Міністерство освіти і науки України
Тернопільський національний економічний університет
Факультет комп'ютерних інформаційних технологій
Кафедра спеціалізованих комп'ютерних систем

ПУКАНЮК Юрій Миколайович

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ / INFORMATION SECURITY IN MOBILE COMMUNICATION SYSTEMS

спеціальність: 8.05010203 – Спеціалізовані комп'ютерні системи
магістерська програма – Спеціалізовані комп'ютерні системи

Дипломна робота за освітньо-кваліфікаційним рівнем "магістр"

Виконав студент групи СКСм-21
Ю.М. Пуканюк
_____

Науковий керівник:
к.т.н., доцент А.І. Сегін
_____

Дипломну роботу допущено до захисту:
"____"_____20___ р.

Завідувач кафедри
_____ Я.М. Николайчук

Тернопіль 2017

РЕФЕРАТ

Дипломна робота складається із переліку умовних скорочень, вступу, чотирьох розділів, висновків і списку використаних джерел. Основний зміст викладений на 81 сторінці друкованого тексту, містить 23 рисунки і 11 таблиць. Список використаних джерел містить 33 найменування.

Мета роботи. Проаналізувати мобільні стандарти які використовуються у світі, як відбувається в них захист інформації,а також провести криптоаналіз і модифікувати шифрування Kasumi, а також програмно реалізувати шифрування.

Методи дослідження. Дослідження алгоритму шифрування Kasumi, сучасних систем мобільного зв’язку, аналіз їхніх технічних характеристик і захисту інформації в них.

Результати роботи. Результати роботи дає змогу досліджувати надійність мобільних систем та її криптографічних компонент, які забезпечують цілісність та конфіденційність даних, що передаються шляхом використання алгоритму шифрування Kasumi.

Рекомендації по використанню результатів роботи. Доцільним є проведення порівняльного аналізу різних програмно-апаратних засобів паралельних та розподілених комп'ютерних систем з метою визначення найбільш ефективних на різних етапах крипто аналітичної атаки.

Можливі напрямки розвитку. Даний аналіз дасть змогу розробляти ефективніші крипто аналітичні алгоритми для інших симетричних блокових шифрів.

Ключові слова: шифрування, системи мобільного зв’язку, криптоаналіз, захист інформації, алгоритми.

ABSTRACT

Thesis consists of a list of abbreviations, introduction, four chapters, conclusions and list of references. Main content posted on 81 pages of printed text contains 23 drawing and 11 tables. References contains 33 items.

Purpose of work. Analyze the mobile standards used in the world as there are in information security, and spend cryptanalysis and modify Kasumi encryption and encryption software to implement.

Research methods. Research Kasumi encryption algorithm, advanced mobile communication systems, analysis of their technical characteristics and protection of information in them.

Job performances. The results of work allows to investigate the reliability of mobile systems and their cryptographic components that ensure the integrity and confidentiality of transmitted data using encryption algorithm Kasumi.

Recommendations after the use of job performances. It is reasonable to conduct a comparative analysis of various software and hardware parallel and distributed computer systems to determine the most effective at different stages of crypto analytic attack.

Possible directions of development. This analysis will help to develop effective cryptanalytic algorithms for other symmetric block ciphers.

Keywords: encryption systems, mobile communications, cryptanalysis, information security algorithms.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

СМЗ	–	Стільникові Мережі Зв'язку
EDGE	–	Enhanced Data Rates for Global Evolution
GSM	–	Global System for Mobile communication
UMTS	–	Universal Mobile Telecommunications System
PDC	–	Personal Digital Cellular
CDMA	–	Code Division Multiple Access
ISDN	–	Integrated Service Digital Network
EVDO	–	EVolution Data Only
AMPS	–	Advanced Mobile Phone Service
NMT	–	Nordic Mobile Telephone system
RTMS	–	Radio Telephone Mobile System
NTT	–	Nippon Telephone and Telegraph System
TACS	–	Total Access Communications System
PCN	–	Personal Communication Network
DCS	–	Digital Cellular System
HSCSD	–	High-Speed Circuit-Switched Data
GPRS	–	General Packet Radio Service
IMT	–	International Mobile Telecommunications
UTRAN	–	Universal Terrestrial Radio Access Network
CAVE	–	Cellular Authentication, Voice Privacy and Encryption
CMEA	–	Cellular Message Encryption Algorithm.
USIM	–	User Services Identity Module
AKA	–	Authentication and Key Agreement
1xEV-DO	–	Evolution Data Only
LTE	–	Long-Term Evolution
WiMAX	–	Worldwide Interoperability for Microwave Access

ВСТУП

Актуальність теми. На сьогодні існує досить багато різних систем зв'язку, які суттєво допомагають в роботі та повсякденному житті. Із появою цих систем значно збільшився обмін та потік різноманітної інформації. Особливо у державній, приватній та комерційній сферах, а також законодавчих і виконавчих структур органів державної влади. Однак у системах мобільного зв'язку передавання інформації між мобільною й базовою станціями відбувається радіоканалом, що накладає досить жорсткі вимоги на забезпечення їхньої інформаційної безпеки, що реалізується на основі відповідних криптографічних алгоритмів.

Оскільки інформація дуже важлива, а кількість людей бажаючих заволодіти нею досить велика, то її слід захищати. Тому ,ця тема є досить актуальною в даний час.

Мета дослідження: проаналізувати алгоритми та методи шифрування, в мобільній мережі, та на основі аналізу модифікувати шифрування Kasumi і включити в алгоритм шифрування 3G мережі.

Предметом дослідження є захист інформації в системах мобільного зв’язку.

Об’єктом дослідження є шифрування методом Kasumi та алгоритм його реалізації.

Методи дослідження: Базується на криптоаналізах і методах шифрування в мобільній мережі.

Наукова новизна одержаних результатів. Модифіковано алгортм kasumi та включення його в якості ядра в алгоритм f8 який використовується для шифруваня даних в 3g мережі.

Практичне значення одержаних результатів. Результати роботи дає змогу покращити надійність мобільних систем та її криптографічних компонент, які забезпечують цілісність та конфіденційність даних, що

передаються шляхом використання модифікованого алгоритму KASUMI.

Публікації:

1**.** Пуканюк Ю.М. Методи захисту інформації в системах мобільного зв’язку / Ю.М. Пуканюк// Збірник матеріалів проблемно-наукової міжгалузевої конференції «Юриспруденція та проблеми інформаційного суспільства» (ЮПІС – 2016)». – Івано-Франківськ, – 2016. - С.128-130.

2.Пуканюк Ю.М. Методи та Verilog–бібліотека пристроїв виконання арифметичних операцій в модулярній арифметиці: Всеукраїнський конкурс студентських наукових робіт з напрямку «Інформатика, обчислювальна техніка та автоматизація» / В.І. Пашко, Ю.М. Пуканюк – Вінниця, – 2016. - С. 33.

РОЗДІЛ 1
РОЗВИТОК МОБІЛЬНОГО ЗВ’ЯЗКУ

1.1 Етапи розвитку мобільного зв’язку

На сьогодні існує досить багато різних систем зв'язку, які суттєво допомагають в роботі та повсякденному житті. Чільне місце серед них займають системи мобільного зв'язку. З появою цих систем значно збільшився обмін та потік різноманітної інформації. Однак у системах мобільного зв'язку передавання інформації між мобільною й базовою станціями відбувається радіоканалом, що накладає досить жорсткі вимоги на забезпечення їхньої інформаційної безпеки, що реалізується на основі відповідних криптографічних алгоритмів. Оскільки інформація дуже важлива, а кількість людей бажаючих заволодіти нею досить велика, то її слід захищати. Тому стандарти системи мобільного зв'язку передбачають різноманітні механізми захисту інтересів законних користувачів і мережі від несанкціонованного доступу та незаконного використання інформації. Розгалядаючи захист в мобільному звязку потрібно розуміти, як розвивався сам мобільний звязок і його системи.

Розгладаючи системи мобільного звязку потрібно почати з другого покоління мобільного звязку і його стрімки розвиток. 2G передає цифрований звук, що збільшує надійність зв'язку і підвищує швидкість передачі до 14,4 Кбіт / сек., дозволяючи обмінюватися невеликими текстовими «пакетами» - SMS.

Ще на початку 60-х років минулого століття інженер Пол Баран запропонував американським військовим оцифровувати передану інформацію для збереження її первісного вигляду. Міністерство оборони ідею проігнорувало, але за неї вхопилися цивільні компанії.

Застосування на мобільних мережах технології цифрового сигналу в ефірі, а, отже, виникнення цифрових мобільних мереж і цифрового мобільного

зв'язку дозволило значно збільшити ємність системи, а так само значно покращило якість голосового зв'язку,але на цьому розвиток не зупинився і виникло покоління мобільного зв'язку 2,5G - перехідний етап. Передумовою виникнення даного покоління з'явилася потреба в більшому ресурсі для передачі даних.

Для більш повного розуміння рішення, застосованого для збільшення пропускної здатності передачі даних необхідно дати чітке поняття терміну "залишковий ресурс" це поняття можна розглянути на прикладі з кімнатою і парами людей. Для того, щоб всі пари людей (голосові виклики) розмістилися уздовж стіни , заповнення даної кімнати обов'язково має контролюватися таким чином, щоб уздовж стіни незмінно залишалося місце для нових пар (вільні канали). У випадку, коли абонент бажає провести дзвінок, а немає вільних каналів, система повідомить йому, що "мережа перевантажена" або "Виклик не виконано". Деяка кількість каналів , яка в даний момент не зайнято абонентами, називається залишковим ресурсом. Кожен оператор зв'язку будує свою мережу таким чином, щоб залишковий ресурс обов'язково присутній для забезпечення голосовим зв'язком усіх бажаючих на випадок різкого збільшення кількості тих, що дзвонять.

Основною ідеєю покоління 2,5G є надання користувачу пакетної передачі даних додаткових каналів із залишкового ресурсу. При цьому на початку сесії пакетної передачі даних абоненту призначається все той же, визначений поколінням 2G базовий канал 9,6 кілобіт / сек.

У міру того, як система фіксує повне споживання виділеного ресурсу, абоненту призначаються додаткові канали до тих пір, поки не буде вичерпано залишковий ресурс, або поки даними абонентам не буде досягнута пропускна здатність 153 кілобита / сек. При цьому, як тільки в даному секторі з'явиться абонент, який встановлює голосове з'єднання, система відбере один з додаткових каналів у абонента пакетної передачі даних і виділить його голосовому абоненту. Таким чином, голосові з'єднання мають пріоритет по отриманню ресурсу мережі[1,3].

Через те, що абонентська база оператора, як правило, зростає швидше, ніж нарощується ресурс базових станцій, залишковий ресурс має тенденцію до безперервного зменшення. У свою чергу пропускна здатність в частині пакетної передачі даних на одного абонента неухильно скорочується, що призводить до невдоволення абонентів.

Через такого роду особливостей розподілу ресурсу в ефірі мережі, побудовані на технологіях покоління 2,5G (GPRS, EDGE для GSM, CDMA2000 1x), не можуть забезпечити достатньої пропускної спроможності для застосування мультимедійних додатків (Мобільне телебачення, відео за запитом і т. п.). Тому почався розвиток мультимедійних мереж 3G - високошвидкісна передача даних, мультимедійні додатки[2,5].

Основною ідеєю третього покоління мобільного зв'язку є організація такого розподілу голосу і даних в ефірі, при якому збільшення голосового навантаження ніяк не вплине на швидкість передачі даних. Це рішення полягає в принциповому поділі за різними несучими голосами і даними.

