Epäsymmetrinen salaus eroaa symmetrisestä salauksesta siinä mielessä, että käytetty avain voi olla julkinen, kunhan purkuavain pidetään salaisena. Tästä syystä tekniikkaa kutsutaan asymmetriseksi salaukseksi. Tekniikka pohjautuu yksisuuntaiseen funktioon, joka riittää tiivisteen laskemiseen mutta ei itse salaustekniikaksi. Tarvitaan siis jotain, millä funktio saadaan toimimaan toiseen suuntaan, tätä keinoa kutsutaan salaluukuksi (trapdoor). /2, s. 131 - 132/

Epäsymmetrisessä salauksessa käytetty avain voi siis olla julkinen, joten salaisuutta ei tarvitse jakaa. Käyttäjillä voi olla omat salaisuutensa, jotka kuitenkin toimivat yhteen. Julkisen avaimen järjestelmä käyttää kahta avainta, toista käytetään salaukseen ja toista luonnollisesti purkamiseen. Salausavaimet eivät ole mielivaltaisia, vaan liittyvät toisiinsa matemaattisesti, tavalla jota ulkopuolisen on hyvin vaikea keksiä. Julkisen avaimen paljastumista ei tarvitse pelätä, koska sillä voidaan vain salata, kun taas tähän avaimeen liittyvä yksityinen avain pidetään omana tietona. /2, s. 131 - 132/

Kun halutaan lähettää salattavaa tietoa, se koodataan vastaanottajan julkisella avaimella, jonka jälkeen tiedon voi avata vain henkilö, jolla on julkista avainta vastaava salainen avain. Julkisen avaimen järjestelmä ei ole kuitenkaan täydellinen sillä sen tarvitsemat avaimet ovat paljon pidempiä kuin symmetrisessä salauksessa, avaimet venyvät useisiin tuhansiin bitteihin. Lisäksi epäsymmetriset menetelmät perustuvat vahvasti matematiikkaan ja hyvin suuriin lukuihin, mikä tekee järjestelmästä vaikean toteuttaa ja ennen kaikkea hitaan. RSA-menetelmä on yksi tunnettu epäsymmetristä salausta hyödyntävä menetelmä. Se pohjautuu alkulukuihin, eli lukuihin jotka ovat jaollisia vain ykkösellä ja itsellään. /2, s. 131 - 132, 134 - 136/

3 Salaus langattomissa verkoissa

Kun ajatellaan mitä tahansa langatonta järjestelmää, tulee mieleen heti salaus ja sen tekeminen onnistuneesti ja tehokkaasti. Seuraavaksi tutustutaan hieman tarkemmin muutamiin yleisesti käytössä oleviin langattomiin järjestelmiin sekä niissä käytettäviin salausmenetelmiin.

3.1 Salaus WLAN-verkossa

Wlan-verkkoja on nykyään joka puolella: osa niistä on avoimia ja kaikkien vapaassa käytössä, osa on suojattu oikein ja tehokkaasti. Wlan-verkkojen yleisyyden vuoksi on niiden käyttöön syytä kiinnittää huomiota varsinkin salauksen ja tietoturvan kannalta. IEEE:n 802.11x-standardiin kuuluu se, että käytetttävä taajuus on luokkaa 2,5 tai 5 GHz ja tiedonsiirtonopeudet 6-150 Mbps. Tietoturvamenetelmät, jotka ovat yleisessä käytössä, ovat WEP, AES ja WPA. WLAN-verkon kantama on yleensä noin 50-250 metriä. Langaton tukiasema lähettää oletusarvoisesti omaa SSID-tunnistettaan muutaman sekunnin välein, mutta salauksen ja tietoturvan kannalta tämä toiminto täytyy lopettaa ensimmäisenä. /6, s. 277 - 279/

3.1.1 WEP-salaus

Varsinaiseksi salaukseksi WLANiin suunniteltiin WEPiä (Wired Equivalent Privacy), joka ei varsinaisesti ole tietoturva-algoritmi, eikä sitä sellaseksi ollut suunniteltukaan. Tarkoitus oli ainoastaan suojata langaton verkko samalle tasolle lankaverkon kanssa. Toisin sanoen WEP tekee tiedosta yhtä suojattua kuin se olisi suojaamattomassa Ethernet-verkossa. WEP voidaan asettaa kolmeen eri tilaan: Ei salausta, 40-bittinen salaus,

128-bittinen salaus. WEP konfiguroidaan ennen kuin muodostetaan yhteys tukiasemaan, joten toimiessaan se suojaa kaiken ilmateitse kulkevan tiedon. Ainoa ongelma oli, että WEP:ssä huomattiin vakavia puutteita jo vuoden 2001 alussa. Näistä puhuttaessa täytyy aluksi tietää hieman WEPin toiminnasta. WEP toimii siten, että se yhdistää ”salaisen” WEP-avaimen 24-bittiseen satunnaisesti luotuun lukuun, jota kutsutaan alustusvektoriksi IV (Initialization Vector). 24-bittinen IV liitetään joko 40-bittiseen tai 104-bittiseen WEP-salalauseeseen, joista muodostuu liikenneavain RC4:n avulla, ja näennäisesti saadaan täysi 128-bittiä vahva salaus ja suojaus. Näitä kutsutaan myös nimillä WEP-40 ja WEP-104. /6, s. 304 - 307/