Для мереж CDMA стандартом третього покоління в даний час прийнятий EVDO (EVolution Data Only), для GSM - UMTS.

З постійним розвитком мобільного зв’язку потреба в швидкості передачі даних і якості її збільшується тому стрімко почали розробляються обладнання та стандарти для наступних поколінь стільникового зв'язку. До 3,5G умовно відносять системи зі швидкістю передачі інформації до 10 Мбіт / сек. В основу 4G включена технологія OFDM- ортогенальне частотне розділення каналів з мультиплексуванням, яка при максимальному використанні частотного діапазону дозволяє передавати дані зі швидкостями понад 100 Мбіт / сек.

Саме OFDM лежить в основі самого прогресивного стандарту Wi-Fi - 802.11a.Стільниковий зв'язок зараз розвинений так що одночасно співіснують мережі кількох поколінь, розширюючи для нас, абонентів, вибір способу спілкування на відстані.

Таблиця 1.1

Покоління мобільної телефонії та їх характеристики

Покоління	Розвиток та реалізація мереж	Послуги	Передача даних
1	2	3	4
1G Мобільність	ARP з 1946 р. до 80х NMT з1981 – 2002р. AMPS з 1983 р. до 90х	Телефонний зв'язок (аналогова передача мови)	відсутня
2G Якість, ємність 2,5G Передача даних	GSM, D - AMPS, CDMA з1990р до 2009 GPRS 1999 р CDMA 2000 EDGE	• Телефонний зв'язок (цифрова передача мови) • Прийом / відправка SMS • Прийом / відправка факсів • Голосова пошта • Доступ в Інтернет • Телефонний зв'язок (цифрова передача мови) • Прийом / відправка довгих SMS • Конференції Прийом / відправка аудіо / відео файлів • Прийом / відправка факсів • Голосова пошта • Доступ в Інтернет • Радіо / MP3 Плеєр, Караоке • Мульти-ігри • Послуги, засновані на місцезнаходження клієнта • Потокове відео (тестування)аудио/видео файлів	9,6-14,4 кбіт / с до 153 кбіт/с
3G Високошвидкісна передача даних, мультимедійні додатки	WCDMA UMTS у використанні з 2003 р CDMA 2000 1xEV-DO	• Телефонний зв'язок (цифрова передача мови) • Високошвидкісний доступ в Інтернет • Віддалений доступ до корпоративної мережі • Прийом / відправка текстових повідомлень • Прийом / відправка ел. пошти • Прийом / відправка аудіо / відео файлів	2,4—4,9 Мбит/с
3G		• Голосова пошта • Послуги, засновані на місцезнаходження абонента • Мобільна електронна комерція • Дистанційна медична діагностика • Відео пошта • Відеотелефонія • Високошвидкісний доступ в Інтернет • TV / Відео Плеєр	

Продовження таблиці 1.1

Покоління мобільної телефонії та їх характеристики

1	2	3	4
4G	«LTE-Advanced» «WirelessMAN-Advanced» затвердженні з 2010	Підтримка і покращення всіх послуг 3G	перевищує 10 Мбіт / с

Таким чином, менш ніж за 40 років технології стільникового зв'язку вчинили запаморочливий стрибок. Тепер абонент вже не відчуває географічної прихильності і може користуватися високоякісними телекомунікаційними послугами де б він не знаходився.

1.2 Основні характеристики систем мобільного зв’язку

Слід особливо відзначити, що в стільникового зв'язку зміна поколінь виражена набагато більш яскраво, ніж, скажімо, в індустрії персональних комп'ютерів або іншої подібної техніки. У мобільному світі все чітко: 1G (перше покоління) - це аналоговий зв'язок (стандарт NMT), 2G - покоління цифрового зв'язку з комутацією каналів (стандарти GSM і CDMA), Третє покоління - 3G (стандарт IMT-2000) - передбачає поряд з комутацією каналів і пакетну передачу даних. Про мобільного зв'язку 3G зараз багато говорять буквально як про символ прогресу. Але на наших очах відбувається дивовижна річ: вперед вирівається вже наступне покоління стільникового зв'язку, іменоване 4G (WiMAX, Wi-Fi, LTE). Якщо так піде і далі, то мережі 3G так і не розвинуться в повну силу - їх місце займе 4G. Покоління стільникових мереж зв'язку та етапи їх розвитку представлені на рисунку 1.1.

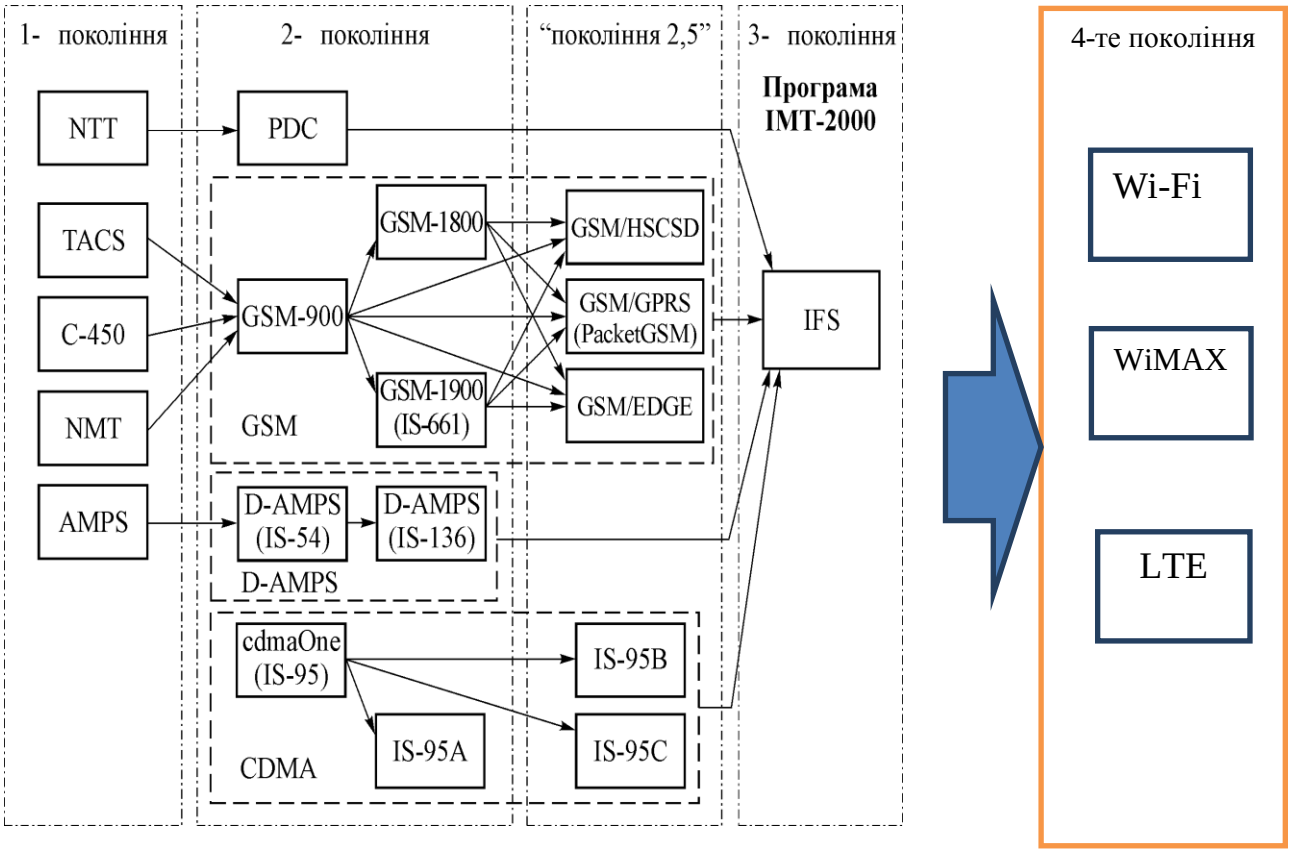


Рисунок 1.1– Покоління стільникових мереж зв'язку та етапи їх розвитку

До аналогових стільникових мереж зв'язку належать такі стандарти:

AMPS (Advanced Mobile Phone Service - удосконалена мобільна телефонна служба, діапазон 800 МГц) - широко використовується в США, Канаді, Центральній і Південній Америці, Австралії. Це найбільш поширений стандарт у світі. Станом на початок 1999 року СМЗ(Стільникові Мережі Зв'язку) стандарту AMPS використовувалися в 95 країнах світу (разом зі своєю цифровою модифікацією D-AMPS).[4,3] Стандарт має модифікацію NAMPS (Narrow AMPS);

TACS (Total Access Communications System - загальнодоступна система зв'язку, діапазон 900 МГц) - використовується в Англії, Італії, Іспанії, Австрії, Ірландії, Японії та інших країнах з модифікаціями ETACS (Enhanced TACS - вдосконалений TACS) (Англія), JTACS (Japanese TACS - японська TACS) (Японія), NTACS (Narrow TACS (узкополосная TACS). Другий по застосуванню стандарт серед аналогових систем. Початок комерційного

застосування 1985 рік. Модифікації стандарту відрізняються одна від однієї за діапазоном частот, який використовується, ширині смуги частот каналу та ін .;

NMT-450 і NMT-900 (Nordic Mobile Telephone system - Скандінавська система мобільного телефонного зв'язку, діапазони 450 і 900 Мгц) - використовується в Скандинавії і в багатьох інших країнах Західної та Східної Європи та ряді інших регіонів світу.[2] Третьою по застосуванню серед аналогових стандартів, знайшов широке поширення і в Україні. Початок комерційного використання - 1991 (NMT-450) і 1996 (NMT-900). Існує модифікація стандарту NMT-450 з удосконаленою системою аутентифікації NMT-450i (improved - покращений);

З-450 (діапазон 450 МГц) - використовується у Німеччині та Португалії;

RTMS (Radio Telephone Mobile System - мобільна радіотелефонна система, діапазон 450 МГц) - використовується в Італії; Radiocom-2000 (діапазон 170, 200, 400 МГц) - використовується в Франції;

NTT (Nippon Telephone and Telegraph System - японська система телефону і телеграфу, діапазон 800-900 МГц) - використовується в Японії.

З усіх перерахованих аналогових стандартів найбільше поширення отримали AMPS, TACS і NMT.

Характеристики стільникових мереж зв'язку основних аналогових стандартів представлені в таблиці 1.2.

У всіх аналогових стандартах використовується частотна (ЧМ) або фазова (ФМ) модуляція для передачі мови і частотна маніпуляція для передачі інформації управління.

У зв'язку з цим аналогові стандарти мають ряд суттєвих недоліків:

– можливість прослуховування розмов іншими абонентами;

– відсутність ефективних методів боротьби з завмираннями сигналів через вплив навколишнього ландшафту і будинків або внаслідок переміщення абонентів;

– несумісність різних стандартів між собою, неможливість взаємодії з цифровими мережами з інтеграцією служб ISDN (Integrated Service Digital Network) і мережами пакетної передачі даних PDN (Packet Data Network);

– низька канальна ємність, що є наслідком недостатньо раціонального використання виділеної смуги частот при частотному рознесенні каналів.