WEP ei kuitenkaan anna tarvittavaa suojausta. Ensimmäinen heikkous on juuri 24-bittisen alustusvektorin koko, sillä mahdollisia arvoja on 2^{24} eli reilut 16 miljoonaa, mikä saattaa kuulostaa paljolta mutta on kattavaan salaukseen riittämätön. Ongelmia syntyy, koska pienen määrän takia arvot ja avaimet alkavat toistua, mikä avaa oven hyökkääjille. Lisäksi kaikki 16 miljoonasta arvosta eivät ole käyttökelpoisia, esimerkiksi numero 1. Yksi suuri heikkous WEP:ssä on myös se, että 64-bittinen ja 128-bittinen salaus käyttävät kumpikin samaa 24-bittistä alustusvektoria. Näistä heikkouksista johtuen WEP on korvattu WPA ja WPA2-standardeilla. /6, s. 304 - 307/

3.1.2 WPA/WPA2-salaus

Kun tarvittiin seuraaja huonolle WEP-salaukselle, aluksi otettiin käyttöön WPA, joka käyttää vain osaa IEEE 802.11i-standardista, mutta WPA:n seuraaja WPA2 hyödyntää standardin pakollisia osia ja ottaa käyttöön uuden AES:ään pohjautuvan CCMP-algoritmin. WPA:n suunniteltiin olevan vain väliaikainen korvaaja WEP:lle kun WPA2 olisi varsinainen 802.11i-standardin hyödyntäjä. WPA2 käyttää tehokasta EAS-lohkosalainta, kun WEP sekä WPA käyttävät vain RC4-jonosalainta. WPA2:n salausprosessiin kuuluu tärkeinä osina luottamuksellisuus, eheys sekä todennus. /15 ; 16/

Todennukseen käytetään 802.1X-standardia, joka hyödyntää EAP-protokollaa, joista yksi käytetyin on EAP-TLS. Protokolla toimii seuraavasti: Ensimmäiseksi tukiasema pyytää asiakkaan todennustietoja. Käyttäjän annettua tiedot lähettää tukiasema annetut tiedot RADIUS-palvelimelle todennusta ja valtuutusta varten. Kun RADIUS-palvelin on suorittanut valtuutuksen, asiakas voi muodostaa yhteyden. Koska tämän prosessin avulla luotiin niin sanottu jaettu pääavainpari PMK, joka säilyy samana koko istunnon ajan, ei sitä myöskään tästä syystä haluta käyttää liikenteessä usein. Täytyy luoda vielä toinen avain, jota kutsutaan PTK:ksi. Tämä avain luodaan nelisuuntaisella kättelyllä, tukiaseman ja langattoman aseman kesken. Wlan-salauksen asettaminen on käytännössä tehty hyvin yksinkertaiseksi. Kun valitaan vahva salasana, voidaaan olla varmoja, että salaus kestää tavanomaisen käytön. /15 ; 16/

3.2 Salaus BLUETOOTH-järjestelmässä

Bluetooth on lyhyen kantaman radiotekniikkaan perustuva langaton tiedonsiirtotekniikka, jota käytetään yleisesti matkapuhelinten lisälaitteita hyödynnettäessä. Bluetoothin tarkoitus oli myös syrjäyttää IrDA, koska siinä voidaan käyttää salausta ja yhteyslaitteiden todennusta. Bluetoothin yksi tärkeimmistä toimenpiteistä salauksen kannalta on parinmuodostus, joka perustuu usein kahteen salaiseen avaimeen, eli molemmat laitteet syöttävät saman Bluetooth PIN-numeron ja näin muodostavat parin. /1, s. 79 - 86/

Varsinainen pakettien salaus ja luottamuksellisuus saadaan aikaan E0-nimisellä jonosalaimella. E0 luo pseudosatunnaisia lukuja ja yhdistää ne salattavaan tietoon XOR-operaatiolla. Avainpituus vaihtelee mutta yleisesti käytössä on 128-bittiä. Parinmuodostus voi myös tapahtua ilman että toiseen laitteeseen tarvitsee syöttää PIN-koodia. Tälläisiä ovat esimerkiksi langattomat Bluetooth handsfree -kuulokkeet. Näissä PIN-koodi on tehdasasetettu itse laitteeseen. /1, s. 79 - 86/