Таблиця – 1.2

Характеристики аналогових стандартів стільникового зв'язку

Характеристика і її розмірність	AMPS (NAMPS)	TACS (ETACS)	NMT-450 (NMT-450i)	NMT-900	Radiocom-2000	NTT
Діапазон робочих частот, МГц: для передачі мобільною станцією	825-845	935-950 (917-933)	453-457,5 (453-457,5)	935-960	424,8-427,9	925-940
для передачі базовою станцією	870-890	890-905 (872-888)	463-467,5 (872-888)	890-915	418,8-421,9	870-885
Радіус , км	2…20	2…20	15…40	2…20	5…20	5…10
Ширина полоси частот каналів, кГц	30 (10)	25	25 (20)	25/12,5	12,5	25
Дуплексне рознесення каналів, МГц	45	45	10	45	6	55
Число частотних каналів.	666 (2000)	600 (640)	180 (225)	1000/1999	256	до 1000
Потужність передавача базової станції, Вт	45	50	до 50	до 25	до 25	25
Потужність передавача рухомої станції, Вт	12; 1	-	15; 1,5; 0,15	6; 1; 0,1	-	-
Час перемикання каналу на кордоні , мс	250	290	1250	270	-	800

Перераховані недоліки зумовили появу цифрових стільникових мереж зв'язку. Перехід до цифрових систем також стимулювався широким втіленням цифрової техніки в область радіозв'язку. Характеристики стільникових мереж зв'язку основних цифрових стандартів представлені в таблиці 3[4].

Таблиця – 1.3

Характеристики цифрових стандартів стільникового зв'язку

Характеристика і її розмірність	GSM-800/ 1800/1900	D-AMPS (IS-136)	PDC	CDMA (IS-95)
Діапазон робочих частот, МГц: для передачі мобільною станцією для передачі базовою станцією	890-915/ 1710-1785/ 1850-1910 935-960/ 1805-1880/ 1930-1990	824-849; 1750-1810 869-894; 1830-1890	810-826; 1429-1453; 1477-1489 940-956; 1477-1501; 1501-1513	824-849 869-894
Радіус , км	GSM-800 (0,5…35); GSM-1800/1900 (0,5…6)	0,5…20	0,5…20	0,5…25
Дуплексне рознесення каналів, МГц	45/95/80	45	130; 48; 24	45
Характеристика і її розмірність	GSM-800/ 1800/1900	D-AMPS (IS-136)	PDC	CDMA (IS-95)
Ширина смуги частот радіоканалу, кГц	200	30	50 (25)	1288,8
Число частотних каналів (несучих), од.	124/374/239	832	320 (640); 480 (960); 240 (480)	20
Число каналів на одну несучу, од.	8 або 16	3 або 6	3 або 6	66
Швидкість перетворення мови, кбіт / с	13 або 6,5	8	11,2 або 5,6	13 або 8,55
Швидкість передачі інформації в радіоканалі, кбіт / с	270,833	48,6	42	1288,8
Швидкість передачі інформації у фізичному каналі, кбіт / с	9,6; 14,4	-	-	1,2; 2,4; 4,8; 9,6; 14,4

D-AMPS (Digital AMPS цифровий AMPS, діапазони 800 і 1800 МГц) - широко використовується в США, Канаді, Центральній і Південній Америці, Австралії, знайшов поширення і в Україні. Перший із застосування в світі стандарт цифрового стільникового зв'язку, являє собою аналого-цифрову, СМЗ діапазону 800 МГц. Початок практичного використання відноситься до 1992

році. Удосконалена версія даного стандарту IS-136 повністю цифрова СМЗ діапазону 800 і 1800 МГц, спільна з AMPS, почала застосовуватися з 1996 року.

GSM (Global System for Mobile communication глобальна система стільникового зв'язку, діапазони 900, 1800 і 1900 МГц) загальноєвропейський стандарт стільникового зв'язку, використовується більше, ніж в 130 країнах світу, в тому числі і в Україні, другий по застосуванню серед цифрових стандартів СМЗ. Практичне застосування стандарту GSM-900 почалося в 1991 році. Удосконалення даного стандарту призвело до освоєння нового частотного діапазону 1800 МГц. Спочатку дана версія називалася PCN (Personal Communication Network мережу персонального зв'язку), потім DCS (Digital Cellular System цифрова система стільникового зв'язку), через три роки після початку експлуатації (1993 рік) була перейменована в GSM-1800.

Так, спільнотою GSM були розпочаті і успішно реалізуються кроки в напрямку створення ССЗ перехідного "покоління 2,5" (2,5G), що характеризуються трьома основними доповненнями до базового стандарту:

– перше, що позначається абревіатурою HSCSD (High-Speed Circuit-Switched Data - високошвидкісна передача даних у мережах рухомого радіозв'язку з комутацією каналів), полягатиме в наданні одному і тому ж користувачеві кілька слотів в GSM-кадрі;

– друге - GPRS (General Packet Radio Service пакетна комутація в мережах рухомого радіозв'язку) передбачає організацію спеціального каналу пакетної передачі зі швидкостями до 115 кбіт / с (або вище, але без завадостійкого кодування) і Packetgsm (пакетний GSM), що пропонує пакетну передачу мови за допомогою технології Vogprs (мовної GPRS) і даних по СМЗ GSM-стандарту;

– третій - EDGE (Enhanced Data Rates for Global Evolution (покращена швидкість передачі даних для глобальної еволюції систем рухомого радіозв'язку) передбачає введення, поряд з Гаусовим модуляцією з мінімальним частотним зрушенням, додаткового модуляционного формату: восьмирівневою

ФМ, що потроює цих заходів дозволила підвищити швидкість передачі до 384 кбіт / с.

PDC (Personal Digital Cellular персональний цифровий стільниковий зв'язок, діапазони 800, 1400 і 1500 МГц) використовується в Японії і має можливість роботи в декількох діапазонах частот. Хоча стандарт PDC використовується тільки в Японії, його абонентська база складає 20% від загальносвітового числа абонентів.

CDMA (Code Division Multiple Access стандарт множинного доступу з кодовим поділом каналів, діапазони частот 800, 1900 і 2000 МГц) використовується в США, Південній Кореї, Гонконгу і останнім часом знаходить все більш широке застосування в країнах Європи і в світі в цілому . Існує в декількох версіях. Найбільш поширена з них cdmaone або діапазону 800 МГц, практичне застосування якої, почалося в 1995 році (Гонконг). У США СМЗ стандарту IS-95 використовують діапазон 1900 МГц. Стандарт IS-95 має декілька версій, які відрізняються одна від однієї, в основному, швидкостями передачі інформації в фізичному каналі:

IS-95A, швидкість передачі інформації - 9,6 кбіт / с (з кодуванням) і 14,4 кбіт / с (без кодування);

IS-95B, швидкість передачі інформації від 28,8 до 115,2 кбіт / с (без кодування);

IS-95C зі швидкістю передачі інформації до 144 кбіт / с (без кодування);

IS-95HDR (High Data Rate висока швидкість передачі даних) зі швидкістю передачі інформації до 1 Мбіт / с у прямому каналі (канал БС-МС) і в зворотному каналі (канал МС-БС) такий же, як і для IS-95C (до 144 кбіт / с).

При цьому важливим моментом, який потрібно відзначити окремо, є те, що при розробці вище перерахованих версій стандарту IS-95 необхідною умовою було забезпечення взаємної сумісності обладнання СМЗ на базі кожної наступної версії з обладнанням СМЗ попередніх версій.[6,7]

Інші версії стандарту CDMA, що запропоновані компаніями : B-CDMA (компанія Inter Digital), FH-CDMA (компанія Tadiran Communications),

cdma2000 (компанії Qualcomm, Lucent і Motorola). Окремо потрібно відзначити стандарти CDMA, що розробляються згідно концепції щодо створення міжнародної системи мобільного зв'язку третього покоління IMT-2000 (International Mobile Telecommunications) в рамках відповідних проектів і однойменних їм стандартів:

- європейського UTRA-FDD (Universal Terrestrial Radio Access - Frequency Division Duplex універсальний радіодоступ з дуплексной передачею на основі частотного поділу каналів) і японського W-CDMA (Wideband CDMA широкосмуговий CDMA), що будуть мати загальний стандарт радіопослуга IMT-DS (IMT- 2000 Direct Spread - радиоинтерфейс IMT-2000 з прямим розширенням спектру). Обидва проекти засновані на використанні технології W-CDMA FDD (W-CDMA Frequency Division Duplex - W-CDMA з частотним дуплексним рознесенням каналів) з прямим розширенням спектру, орієнтованої на роботу в парних смугах частот. Системи СМЗ з радіоінтерфейсом IMT-DS працюють в діапазоні 2000 МГц; європейського UTRA-ADD (Universal Terrestrial Radio Access - Time Division Duplex -універсальний радіодоступ з дуплексной передачею на основі тимчасового розділення каналів) і китайського TD-SCDMA (Time Division - Space CDMA- CDMA з тимчасовим і просторовим розділенням каналів), що будуть мати загальний стандарт радіо-інтерфейсу IMT-TC (IMT-2000 Time Code- радіо-інтерфейс IMT-2000 з тимчасовим прямим розширенням спектру). Обидва проекти засновані на використанні технології W-CDMA TDD (W-CDMA Time Division Duplex - W-CDMA з тимчасовим дуплексним рознесенням каналів) з прямим розширенням спектра.[11,13] Системи СМЗ з радіо-інтерфейсом IMT-TS працюють в діапазоні 2000 МГц;

- cdma2000, представленого США і максимально наближеного до cdmaone (IS-95), зі стандартом радіо-інтерфейсу IMT-MC (IMT-200 Multi-carrier - радіо-інтерфейс IMT-2000 з багатьма несучими частотами). Проект заснований на використанні технології W-CDMA FDD з одночасною передачею сигналів на декількох несучих частотах, орієнтованої на роботу в непарних

смугах частот. Системи СМЗ з радіо-інтерфейсом IMT-MC працюють в діапазоні 800 і 1900 МГц.

Універсальна система мобільного зв'язку (UMTS) є третім поколінням мобільного стільникового системи для мереж, заснованих на GSM стандарту. Розробка та підтримка по 3GPP (проект 3-го покоління Партнерство), UMTS є складовою частиною Міжнародного союзу електрозв'язку стандартного набору IMT-2000 і порівнює зі стандартним набором CDMA2000 для мереж на основі конкуруючих CDMAOne технології. UMTS використовує широкосмуговий поділом множинного доступу з кодовим (W-CDMA) технологія радіо доступу, щоб запропонувати більш спектральную ефективність і пропускну здатність для операторів мобільного зв'язку. UMTS повністю визначає мережеву систему, яка включає в себе мережу радіодоступу (UMTS Terrestrial Radio Access Network , або UTRAN), базової мережі (Mobile Application Part , або карта) і аутентифікацію користувачів за допомогою SIM-карти (модуль ідентифікації абонента) карти. Технології, описаної в UMTS іноді також називають свободі мобільних мультимедійних Access (FOMA) або 3GSM. На відміну від EDGE (IMT однієї несучої, на основі GSM) і CDMA2000 (IMT з безліччю несучих), UMTS вимагає нових базових станцій і нових розподілів частот.[19,20]

Принципова відмінність технології 3-го покоління від попередніх - можливість забезпечити весь спектр сучасних послуг (передачу мови, роботу в режимі комутації каналів і комутації пакетів взаємодія з додатками internet, симетричну і асиметричну передачу інформації з високою якістю зв'язку) і в той же час гарантувати сумісність з існуючими системами.

Сьогодні на зміну 3G прийшла технологія 4G яка швидко розвивається і вдосконалюється. До 4G як правило, відносять технології, які дозволяють передавати дані в стільникових мережах з швидкістю вище 100 Мбіт / сек. У широкому розумінні 4G - це ще і технології бездротової передачі інтернет-даних Wi-Fi (швидкісні варіанти цього стандарту) і WiMAX (в теорії швидкість передачі інформації може перевищувати 1 Гбіт / сек). У найбільш поширеному

у світі стандарті стільникового зв'язку GSM / EDGE (2G) межа швидкості передачі даних становить, всього 240 кбіт / сек .