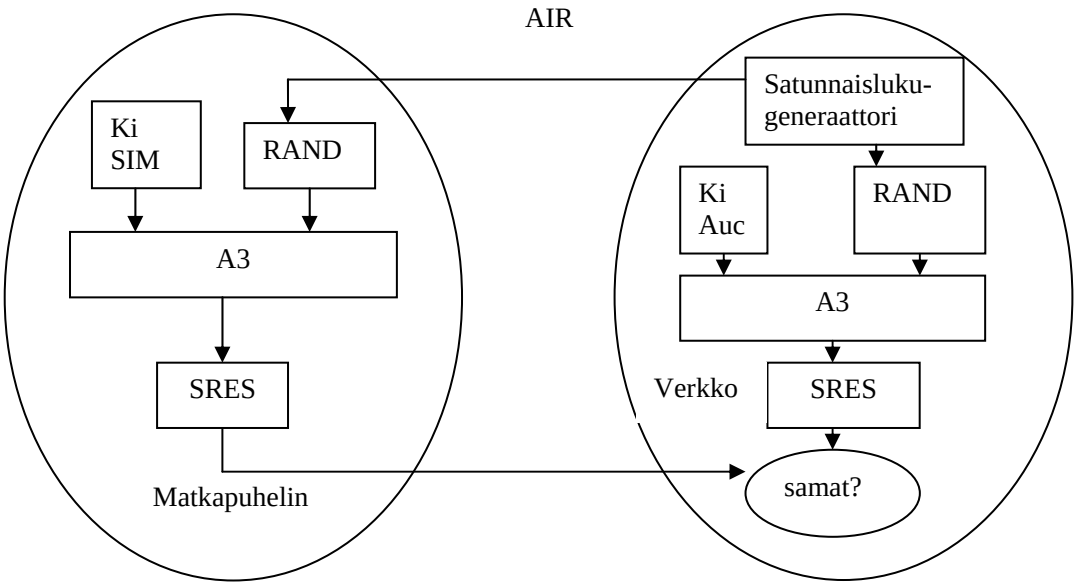
3.3 Salaus GSM-järjestelmässä

Kaikkien tunteman ja käyttämän GSM:n eli 2G-järjestelmän salaukseen tutustuminen alkaa perusteista. Joka puhelimissa täytyy olla SIM-kortti, jos sillä halutaan soittaa tai lähettää viestejä. Ilman SIM-korttia voi ainoastaan soittaa yleiseen hätänumeroon. SIM-kortti sisältää tilaajaan tunnistukseen tarvittavia tietoja sekä operaattorikohtaisia salaisia avaimia. SIM-kortti onkin tärkein turvallisuuteen liittyvä ominaisuus, ja siihen kuuluvan IMSI-koodin (International Mobile Subscriber Identify) perusteella operaattori osaa laskuttaa asiakasta. Kortilla on myös salainen tunnistusavain Ki sekä salausalgoritmit A3 ja A8. Myös puhelimessa itsessään on turvakoodi, jota kutsutaan IMEI:ksi (International Mobile Equipment Identity). IMEI:n avulla voidaan puhelin asettaa mustalle listalle, eli estää sen käyttö. GSM-puhelun salakuuntelua vaikeuttaa myös se, että käytössä on GMSK-modulointi, taajuushyppely ja aikajakokoodaus eli TDMA-kehykset. Kaiken tämän lisäksi liikenne vielä salataan. Seuraavaksi hieman tarkemmin tilaajan tunnistuksesta. /2, s.310 - 312 ; 4/

3.3.1 Tilaajan tunnistus

Käyttäjän halutessa verkkoon käynnistyvät tilaajan tunnistustoiminnot, jotka on kuvattu kuviossa 2. Aluksi verkko lähettää puhelimelle satunnaisen luvun RAND, joka on väliltä 0 - 2^{128}-1, eli 128-bittiä. SIM-kortin sisällä lasketaan 32-bittinen kuittausparametri SRES. Tämä tapahtuu algoritmin A3, satunnaisluvun RAND sekä tilaajakohtaisen tunnisteavaimen Ki (Authentication Key, 128-bittiä) avulla. Tämän laskettuaan lähettää puhelin kuittausparametrin (SRES) verkolle, joka tarkistaa lasketun SRESin arvon tekemällä saman laskutoimituksen.

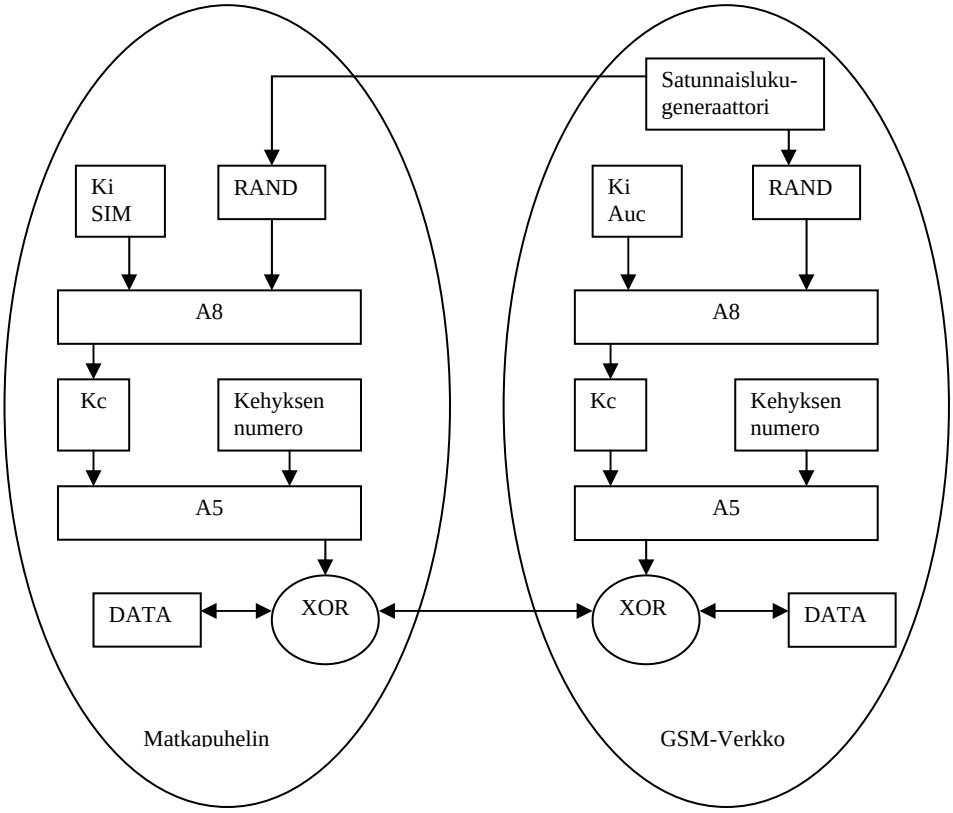
Verkko toisin sanoen tietää käytetyn Ki-arvon. SRES-arvojen ollessa samat pääsy verkkoon on sallittu. /2, s.310 - 312 ; 4/