WiMax - це технологія, яку оголосили майбутнім бездротових мережевих технологій дальньої дії. Правда, пізніше такі асоціації стали вважатися перебільшеними завдяки розвитку технології під назвою Long Term Evolution (LTE). WiMax - це стандарт асоціації Institute of Electrical and Electronics Engineers (IEEE) під номером 802.16. У 2001 IEEE випустив стандарт 802.16 для широкосмугового бездротового доступу. Незабаром після цього був відкритий форум WiMax для просування стандарту, і тоді ж народився термін WiMax.

Головна відмінність мереж четвертого покоління 4G від попереднього, третього, полягає в тому, що ця технологія повністю заснована на протоколах пакетної передачі даних, у той час як 3G поєднує в собі передачу, як голосового трафіку в режимі комутації каналів, так і пакетів даних. Міжнародний союз телекомунікацій визначає технологію 4G як технологію бездротової комунікації, яка дозволяє досягти швидкості передачі даних до 1 Гбіт / с в умовах руху джерела або приймача і до 100 Мбіт / с в умовах обміну даними між двома мобільними пристроями.[25]

Пересилання даних в 4G здійснюється по протоколу IPv6 (IP версії 6). Це помітно полегшує роботу мереж, особливо якщо вони різних типів. Для забезпечення необхідної швидкості передачі використовуються частоти від 2 до 40 і 60 ГГц.

Розробники приймально-передавального обладнання для 4G застосували випробуваний в цифровому мовленні прийом - технологію мультиплексування з ортогональним поділом частот (OFDM). Така методика маніпулювання сигналом дозволяє значно «ущільнити» дані без взаємних перешкод і спотворень. При цьому відбувається розбиття по частотах з дотриманням ортогональності: максимум кожної несучої хвилі припадає на той момент, коли сусідні мають нульове значення. Цим виключається їх взаємодія, а також більш ефективно використовується частотний спектр - не потрібні захисні «протиінтерференційні» смуги. Для передачі сигналу застосовується

модуляція зі зрушенням фази (PSK та її різновиди), при якій пересилається більше інформації за відрізок часу, або квадратно амплітудна (QAM), більш сучасна і дозволяє вичавити максимум з пропускної здатності каналу.

Конкретний тип вибирається залежно від необхідної швидкості та умов прийому. Сигнал розбивається на певну кількість паралельних потоків при передачі і збирається при прийомі. Для впевненого прийому і передачі на надвисоких частотах планують застосовувати так звані адаптивні антени, які зможуть підлаштовуватися під конкретну базову станцію[29].

Але в умовах міста таким антен у визначенні правильного напрямку можуть перешкодити завмирання сигналу - його спотворення, що виникають у процесі поширення. Тут виручає ще одна особливість OFDM - стійкість до завмирань (для різних типів модуляції є свій запас на завмирання). Можлива і робота в умовах відсутності прямої видимості, що так заважає телефонами стандарту GSM.

Таблиця – 1.4

Порівняльна характеристика 3G з 4G

Параметри	3G	4G
Швидкості	384 Kbps до 2 Mbps	100 Мбіт до 1 Гбіт
Частотний діапазон	Залежно від країни або континенту (1800-2400 МГц)	Більш високі діапазони частот (2-8 ГГц)
Ширина смуги	5-20 МГц	100 МГц (або більше)
Схема перемикання	Схеми і пакети	Пакет
Технології доступу	W-CDMA, 1xRTT, Край	OFDM і MC-CDMA
IP	Кількість протоколів повітряної лінії	Всі IP

Розглянувши основні характеристики систем мобільного зв’язку стає зрозумілим , як саме здійснюється передача зв’язку і даних в кожному поклінні і його технологіях.

РОЗДІЛ 2
ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ

2.1 Методи захисту та алгоритми мобільного зв’язку.

Починаючи з другого покоління мобільного зв’язку захист інформації набув нового розвитку, до системи другого покоління D-AMPS ввійшли нові алгоритми: аутентифікації – CAVE (Cellular Authentication, Voice Privacy and Encryption) і шифрування – CMEA (Cellular Message Encryption Algorithm). На відміну від AMPS у цьому стандарті застосовується інтерлівінг (англ. Interleaving) для подолання швидких завмирань.

Для захисту від несанкціонованого доступу в системах AMPS і D-AMPS використовується система аутентифікації A-KEY. Власне AKEY представляє собою 8-байтове число-ключ, яке зберігається в стільниковому телефоні абонента і є унікальним для кожного абонента. AKEY вводиться при продажі телефону клієнта і зберігається в базі. AKEY не змінюється і залишається постійним при нормальній роботі телефону. Оскільки даний ключ не передається в ефір, його не можна перехопити і використовувати, як це робилося з серійними номерами. На основі AKEY (постійний ключ) за допомогою хеш-функції CAVE (Cellular Authentication and Voice Encryption), що використовує в якості вхідних параметрів AKEY, ESN (Electronic Serial Number), MIN (Mobile Identification Number) телефону, а також випадкове число, прислане по ефіру від базової станції, генерується часовим ключем, так званий SSD_A (теж 8 байт). Цей ключ надалі і використовується при аутентифікації для генерації відповідного значення. Постійна AKEY не використовується при аутентифікації і служить тільки для розрахунку тимчасового ключа. При встановленні з'єднання система передає стільниковому телефону випадкове число, яке шифрується по алгоритму CAVE з використанням тимчасового ключа SSD_A і інших унікальних параметрів телефону (ESN, MIN) як ключ. Відповідь надсилається через базову станцію

комп'ютера в HLR або AC - Authentication Center, який, в свою чергу, незалежно від телефону генерує відповідь число (всі параметри телефону, у тому числі і AKEY, і поточний SSD_A зберігаються в базі даних системи аутентифікації), і порівнюють його з отриманим. У разі незбігу числа прийнятого від телефону з незалежно обрахованим числом, аутентифікація вважається невдалою і телефону відмовляється в з'єднанні[19]. Періодично (приблизно раз на тиждень) станція посилає стільниковому телефону повідомлення про генерацію нового тимчасового ключа, SSD_A, після отримання цього повідомлення (SSD_UPDATE) телефон розраховує новий часової ключ SSD_A, використовуючи вже відомий постійний AKEY, ESN, MIN, і випадкове число зі станції. Таким чином, сам ключ аутентифікації (SSD_A) являється тимчасовим і періодично змінюється, при цьому стає безглуздим "клонування" трубок (а також знаходження SSD_A методом послідовного перебору), оскільки після першої ж зміни ключа працювати далі буде тільки один телефон з новим ключем.

Ще одна система другого покоління GSM має безліч особливостей у плані безпеки, які розроблені, щоб надати абонентові й мережному оператору більший рівень захисту від шахрайської діяльності. Механізми аутентифікації гарантують, що тільки добросовісним абонентам, які мають добросовісне обладнанням, тобто не вкрадене або нестандартне, буде надано доступ до мережі. Як тільки зв'язок було встановлено, інформація в лінії зв'язку передається в зашифрованій формі, щоб уникнути підслуховування. Конфіденційність кожного абонента захищена, гарантована тим, що його особу та місце розташування захищено. Це досягнуто шляхом призначення для кожного користувача тимчасового ідентифікатора рухомого абонента (Temporary Mobile Subscriber Identity - TMSI), який змінюється від дзвінка до дзвінка. Таким чином немає необхідності передавати міжнародний ідентифікатор мобільного абонента (International Mobile Subscriber Identity - IMSI) по радіо-інтерфейсу, що ускладнює завдання ідентифікації та визначення місцезнаходження користувача для того хто підслуховує.

Процедура встановлення автентичності або аутентифікації (authentication) виконується під керуванням і з ініціативи VLR (Visitor Location Register - реєстр переміщення). Для її проведення використовується сценарій запит-відповідь, в якому VLR відправляє в MS спеціальне випадкове число RAND, яке є одним із вхідних параметрів алгоритму A3, використовуваного в SIM-картці для обчислення значення відгуку SRES. Іншим вхідним параметром алгоритму A3 є секретний ключ Ki, що міститься в SIM-картці. Ключ Ki не доступний для зчитування з SIM і це є одним з основних аспектів безпеки GSM[10].

Основу системи безпеки GSM складають три секретних алгоритми (аж до кінця 2003 р. офіційно так і не розкриті, повідомляються лише тим, кому це потрібно за необхідності - постачальникам обладнання, операторам зв'язку і т.д.):

– A3 - алгоритм аутентифікації, що захищає телефон від клонування;

– A8 - алгоритм генерації крипто ключа, по суті справи, односпрямована функція, яка бере фрагмент виходу від A3 і перетворює його в сеансовий ключ для A5;

– A5 - власне алгоритм шифрування оцифрованого мовлення для забезпечення конфіденційності переговорів.

У GSM використовуються два основні різновиди алгоритму: A5 / 1 - "сильна" версія шифру для обраних країн і A5 / 2 - ослаблена для всіх інших. (У 2000-і роки для наступного покоління мобільного зв'язку, G3, створений абсолютно новий крипто алгоритм, що отримав назву A5 / 3. Ще є варіант A5 / 0 - це коли режим шифрування ніби як включений, але насправді його немає, оскільки замість бітів ключа використовуються одні нулі.).

VLR, в якому реєструється абонент, відправляє запит до AuC домашньої мережі абонента, у відповідь на який AuC надсилає набір триплетів, кожен з яких містить RAND, SRES і ключ шифрування Kc. RAND є випадковим числом, SRES обчислюється в AuC алгоритмом A3 на основі таємного ключа Ki і RAND, а Kc є ключем шифрування радіо інтерфейсу і обчислюється алгоритмом A8 на основі Ki і RAND. Ці триплети надалі будуть використані в

VLR для встановлення автентичності та шифрування[4]. Таким чином, всі обчислення з використанням ключа Ki відбуваються всередині AuC, на стороні мережі і всередині SIM, на стороні абонента, що виключає витік Ki і перехоплення зловмисником. У сучасному обладнанні зв'язку, ключі Ki завантажуються в AuC в зашифрованому вигляді і це виключає доступ до ключів навіть з боку технічного персоналу оператора. Процедура встановлення автентичності може виконуватися при вихідних, вхідних дзвінків, при реєстрації в мережі, пакетної передавання даних, надсилання або отримання SMS, а так само при оновленні місця розташування (location update). Кожен оператор зв'язку самостійно визначає, в яких випадках VLR буде виконувати аутентифікацію.

Процедура встановлення автентичності починається після того, як між MS й MSC організований прозорий канал для обміну службовою інформацією. VLR вибирає перший триплет і відправляє в мобільну станцію його RAND разом з номером триплетів, який надалі буде позначатися як CKSN – Ciphering Key Sequence Number, він же - номер ключа шифрування Kc. На боці MS, за алгоритмом A3 обчислюється SRES, який повертається в VLR, де порівнюється зі значенням SRES зі складу триплетів, отриманого з AUC. Ідентичність двох SRES є ознакою дійсності абонента. Триплет в VLR позначається як використаний і в наступний раз буде використаний інший триплет. Після того, як всі триплети будуть витрачені, VLR запитує у AuC нову порцію кодонів. Секретний алгоритм A3 надає можливість відносно простій генерації SRES з RAND і Ki, однак ускладнює визначення Ki з SRES і RAND, або пари SRES і RAND, чим забезпечується висока стійкість до компрометації.