Kuvio 2: Tilaajan tunnistus ja pääsy verkkoon. /4, s. 55/

3.3.2 Radiorajapinnan salaus

Radiorajapinnan ja puheluiden salaukseen tarvitaan algoritmia A5, salausavainta Kc sekä algoritmiä A8. Salausavain Kc asetetaan aina tilaajan tunnuksen tarkistuksen yhteydessä; se myös lasketaan jokaista yhteyttä varten erikseen. Kc lasketaan matkapuhelimessa algoritmin A8 avulla, ja sitä ei siirretä suoraan radiotiellä, ainoastaan RAND-satunnaisluku siirtyy radiotiellä. Salaus on luonnollisesti syknoroitu sekä purku että lähetyspäässä käyttäen kehysnumerointia. Salauksen kulku etenee seuraavasti: Aluksi suoritetaan tilaajan tunnistus kuten edellä on kuvattu. Tämän jälkeen lasketaan salausavain Kc, algoritmilla A8, käyttämällä satunnaislukua RAND sekä avainta Ki. Varsinainen bittien salaus tapahtuu XOR-funktiolla kullekin purskeelle erikseen. XOR-funktioon tarvitaan algoritmin A5 tulosta, joka saadaan kehysnumerosta ja Kc-avaimesta. Samanlainen operaatio tehdään myös GSM-verkossa. Kuviossa 3 on esitelty radiorajapinnan salaus. /4/

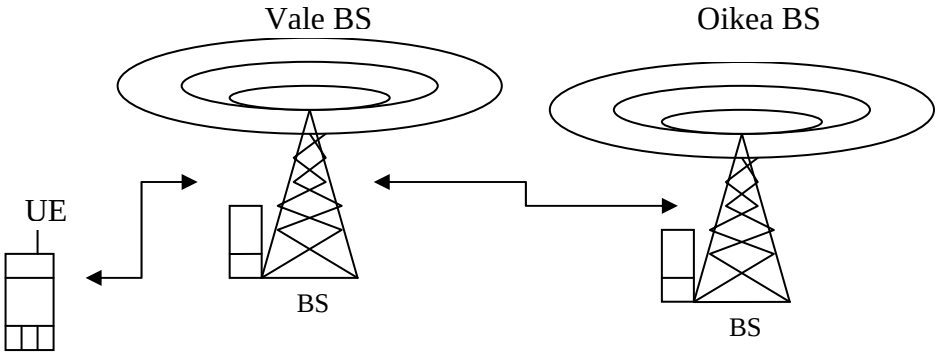


Kuvio 3: Radioliikenteen salaus datan lähetyksessä. /4, s.62/

3.3.3 Vahvuudet ja heikkoudet

GSM-järjestelmän vahvuuksina voidaan pitää todennustapaa, jossa käyttäjä tunnistetaan verkkoon, ja näin estetään asiattomien pääsy verkkoon. Toinen vahvuus on myös luvussa 3.3.2 esitelty tyyli salata radiotie puhelun ajaksi ja näin suojata käyttäjien puheluita salakuuntelulta. Viimeinen tärkeä seikka ja vahvuus GSM-järjestelmässä on väliaikaistunnisteiden käyttö. Näistä mainittakoon TMSI:n käyttö IMSIn sijaan, joten tärkeää IMSI-koodia ei lähetä verkossa turhaan. /3, s. 7 - 8/

GSM-järjestelmä yleistyi nopeasti ja on edelleen todella käytetty järjestelmä. Tästä syystä siinä on myös havaittu monia heikkouksia. Yksi suurimmista huolenaiheista on niin sanottu aktiivinen hyökkäys. Millä tarkoitetaan sitä että henkilö, jolla on tarvittavat resurssit käytössään, voi naamioida itsensä päteväksi verkkoelementiksi ja näin päästä käsiksi verkossa kulkevaan tietoon. Esimerkki tästä on kuviossa 4. /3, s. 7 - 8/



Kuvio 4: Aktiivinen hyökkäys, tukiasemaksi naamioitu laite sieppaa signaalit. /3, s. 8/

Toinen huolenaihe GSM-järjestelmässä on herkän ohjaustiedon, esimerkiksi avainten, joita käytetään radiotien salaukseen, lähettäminen ilman salausta verkosta toiseen. Lisäksi GSM:ssä jätettiin tärkeitä salausarkkitehtuurin tietoja salaisiksi, mikä luo vain epätietoisuutta niiden toiminnasta, eikä niitä myöskään voida tutkia ja todeta hyviksi. Myös radiotien salaamiseen käytetyt avaimet tulevat ajan kuluessa alttiiksi suurelle ”brute force”-hyökkäykselle, missä väärinkäyttäjä kokeilee kaikkia mahdollisia yhdistelmiä kunnes osuu oikeaan. Kaikki nämä kohdat jätettiin tahallaan GSM:ssä vaille suurempaa huolenaihetta, koska ajateltiin, että niiden ehkäisemiseen käytetyt resurssit olisit suurempia kuin hyödyt. /3, s. 7 - 8/