Як тільки справжність абонента була перевірена, таким чином захищаючи і абонента і мережевого оператора від впливу шахрайського доступу, користувач повинен бути захищений від підслуховування. Це досягається шляхом шифрування даних, переданих по радіо-інтерфейсу, з використанням другого ключа Kc і секретного алгоритму A5. Kc генерується в ході перевірки автентичності, використовуючи Ki, RAND і секретний алгоритм A8, який також

зберігається в SIM карті. Подібно до алгоритму A3, A8 не унікальний, і він може також бути обраний оператором. Ключі Kc для кожного користувача обчислюються в AuC домашньої мережі і передається в VLR в складі набору триплетів, де кожному триплети і, відповідно - ключу Kc, присвоюється номер ключа - CKSN. У деяких реалізаціях A3 і алгоритми A8 об'єднані в єдиний алгоритм A38, який використовує RAND і Ki, щоб згенерувати Kc і SRES. На відміну від A3 і A8, які, можливо, різні для кожного індивідуального оператора, A5 буде вибирається зі списку з 7 можливих варіантів.

Перед шифруванням відбувається фаза переговорів у ході якої визначається, яка версія A5 буде використана. Якщо мережа і мобільна станція не мають загальних версій A5, зв'язок має продовжитися у відкритому режимі або з'єднання повинно бути розірване. Алгоритм A5 використовує 64-бітний ключ Kc, і 22-бітний номер фрейму TDMA, для обчислення двох 114-бітних слова шифрування, BLOCK1 і BLOCK2, для використання при передавання та прийомі відповідно. Слова шифрування - EXORed з 114 бітами даних у кожній посилці. Оскільки зашифровані дані обчислені, використовуючи номер фрейму TDMA, то слова змінюються від посилки до посилки і не виконують впродовж гіперфрейма (приблизно 3,5 години)[7].

Перед тим, як почати шифрування, мобільна станція (MS) відправляє в VLR номер ключа шифрування CKSN, який зберігається в її пам'яті з моменту останньої процедури аутентифікації. CKSN не містить секретних даних, а служить лише для того, щоб MS могла повідомити мережі, який ключ Kc вона "пам'ятає". Після цього VLR відправляє в MS команду на включення шифрування і передає в базову станцію (BTS) ключ Kc, з того триплету, який відповідає номеру CKSN отриманому від MS. Таким чином між MS і VLR досягається домовленість про вибір ключа шифрування без передавання самого ключа по радіо інтерфейсу.

Деякі передавання на лінії радіозв'язку не можуть бути захищені шифруванням. Наприклад, після початкового призначення, мобільна станція повинна передати свій ідентифікатор мережі перш, ніж шифрування може бути

активізовано. Це очевидно дозволило б підслуховуючи визначати місце розташування абонента, перехоплюючи це повідомлення. Ця проблема вирішена в GSM введенням тимчасового ідентифікатора рухомого абонента (TMSI), який є «псевдонімом», призначеним на кожній мобільної станції з боку VLR. TMSI передається мобільної станції протягом попередньої зашифрованою сесії зв'язку, і він використовується мобільною станцією і мережею при будь-якому подальшому пейджингу та процедурі доступу. TMSI дійсний тільки в межах області, яку обслуговує певний VLR. Безпека в системі GSM вивела захист в мобільному зв’язку на новий рівень.

Процес кодування каналу в GPRS, а також EGPRS складається з двох етапів: по-перше, циклічний код використовується для додавання бітів парності, які також згадуються як блок послідовності перевірки. В GPRS, кодування схеми CS-1 CS-4 вказують кількість бітів парності, що генеруються циклічним кодом і частотою виключення загортального коду. У EGPRS / EDGE, модуляції та кодування MCS-1 до MCS-9 займають місце в схемах кодування в GPRS, і додатково вказують, які схеми модуляції використовується,GMSK або 8PSK.MCS-1 по MCS-4 використовувють GMSK і мають таку ж продуктивність (але не рівну) GPRS.

У стандарті EDGE адресація пакетів розширена до 2048 (звичайно, буває задіяно більше 1 таймслота), а розмір ковзаючого вікна - до 1024. Така техніка, в кінцевому рахунку, також призводить до збільшення пропускної здатності каналу.

Перед початком комунікаційної сесії MS інформує мережу про свою присутність, при цьому SGSN насамперед ідентифікує користувача (по IMEI і / або IMSI / TMSI). В основному, ця процедура однакова для всіх GSM сервісів і служить для визначення ключа K, який буде використовуватися в подальшому для виконання двосторонньої аутентифікації вибору сесійного ключа у функціях алгоритмів A3 і A8. Оператор асоціює K з конкретним IMSI при підключенні користувача,а при надходженні запиту від SGSN на основі цього ключа НЕ генерує масив векторів AV [1 .. n] для аутентифікації користувача.

Розглянемо механізм обміну ключами між USIM і SGSN. Синхронізація SGSN і USIM забезпечується за допомогою лічильника SQNHE (на MS і HE) і числа SQNMS. SQNHE - це індивідуальний для кожного користувача лічильник, SQNMS - максимальне число в послідовності SQNHE, прийняте USIM.

Як вже згадувалося раніше, розробники описуваного стандарту намагалися досягти максимальної сумісності з існуючою архітектурою GSM мереж, тому для передавання ключа використовується вже відомий протокол "запит / відповідь" (challenge / response).

Потрібно зазначити, що нижчеописана процедура відбувається в припущенні довіри користувача HE та безпеки передавання даних між HE і SGSN.

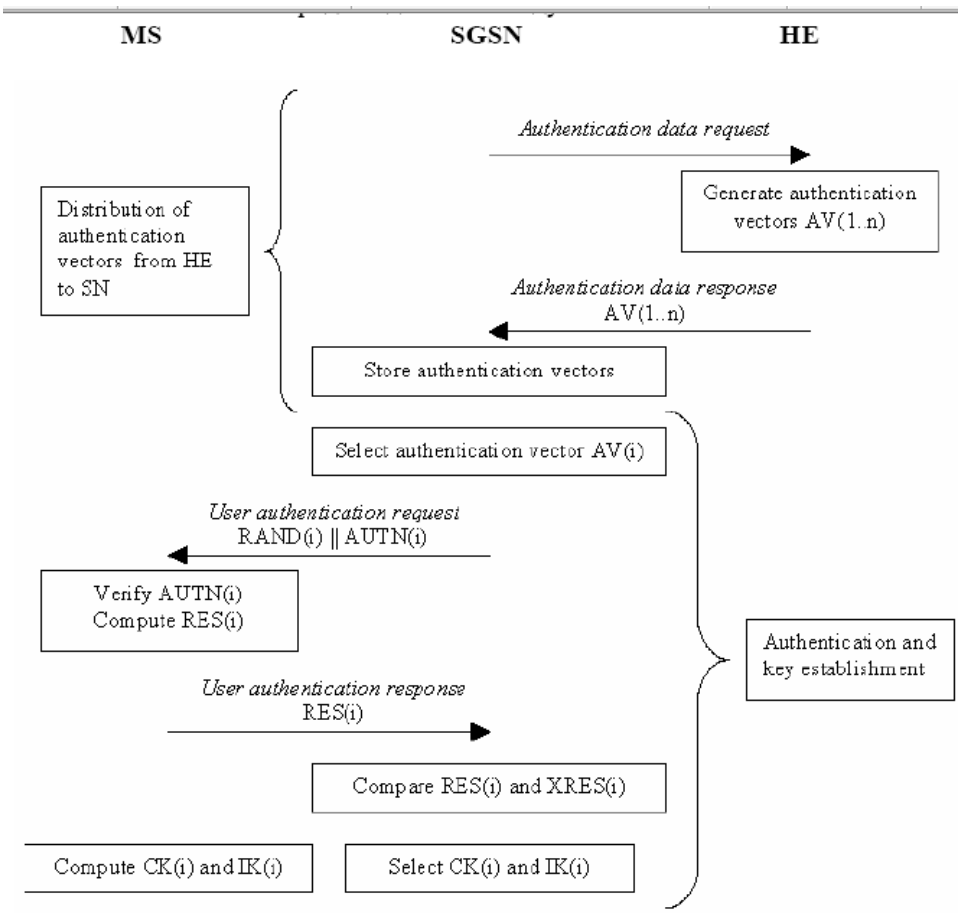
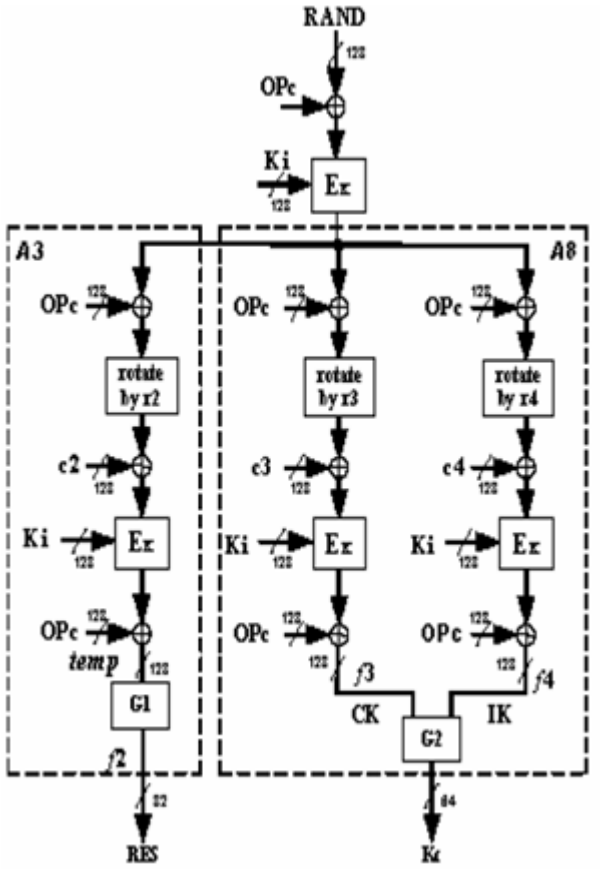


Рисунок 2.1 – Передавання даних між HE і SGSN

У загальних рисах схема виглядає таким чином: при отриманні запиту від SGSN, HE посилає у відповідь послідовно масив n аутентифікаційних векторів (кожен з яких є аналогом "триплета" в GSM). Кожен вектор складається з наступних частин: випадкового числа RAND, очікуваної відповіді XRES, ключа CK, ключа цілісності (integrity key) IK і аутентифікаційної мітки AUTN. Кожен такий вектор годиться для однієї аутентифікації і вибору ключа SGSN і USIM. Коли SGSN починає процедуру визначення ключа, вибирається наступний по порядку аутентифікаційний вектор і користувачеві посилаються параметри RAND і AUTN (вектори організовані за принципом FIFO). Далі, USIM перевіряє AUTN і, в разі прийняття, генерує відповідь RES. При цьому USIM обчислює CK і IK. SGSN порівнює прийнятий RES з XRES. При збігу цих параметрів процедури аутентифікації і обміну ключами вважаються успішними. Обчислені таким чином CK і IK передаються шифрувальним модулям.

Щоб з генеровані описаним способом ключі не використовувалися невизначено довго, в стандарті існують механізми їх заміни після передавання певного обсягу даних.

Для аутентифікації, вибору ключа та шифрування даних використовуються алгоритми A3, A8 (засновані на блочному шифрі Рейндала (Rijndael)) і GEA3 (модифікація A5 / 3), розроблений Mitsubishi (кодове ім'я MISTY), заснований на блочному шифрі Касумі (Kasumi), відповідно .