3.4 Salaus 3G-järjestelmässä

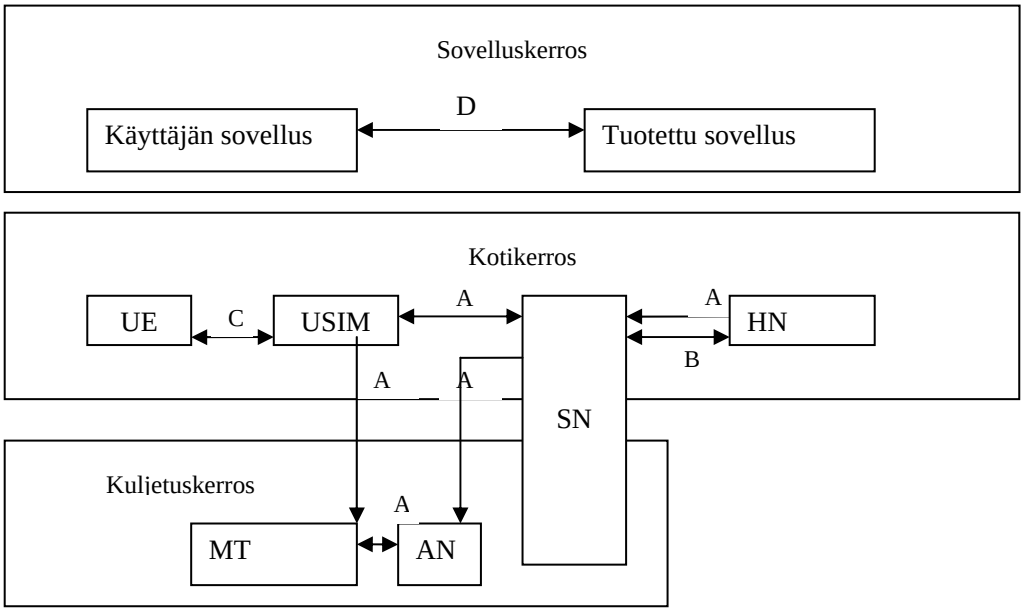
3G-järjestelmä, kutsutaan myös nimellä UMTS, haluttiin tietysti suunnitella turvallisemmaksi kuin vanha 2G-järjestelmä, vaikka toisaalta 3G käyttää ja suunniteltiin alunperin käyttämään hyväksi monia GSM-järjestelmästä tuttuja ja toimivaksi todettuja osia. Kuitenkin jo tilaajan tunnistusvaiheessa tulee pieni muutos GSM-järjestelmään verrattuna. Suurin etu uudessa tavassa on, että myös tilaaja tarkistaa kuuluvansa oikeaan verkkoon. 3G-verkko käyttää ns. kvintettiä tunnistukseen, se koostuu siten viidestä eri osasta. /8 ; 10/

Kuten GSM-järjestelmässä käytetään myös 3G:ssä satunnaislukua RAND, salausavainta Ck sekä kuittausparametriä RES, jota 3G:ssä kutsutaan nimeltä XRES. Uusina tulevat käyttöön Ik-avain (integrity key) sekä AUTN (authentication token). AuC luo AUTN:n käyttäen satunnaislukua sekä käyttäjäkohtaista salaista avainta, minkä jälkeen avain lähetetään satunnaisluvun kanssa puhelimelle, mutta kaikki muut arvot pysyvät MSC:llä tai VLR:ssä. AUTN:n avulla matkapuhelin tarkistaa, että verkko on oikea ja hyväksyttävä. AUTN sisältää myös numeroinnin, joka kasvaa aina onnistuneissa todennuksissa. Lopuksi puhelin vielä laskee oman kuittaisparametrinsa XRESin, jota verkko vertaa omaansa. Jos parametrit täsmäävät, tilaaja on tunnistettu onnistuneesti. /8 ; 10/

3.4.1 3G-järjestelmän tietoturva

Kuviossa 5 on esitettynä periaatekuva 3G-järjestelmän tietoturvasta ja eri kerrosten ja kohteiden yhteyksistä toisiinsa. A-kirjaimella merkityt viivat kuvaavat verkkoliitynnän turvallisuutta. 3G-järjestelmä toisin sanoin tarjoaa turvallisen väylän verkkoon ja suojaa radiolinkkiä siihen kohdistuvilta uhilta. B-kirjain kuvaa turvallista liityntää lankaverkkoon

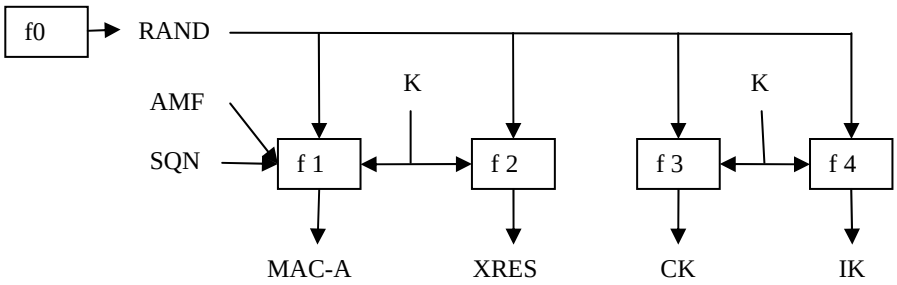
sekä takaisin yhteydentarjoajan verkkoon. C-kirjain taas tarkoittaa turvattua yhteyttä päätelaitteille eli matkapuhelimiin. D-kirjain merkitsee turvattua yhteyttä käyttäjän sovelluksien ja tuotettujen sovelluksien välillä. /8/



Kuvio 5: 3G-järjestelmän tietoturvan periaatekuva. /8/

Muutoksia GSM:ään verrattuna on tapahtunut myös salaimen käytössä, sillä 3G käyttää A5/1-jonosalaimen sijaan KASUMI-lohkosalainta. Tätä salainta hyödynnetään funktioissa f0 - f5 sekä f8 ja f9, joista tarkemmin seuraavaksi. Funktiota f8 käytetään luottamuksellisuuden luomiseen ja f9:ää tiedon eheyteen. Funktio f8 käyttää synkronoitu jonosalainalgoritmia ja suojaa näin käyttäjän lähettämiä tietoja sekä signalointia radiotiellä. Funktiot f8 ja f9 sijaitsevat sekä UE:ssä (user equipment) että RNC:ssä. (radio network controller). Funktiot f1 - f5 sijaitsevat AuC:ssä sekä USIM:llä, f0 taas sijaitsee vain AuC:ssä. Funktiota f0 käytetään kehittämään satunnaisluku RAND, kun taas funktio f1 on verkon tunnistusta varten. Se käyttää tilaaja-avainta K sekä SQN, RAND ja AMF-arvoja luodakseen MAC-A:n. Funktiota f2 käytetään tilaajan tunnistukseen. Tämä funktio käyttää myös K-avainta ja satunnaislukua luodakseen RES- tai XRES-arvon. Funktiolla f3 luodaan CK-avain (cipher

key) käyttämällä K-avainta ja RANDia. IK (integrity key) luodaan funktiolla f4, tähän tarvitaan RANDia sekä avainta K. Funktio f5 luo avaimen AK (anonymity key), johon käytetään avainta K sekä satunnaislukua RAND. Kuviossa 6 on kuvattu nämä toiminnot. Näin saadaan luotua avaimet, joilla suojataan radiotietä ja todennetaan sekä käyttäjä että AuC. /7 ; 10 ; 3/