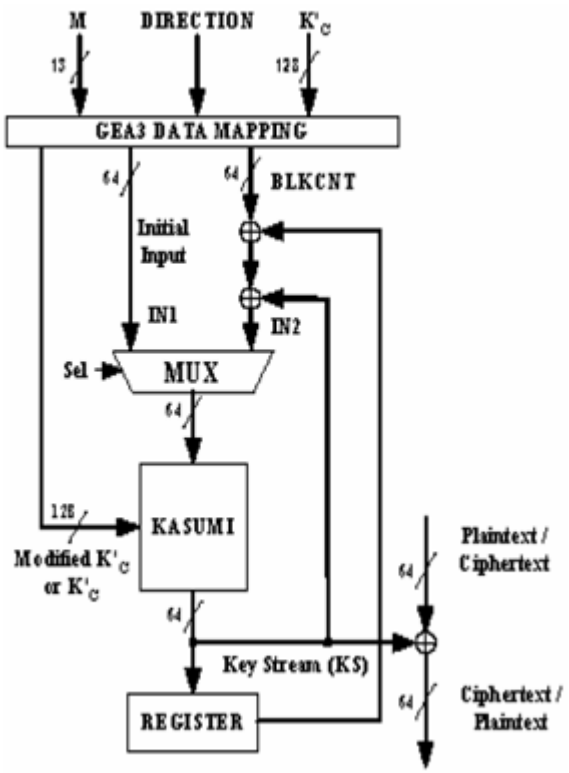


Рисунок 2.2 – Архітектура A3 і A8 Рисунок 2.3 – Блок-схема алгоритму GEA3

На нижче наведених малюнках демонструється робота "клієнтської" і "серверної" частини процесу аутентифікації.

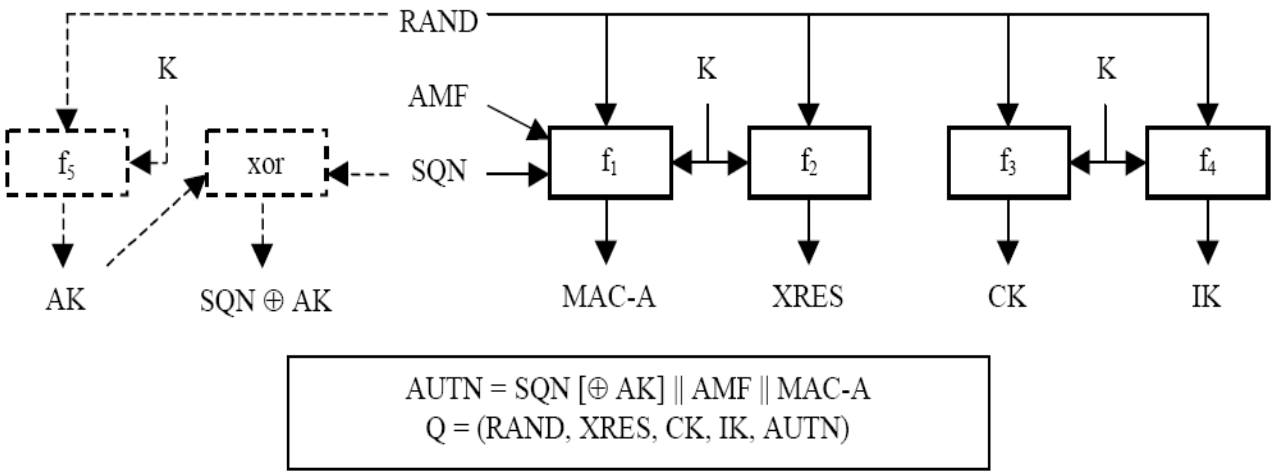


Рисунок 2.4 – «Клієнтська» і «серверна» частина аутентифікації

Генерація аутентифікаційних векторів: На вимогу SGSN HE визначає потрібну кількість векторів і витягує їх з бази даних HLR або ж обчислює нову послідовність (по ключу К). Далі масив векторів відсилається SGSN. У процесі роботи HE контролює індивідуальний лічильник SQNHE кожного користувача.

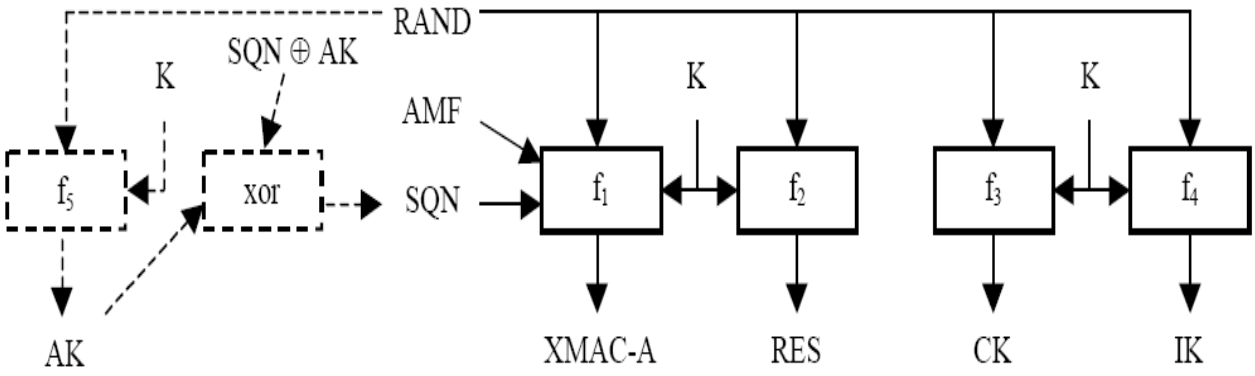


Рис. 2.5 – Генерація аутентифікації векторів

Для визначення ключа, USIM (User Services Identity Module) відновлює ключ АК і послідовність SQN. Далі, обчислений XMAC порівнюється з прийнятим MAC з AUTN. При розбіжності MS посилає SGSN відмову від аутентифікації. SGSN в свою чергу генерує звіт про помилку для HLR. У той же час SGSN може спробувати повторити процедуру. У цьому випадку подальшу поведінку системи відноситься до процесу ресинхронізації.

Такод одним з важливих знач. є захист цілісності даних (data integrity). Захист цілісності реалізований на рівні RRC (Radio Resource Control - наступний за RLC рівень). Для цього використовується ключ IK.

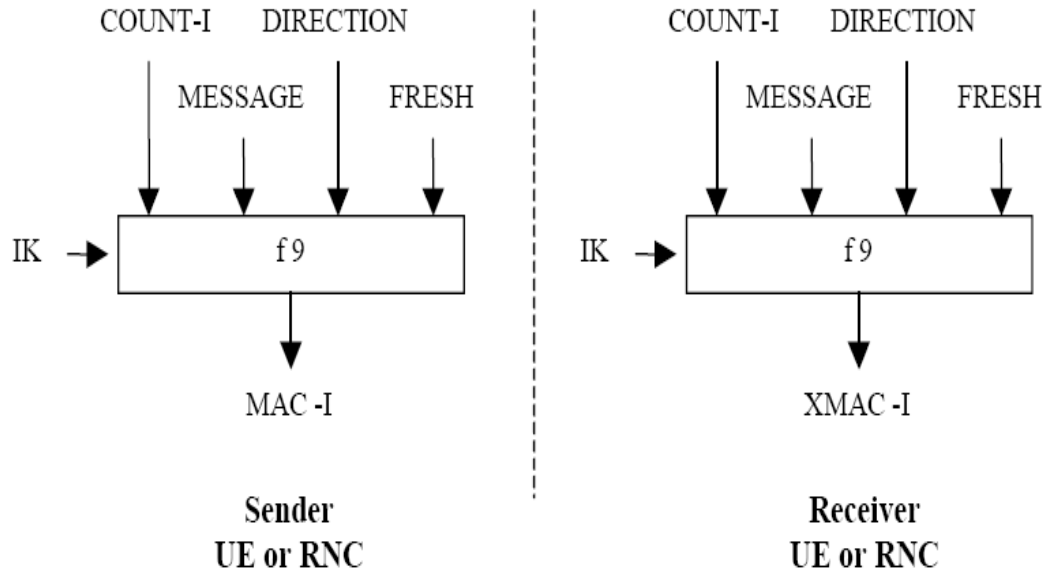


Рисунок 2.6 – Алгоритм захисту цілісності даних

Вхідними параметрами алгоритму є: ключ цілісності IK (integrity key), послідовність чисел COUNT-I, випадкове число FRESH, згенероване на стороні мережі, напрямок DIRECTION і повідомлення MESSAGE. Грунтуючись на цих даних, користувач обчислює аутентифікаційний код повідомлення (message authentication code) цілісності даних MAC-I. Потім MAC-I застосовується до надсилається повідомлення. Одержувач обчислює XMAC-I отримане повідомлення аналогічним чином і перевіряє цілісність даних шляхом порівняння XMAC-I с MAC-I.

При відправці повідомлення HFN (Hiperframe Number) інкрементирується. При цьому користувач зберігає максимальне значення HFN від попередньої комунікаційної сесії і при такій установці зв'язку повідомляє обслуговуючої мережі початкове значення HFN. Цей принцип не дозволяє використовувати однакове значення лічильника з одним і тим же ключем.

FRESH – випадкове число, що генерується BSC. Цей параметр виключає використання користувачем "чужих" MAC-I в тому випадку, якщо одночасно встановилися з'єднання з однаковими IK. MESSAGE - передане

повідомлення,DIRECTION - біт, що ініціює напрям передавання повідомлення,розмір MAC-I становить 32 біта.

Тепер детальніше про шифрування даних у EDGE. Зауважу, що при розробці методу шифрування переслідувалися наступні цілі:

– Неявна синхронізація процесу шифрування, що включає випадки передавання управління (Implicit synchronization of ciphering including handover cases).

– Однаковий підхід до сервісів реального часу

– "Подальше збільшення надмірності"

– Використання існуючих принципів і схем

– Мультиплікування декількох користувачів в 1 таймслоті

Основний принцип описується наступною схемою:

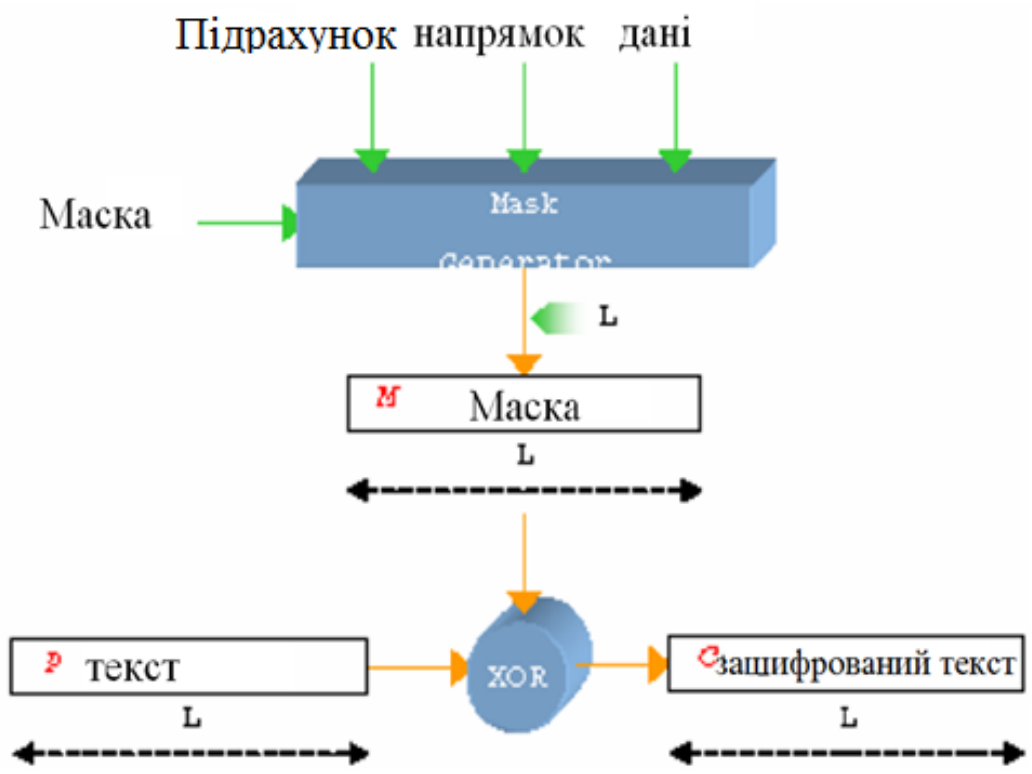


Рисунок. 2.7 – Схема шифрування даних

Шифровані дані виходять за формулою:

$$C = M \oplus P$$

Найбільш важливим параметром для генерації маски є ключ. Решта використовується для різних процесів шифрування (створення масок) блоків в одному або декількох потоках даних, в основному для виключення ситуації, коли за допомогою однакових масок шифруються різні блоки даних. Очевидно, застосування таких масок до блоків, які будуть в подальшому пов'язані, веде до істотної втрати секретності:

$$\begin{array}{ll} & P_1 \oplus M = C_1 \\ \oplus & P_2 \oplus M = C_2 \\ \hline & P_1 \oplus P_2 = C_1 \oplus C_2 \end{array}$$

L (Length) - довжина щифруючого повідомлення (16 біт) в бітах, може приймати значення від 24 до 5000. Data - ідентифікатор каналу передавання даних (Bearer).

Інші параметри аналогічні описаним при розгляді цілісності.

Процес шифрування проходить на одному з рівнів: MAC (відкритий (transparent) режим) або RLC (закритий (non-transparent) режим). Відкритий режим використовується зазвичай для передавання голосу, а закритий - для передавання даних.

Кілька слів про безпеку мереж GSM 2.5G (до яких відноситься EDGE). Для сумісності з існуючим стандартом алгоритми аутентифікації (A3) і вибору ключа (A8) залишилися без змін.

Що стосується захищеності переданих даних (зокрема, алгоритму GEA3), явним чином порівняти самі алгоритми A5 / 1, A5 / 2, що використовуються в мережах другого покоління (GSM 2G) з GEA3 (A5 / 3) не можливо, оскільки офіційно специфікації алгоритмів A5 / 1, A5 / 2 в силу малозрозумілих причин

досі закриті. Але незаперечним фактом є їх злом. Ось два основних типи атак на GSM 2G:

1. Розшифрування переданих повідомлень без знання ключа (атака на сам алгоритм).

Найслабший алгоритм зламується на звичайному комп'ютері за час, менший 1 секунди (однак, підготовка вимагає декількох годин обчислень). Наприклад, слабким місцем A5 / 2 було те, що шифрування вироблялося після внесення надмірності (для виправлення помилок при прийомі) в дані. Як виявилося, таке штучне "збільшення інформації" сильно допомагає при дешифрування.

2. Посередник між телефоном і базовою станцією (атака на процедуру аутентифікації).

Так як в GSM 2G відбувається одностороння аутентифікація: базова станція авторизує телефон, але не навпаки, зловмисник може виступати в якості посередника між користувачем і базовою станцією. Далі, дії наступні: починаємо комунікаційну сесію з користувачем від імені базової станції, повідомляємо йому про використання алгоритму A5 / 2 (тому його найпростіше зламати) і визначити секретний ключ K, про який мова йшла вище. Тепер хакер здатний практично повною мірою дешифрувати складніші для аналізу A5 / 1,3 під час обміну даними між користувачем і справжньої базової станцією.

Як було показано вище, в системах 2.5G автентифіковані як користувач (порівняння RES с XRES), так і базова станція (MAC-A з AUTN? = XMAC-A, обчислений мобільним телефоном). До того ж, A5 / 3, начебто, позбавлений знайдених недоліків, і, по завіреннях розробників, на даний момент забезпечує захищеність близьку до 75%.

2.2. Засоби захисту в сучасних системах мобільного звязку.

Захисту в третьому поколінні мобільного зв’язкуотримав нові протоколи, що забезпечують безпеку передавання інформації в CDMA-IS-41 мережах, і є одними з кращих в індустрії. Крім того сам CDMA стандарт за своєю побудовою робить перехоплення сигналу і його розшифрування дуже складним і дорогим завданням доступним, фактично, тільки державним спецслужбам. Криптографічні протоколи стандарту CDMA грунтуються на 64-бітному аутентифікаційному ключі (A-key) і серійному номері мобільного телефону - Electronic Serial Number (ESN). Для аутентифікації абонента при реєстрації мобільного телефону в мережі, а також подальшої генерації допоміжних підключень для забезпечення конфіденційності передавання голосових даних і кодованих повідомлень використовується випадкове двійкове число RANDSSD, що генерується аутентифікаційним центром реєстру власних абонентів (далі HLR / AC - Home Location Register / Authentification Center). A-key запрограмований в мобільному телефоні і зберігається в аутентифікаційному центрі мережі. CDMA використовує стандартизований алгоритм шифрування CAVE (Cellular Authentification and Voice Encryption) для генерації 128 бітного підключа SSD (Shared Secret Data). A-key, ESN і випадкове число що генерується мережею RANDSSD подаються на вхід CAVE генеруючого SSD. SSD складається з двох частин: SSD_A, яку використовують для створення аутентифікаційного цифрового підпису, і SSD_B, використовуваної при генерації ключів для шифрування голосових даних і службових повідомлень. SSD може бути переданий гостьовій мережі при роумінгу абонента для забезпечення локальної аутентифікації. Новий SSD може бути з генерований при поверненні абонента в домашню мережу або зміні гостьовою мережею у роумінгу[17,19].

Для аутентифікації абонента в CDMA мережі використовується допоміжний ключ SSD_A генерований CAVE алгоритмом з A-key, ESN і RANDSSD. Мережа генерує і розсилає відкрито по ефіру випадкове число

RAND , мобільні пристрої, що реєструються в мережі, використовують його як вхідні дані для CAVE алгоритму, що генерує 18-бітний аутентифікаційний цифровий підпис (AUTH_SIGNATURE), і посилає його на базову станцію. Цей цифровий підпис звіряється в центрі комутації (MSC - Mobile services Switching Center) з підписом генерується самим MSC для перевірки легітимності абонента. Число RAND - може бути як одним і тим же для всіх користувачів, так і генеруватися щоразу нове (використання конкретного методу визначається оператором). Перший випадок забезпечує дуже швидку аутентифікацію. І мобільний телефон і мережа ведуть 6-бітові лічильники викликів, що забезпечує можливість детектування працюючих двійників: для цього достатньо лише контролювати відповідність значень лічильників на телефоні та на MSC. Секретний ключ A-key є перепрограмуваний, в разі його зміни інформація на мобільному телефоні і в HLR / AC повинна бути синхронізована. A-key може бути перепрошитий кількома способами: на заводі, дилером у точках продажу, абонентом через інтерфейс телефону, а також за допомогою OTASP (over the air service provisionig). OTASP передавання використовує 512 бітний алгоритм узгодження ключів Diffie-Hellman'a, що гарантує достатню безпеку. OTASP забезпечує легкий спосіб зміни A-key мобільного телефону на випадок появи в мережі двійника мобільного телефону. Зміна A-key автоматично спричинить за собою відключення послуг двійнику мобільного телефону і повторне включення послуг легітимному абоненту. Таким чином, як можна було помітити, секретність A-key є найважливішою компонентою безпеки CDMA системи.

Мобільний телефон використовує допоміжні з'єднання SSD_B і CAVE алгоритм для генерації Private Long Code Mask (успадковану від TDMA мереж), 64-бітного підключа CMEA (Cellular Message Encryption Algorithm) key і 32-бітного DATA-key. Private Long Code Mask використовується як мобільним телефоном, так і мережею для зміни характеристик Long Code Mask. Цей модифікований Long Code використовується для шифрування голосових даних, що підвищує секретність їх передавання. Private Long Code Mask не шифрує

інформацію, вона просто замінює відомі величини, використовувані в кодуванні CDMA сигналу секретними величинами, відомими тільки мобільному телефону та мережі. Таким чином підслуховування розмов без знання Private Long Code Mask є надзвичайно складним завданням. Більш того, мобільний телефон і мережа використовують CMEA і покращений CMEA (E_CMEA) алгоритми для шифрування і дешифрування службових повідомлень при передавання їх по ефіру. Окремий DATA-key і алгоритм шифрування ORYX використовується мобільним телефоном і мережею для шифрування і дешифрування потоку інформації по каналу зв'язку CDMA. Рисунок ілюструє механізми аутентифікації і шифрування в CDMA мережі.

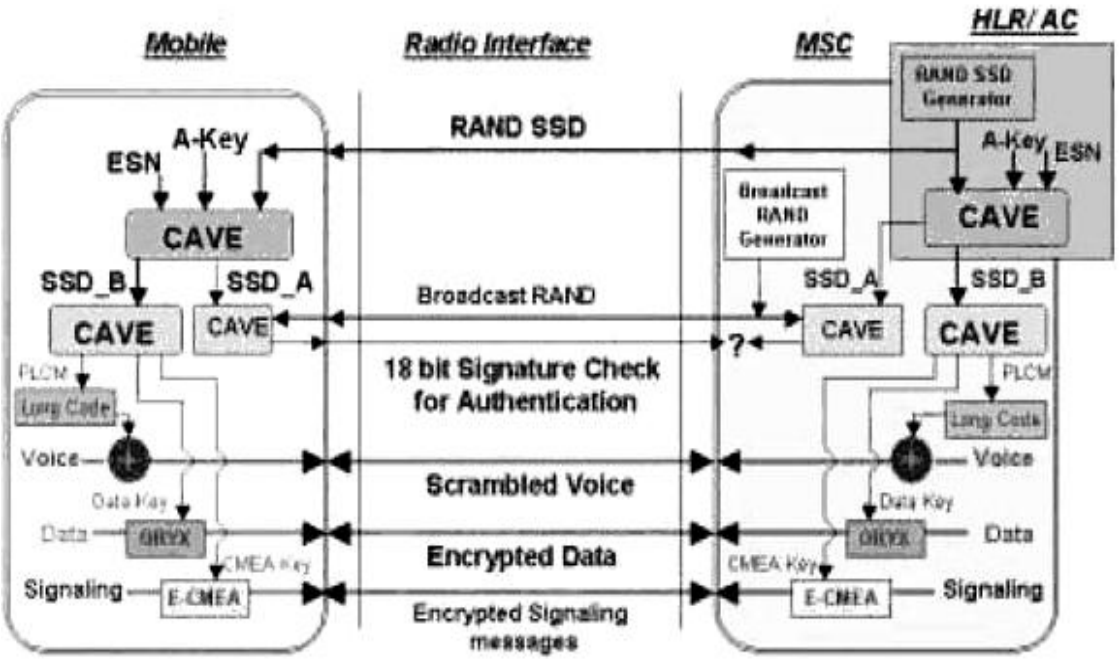


Рисунок 2.8 – Аутентифікація і шифрування в CDMA мережі

CDMA мережа підтримує призначення мобільному телефону тимчасового ідентифікатора мобільного абонента TMSI (Temporary Mobile Station Identifier) для його представлення в процесі передавання інформації по ефіру між мобільним телефоном і мережею. Ця функція ще більше ускладнює зіставлення переданих даних конкретному абоненту.