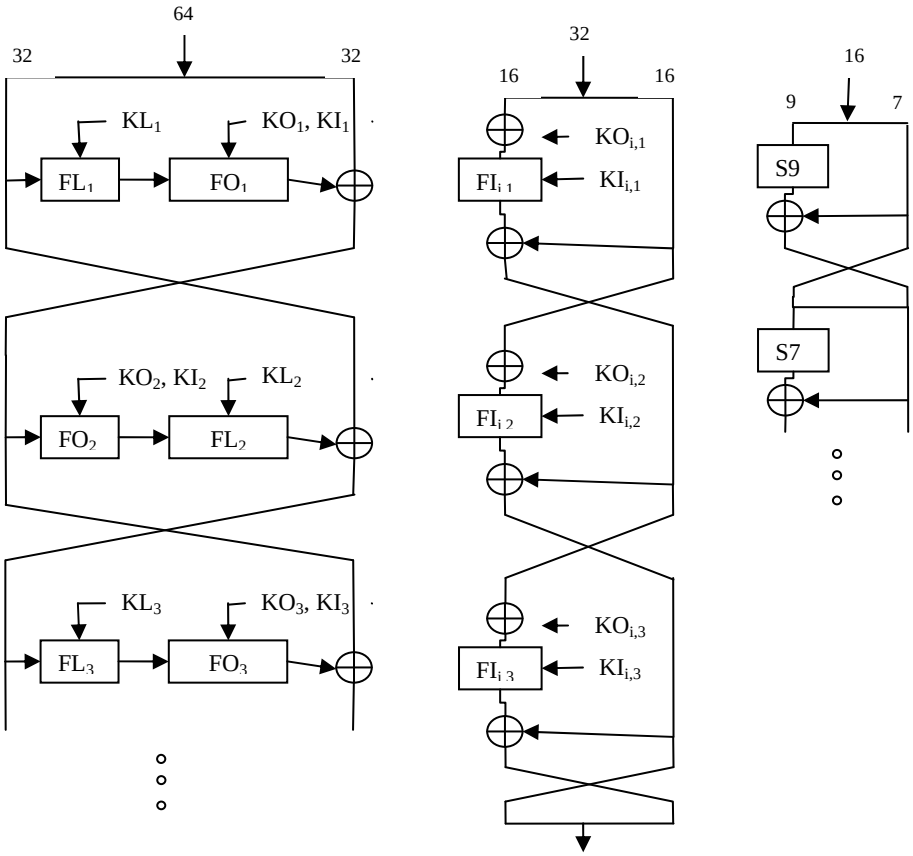


Kuvio 6: Funktioiden käyttö ja avainten luontiprosessi. /3, s. 203/

3.4.2 Kasumi-salaimen toiminta

Kasumi pohjautuu MISTY1-nimiseen salaimeen, johon tehtiin joitain muutoksia sen yksinkertaistamiseksi ja nopeuttamiseksi. Kasumi on kahdeksan kierroksen Feistel-salain. Feistel oli saksalaissyntyinen kryptoanalyytikko, ja hänen ideoimansa salaimet olivat symmetrisiä eli salaus ja purku tapahtuivat lähes samalla tai jopa täysin samalla tavalla. Kasumi käyttää 64-bitin lohkokokoa ja 128-bitin avainta. Kierrosfunktiota, jota käytetään jokaisella i:nellä kierroksella merkitään fi:llä. Tällä funktiolla on 32-bittinen sisääntulo ja 32-bittinen ulostulo. Jokainen Kasumin kierrosfunktioista koostuu kahdesta toisesta funktiosta FL ja FO. FO-funktio taas on määritelty verkoksi, joka käyttää kolmea sovellusta FI-nimisestä funktiosta. FI-funktio koostuu verkosta, joka käyttää kahta sovellusta S9-funktiosta ja kahta sovellusta S7-funktiosta. Näitä kutsutaan myös Kasumin S-laatikoiksi, hieman samaan tapaan kuin

jo aikaisemmin esitellyt DES:n S-laatikot. Näin ollen Kasumi koostuu kerroksista funktioita, joita käytetään yhdessä aliavainten KL, KO ja KI kanssa. Periaatekuva KASUMIn toiminnasta on kuviossa 7. /7 ; 10 ; 3/



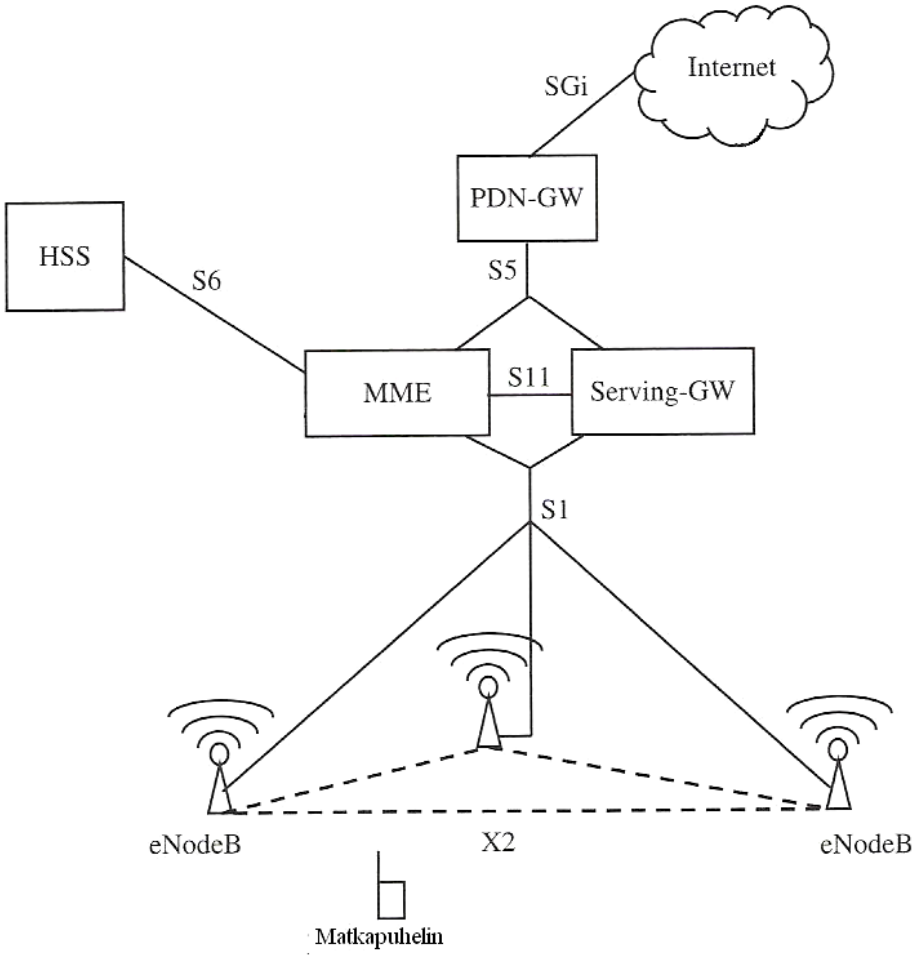
Kuvio 7: KASUMIn toimintakuva, kuvassa vasemmalla kierrokset, keskellä FO-funktio ja oikealla FI_i-funktio. /3, s.180/

3.5 Salaus LTE-järjestelmässsä

LTE on seuraava kehitysaskel langattomissa matkapuhelinjärjestelmissä, puhutaan 3,9G-järjestelmästä, koska se ei aivan täysin täytä kaikkia 4G:n vaatimuksia. Tämä järjestelmä on kuitenkin otettu käyttöön jo

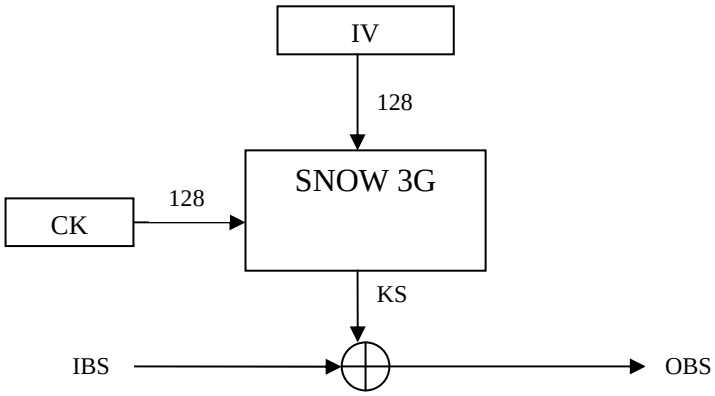
muutamassa suuressa pohjoismaisessa kaupungissa. Suurinpana kehitysaskeleena voidaan pitää siirtymistä kokonaan IP-pohjaiseen verkkoon, eli päätelaitteelle annetaan IP-osoite heti kun rekisteröityminen verkkoon tapahtuu. IP-pohjainen arkkitehtuuri perustuu SAE (System Architecture Evolution) alustaan. Tälläinen verkko luo uusia haasteita salaukselle ja tietoturvalle. /5 ; 13/

Käytössä on niin sanottu tasainen arkkitehtuuri, jossa kaikki radioliikenneprotokollat päättyvät eNB:hen (enhanced nodeB), joka toimii LTE-verkossa tukiasemana. Kuviosta 8 nähdään LTE-verkon rakenne. LTE-verkossa ei ole varsinaista verkon keskustahallintaa, mistä johtuen eNB:t toimivat autonomisesti ja määräävät radiorajapinnasta sekä vastaavat myös palvelun laadusta (QoS). Kuviosta nähdään myös, että tukiasemat kommonikoivat keskenään uuden rajapinnan X2 avulla. eNB:n jälkeen radiorajapinta jakaantuu kahteen eri kohteeseen MME:hen (Mobility Management Entity) sekä Serving-GW:hen (serving gateway). Näistä kahdesta MME hoitaa tunnistuksen *haaste-vaste*-menettelyllä sekä valitsee parhaan reitin ulos verkosta. MME hoitaa myös liikenteenohjauksen LTE-, GSM- ja UMTS-verkkojen välillä. Samaan tapaan kuin GSM- ja 3G-verkoissa, myös LTE:ssä käytetään IMSI:n lähettämisen sijaan väliaikaistunnusta, tässä yhteydessä nimeltä GUTI (Globally Unique Temporary Identity). MME hoitaa näiden tunnusten jakamisen päätelaitteille. LTE-verkossa PDN-GW hoitaa rajareitittimen virkaa eli piilottaa tilaajan liikkuvuuden sekä hallitsee ja jakaa IP-osoitteita päätelaitteiden rekisteröityessä verkkoon. Myös LTE-verkossa käytetään kotirekisteriä nimeltä HSS (Home Subscriber Server). /5, s. 46 - 49 ; 12/



Kuvio 8: LTE-verkon rakenne. /5, s. 47/

LTE:ssä käytetyiksi salaimiksi on määritelty AES ja SNOW 3G. Näistä AES:ää on käsitelty hieman jo tämän työn luvussa 2.1. SNOW 3G taas on symmetrinen jonosalain, jota LTE:ssä käytetään UEA2 ja UIA2 nimisissä algoritmeissa. UEA2 on siis uusi luottamuksellisuus algoritmi, jonka toiminta näkyy kuviossa 9. UEA2 käyttää IV:tä sekä CK:ta luodakseen KS:än eli avainjonon, joka sen jälkeen xorataan IBS:ään eli sisääntulevaan bittivirtaan. Tulokseksi saadaan OBS, eli ulostuleva bittivirta. /14 ; 11/



Kuvio 9: UEA2:n toiminta kuvaus. /11/

Myös UIA2 käyttää IV:tä ja CK:ta, mutta tulokseksi saadaan kolme satunnaisarvoa, 64-bittiset P ja Q sekä 32-bittinen OTP. Näitä käytetään myöhemmin XOR-operaatioissa. Lopulliseksi tulokseksi saadaan 32-bittinen MAC (Message Authentication Code). Toisin sanoen UEA2:ta käytetään samaan tarkoitukseen kuin 3G:n funktiota f8 ja UIA2:ta taas käytetään samoin kuin funktiota f9. /11/

4 Päätelmät

Työssä tutustuttiin alussa hieman salauksen historiaan ja yleisiin salausmenetelmiin ja tyyleihin, käytiin läpi niin symmetrinen salaus kuin epäsymmetrinenkin. Tämän jälkeen syvennyttiin tutkimaan erilaisia tänä päivänä suosittuja langattomia järjestelmiä ja niissä käytössä olevia salaustekniikoita ja algoritmeja. Käytiin läpi WLAN, Bluetooth, GSM-, 3G- ja LTE-järjestelmät.

Salauksiin tutustuttaessa huomataan suurta kehitystä tapahtuneen, mikä ei ole yllätys, kun ajatellaan tietotekniikan kehittymisnopeutta, erityisesti piirien nopeuden kasvamista. Tarvitaan yhä tehokkaampaa salausta pitämään ei-toivotut salakuuntelijat loitolla. Nähdään myös, että salaukset eivät tule katoamaan tästä maailmasta. Omat asiat halutaan edelleen pitää yksityisenä ja omana tietonaan ja kukapa haluaisi nettipankkien tunnuksiaan kaapattavan.

Kun ajatellaan salausta tietoturvan kannalta, on sillä vain pieni merkitys. Salaus on vain työkalu, jolla saavutetaan osa tietoturvaa. Suurin osa tulee käyttäjän omista toimista sekä siitä miten hyvin käyttäjä hoitaa puhelintaan, verkkoaan ja muita langattomia laitteitaan. Ihmisten täytyy huomata, että riskejä on joka puolella langattomassa maailmassa. Yhä enemmän tietoa siirtyy verkkoihin ja yksityisyys tuntuu katoavan. Myös ihmiset, jotka haluavat ja osaavat väärinkäyttää näitä langattomassa maailmassa liikkuvia tietoja, lisääntyvät. Täytyy siis kiinnittää huomiota siihen missä ja miten käyttää langattomia järjestelmiä.

LÄHTEET

Painetut lähteet

1. Imai, Hideki 2006. Wireless communications security. Massachusetts: Artec house, inc.

2. Järvinen, Petteri 2003. Salausmenetelmät. 1. painos. Jyväskylä: Docenda Finland Oy

3. Nyberg, Kaisa, Niemi, Valtteri 2003. UMTS security. West Sussex: John Wiley & Sons Ltd.

4. Rantala, Ari 2000. GSM-järjestelmä.

5. Sauter, Martin 2009. Beyond 3G, Bringing networks, terminals and the web together. West Sussex: John Wiley & Sons Ltd.

6. Thomas, Tom 2005 Verkkojen tietoturva: perusteet. Helsinki: Edita Prima Oy.

Sähköiset lähteet

7. 3GPP TS 33.102 V9.1. 2009 Saatavissa:
http://www.3gpp.org/FTP/Specs/html-info/33102.htm

8. GSM and UMTS Security [www-sivu] [viitattu 30.3.2010] Saatavissa:
http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group7/index.html

9. Mobilesociety [www-sivu] [viitattu 29.3.2010] Saatavissa:
http://mobilesociety.typepad.com/mobile_life/2007/01/deep_inside_the.html

10. Nyberg, Kaisa 2004. Cryptographic algorithms for UMTS. [PDF-tiedosto] 18s. Saatavissa:
http://www.tcs.hut.fi/Publications/knyberg/eccomas.pdf

11. Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. 2006. [PDF-tiedosto] Saatavissa:
http://gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsm_security_algorithms.htm#nav-6

12. Valtteri, Niemi 2009 3GPP security hot topics: LTE/SAE and Home (e)NB. [PDF-tiedosto] Saatavissa:
http://docbox.etsi.org/Workshop/2009/200901_SECURITYWORKSHOP/NOKIA_ValtteriNiemi_3GPPSecurityHotTopics_LTESAEandHome%28e%29NB.pdf

13. Wikipedia [www-sivu] [viitattu 30.3.2010] Saatavissa:
http://en.wikipedia.org/wiki/3GPP_Long_Term_Evolution

14. Wikipedia [www-sivu] [viitattu 5.4.2010] Saatavissa:
http://en.wikipedia.org/wiki/SNOW

15. Wikipedia. [www-sivu]. [viitattu 9.3.2010] Saatavissa:
http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

16. Wikipedia. [www-sivu]. [viitattu 9.3.2010] Saatavissa:
http://en.wikipedia.org/wiki/IEEE_802.11i-2004