У стільникових стандартах третього покоління (3G) використовуються ще більш криптостійкі протоколи забезпечення безпеки системи, що включають використання 128-бітного секретного і аутентифікаційного ключів. У мережах третього покоління стандарту CDMA 2000 для хешування та перевірки достовірності використовується Secure Hashing Algorithm-1 (SHA-1), для шифрування повідомлень - Advanced Encryption Standard (AES Rijndael). Також для всіх наступних версій після CDMA 2000 Release C буде використовуватися AKA (Authentification and Key Agreement) протокол для аутентифікації і узгодження ключів. AKA протокол разом з алгоритмом Kasumi буде використовуватися і в WCDMA-MAP мережах для шифрування та перевірки достовірності повідомлень[25].

В даний час устаткування стандарту CDMA є найновішим і найдорожчим але в той же час найнадійнішим і найзахищенішим. Технологічні рішення і стійкі криптографічні протоколи, що знайшли застосування в цьому стандарті, забезпечують високий рівень конфіденційності мереж, побудованих на його основі. Підслухати з ефіру розмову можна, але вартість і складність обладнання здатного на таке значно вище ніж для інших стандартів. Причому ситуація ускладнюється тим, що при незначному видаленні від БС потужність випромінювана телефоном вкрай низька, тому підслуховувач повинен знаходиться в безпосередній близькості від об'єкта спостереження, а при значній відстані від БС взагалі не зрозуміло через яку БС працює телефон.

Архітектура системи безпеки UMTS охоплює чотири основні компоненти:

- Access domain security (Безпека доступу до домену).
- Network domain security (Доменна безпека мережі).
- User domain security (Доменна безпека користувача).
- Application domain security (Доменна безпека додатків).

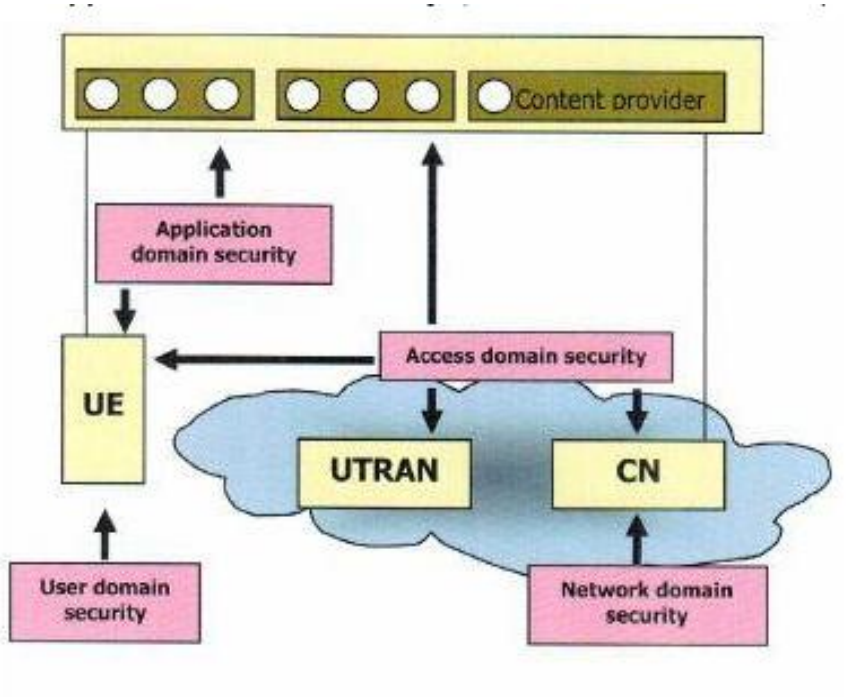


Рисунок. 2.9 – Архітектура безпеки в UMTS

Access domain security (Безпека доступу до домену) охоплює набір опцій безпеки, які надаються користувачам з безпечним доступом до сервісів UMTS, що захищає від атак через радіо інтерфейс.

Network domain security (Доменна безпека мережі) вирішує завдання безпеки на рівні мережевих елементів. Це забезпечує конфіденційність і захищає цілісність зв'язку (інформації) між різними мережевими елементами і між мережами різних операторів.

User domain security (Доменна безпека користувача) забезпечує безпечний доступ до призначеного для користувача устаткування, а також огляд і конфігурованість функцій безпеки.

Application domain security (Доменна безпека додатків) - набір опцій безпеки працюючих на вищому рівні-рівні архітектури базової мережі (Core Network). Ці можливості хоч і незалежні від самої мережі UMTS, але, все-таки, вони вносять свій внесок у всю систему безпеки [23].

У відповідності зі специфікаціями 3GPP, можливості, що забезпечують безпеку для UMTS повинні захищати інформацію, ресурси та сервіси, вироблені або замінені, у всій мережі, від неправильного використання.

Щоб зробити опції безпеки сумісними по всьому світу і мати можливість взаємодіяти з іншими мережами (роумінг між різними мережами), ці опції безпеки повинні бути стандартизовані. Крім того, система безпеки UMTS повинна забезпечувати більше рівнів захисту, ніж мобільні і стаціонарні мережі такого ж самого покоління, і повинна розширюватись, як цього вимагають нові загрози безпеці та сервіси.

Основний механізм безпеки в UMTS базується на моделі безпеки GSM. Безпека включає в себе:

– Поділ модуля абонента від терміналу.
– Аутентифікація.
– Шифрування.
– Конфіденційність ідентифікації абонента.
– Перевірка терміналу.
– Загрози безпеки в мережах 3G

Цілісність системи безпеки це найслабше місце. Тому можливі атаки проти безпеки можуть зосереджуватися на окремій частині цілої мережі, на тій частині мережі, яка не достатньо захищена. Загрози безпеки існують в кожній частині ланцюжка UMTS: мережевий оператор, постачальник послуг і контент-провайдер включаючи інтерфейси між залученими частинами. Фізично, місцем атаки може бути і радіо-інтерфейс, термінал і модуль абонента, або якась інша частина провідної мережі.

Можливі атаки на систему безпеки UMTS діляться на наступні категорії:

– Unauthorized access to data (Заборонений доступу до даних).
– Unauthorized manipulation of data (Заборонена операції (маніпуляції) з даними).
– Unauthorized access to services (Заборонений доступу до сервісів).
– Disturbing the network operation and service provisioning (Порушення забезпечення роботи мережі і сервісів).
– Repudiation (Відмова).

Unauthorized access to data (Заборонений доступ до даних) - є порушенням конфіденційності. У самому простому випадку, порушник підслуховує інформацію користувача, сигнальні дані та дані управління. Такий перехоплення зазвичай не виявляється мережею. Інший метод атак - це маскування (приховування) або легальних користувачів або легальних мереж, щоб отримати конфіденційну інформацію. Порушення конфіденційності означає також аналіз недозволеного трафіку (пасивного або активного), коли порушник отримує (видобуває) час, дату, кількість інформації, а також визначення положення користувача, наприклад, коли трапляються ділові угоди. Заборонений доступ до даних може також бути отриманий за допомогою доступу до реально існуючих систем, які містять велику кількість даних. Порушення конфіденційності може служити відправною точкою для інших атак схожих на маніпуляції з даними.

Unauthorized manipulation of data. Заборонені операції (маніпуляції) з даними - це порушення цілісності, недоторканності даних. Цей вид активних атак трапляється тоді, коли порушник змінює, вставляє, видаляє або перегравє повідомлення. Повідомлення користувачів можуть бути використані навіть, якщо порушник не буде здатний розшифрувати дані.

Unauthorized access to services. Заборонений доступ до сервісів може бути зроблений прихованими порушниками, а також користувачами або навіть мережевими об'єктами, або користувачами, які неправильно використовують свої права доступу. Також, обслуговуючі мережі можуть створювати такі види загроз безпеки у напрямку до домашньої мережі, наприклад, для доказу скритності користувача, щоб неможливо було фальсифікувати тарифікаційні запису користувача.

Disturbing the network operation and service provisioning. Порушення забезпечення роботи мережі і сервісів може привести до відмови або зменшення доступності сервісів. Такий вид атак досить важко запобігти. Одним із прикладів такої проблеми є фізична втручання в канал передавання

інформації. Атакуючий, наприклад, може обрізати дроти або заглушити радіо ефір.

Repudiation (Відмова) має місце тоді, коли в разі виникнення будь-кого не специфікованого події, користувач або мережу відкидають з'єднання. Тобто, здійснюється відмова від прийому чи передавання трафіку, особливо щодо тарифікації послуги.

Загроза безпеки обширна і включає в себе різні типи обману. Обман в телекомунікаціях найбільш активний, і в основному полягає в тому, щоб користуватися сервісами без оплати за них.

UTRAN - це частина системи UMTS, яка найбільш уразлива в питаннях безпеки. Існують на це дві причини:

– UTRAN забезпечує мобільність абонента.

– Особливості радіоінтерфейсу, який постійно піддається різним атакам.

Безпека UTRAN - це спосіб забезпечення безпечного доступу до UMTS. Особливості безпеки описуються в наступних розділах складають основну модель безпеки UMTS.

Типи процедур безпеки:

– Аутентифікація.

– Шифрування.

– Перевірка обладнання.

– Ідентифікація.

– Перевірка конфіденційності та захист проти дій з сигнальними повідомленнями.

Аутентифікація в UMTS відрізняється від аутентифікації GSM. Спочатку, мережа аутентифікує UE і UE перевіряє, чи може вона ввійти в мережу. Основний механізм аутентифікації називається Authentication and Key Agreement (AKA) - Аутентифікація і узгодження ключа. Останнє здійснюється використовуючи технологію запит - відповідь. Процедура аутентифікації

починається, після визначення мережею UE, тобто після того як MSC / VLR або SGSN отримує тимчасовий або постійний користувальницький ідентифікатор IMSI або TMSI.

Рисунок 2.10 – Аутентифікація і узгодження ключа в UMTS

Перша частина в аутентифікації AKA є поширення ідентифікаційної інформації від домашньої мережі на обслуговуючу мережу.

1.MSC/VLR або SGSN відправляє 'запит на аутентифікацію даних (Authentication Data Request)' на AUC домашньої мережі користувача. Це повідомлення містить у собі IMSI.

2. Після цього AUC, грунтуючись на даній інформації, генерує інформацію про безпеку, це один або кілька аутентифікаційних векторів (AV-Authentication Vectors) і відправляє їх назад на MSC / VLR або SGSN у вигляді відповіді на запит про аутентифікації '(Authentication Data Response) '. Набір векторів зберігається в обслуговуючій мережі. Кожен вектор може бути використаний тільки один раз, для одноразової процедури аутентифікації. Вектори використовуються послідовно. Якщо всі вектори закінчилися, то

обслуговуюча мережа запитує домашню за новими векторами. Вся сигналізація проходить по протоколу MAP.

3.Аутентифікація і створення ключа (Authentication and key establishment) починається тоді, коли MSC / VLR (SGSN) вибирає наступний придатний вектор (AV) і відправляє два його елементи (випадкове число і аутентифікаційні AUTN) на UE у вигляді відповіді користувача на аутентифікацію ' User Authentication response. ' RAND і AUTN передаються на USIM, яка (здійснює обчислення для генерації AV в AUC) виробляє схоже обчислення так, як це відбувається в AUC.

4.Як результат, USIM перевіряє легітимність AUTN. Якщо результат перевірки позитивний, тобто мережа, яка надає послугу аутентифікованій, UE передає повідомлення на MSC / VLR або SGSN відповіді користувача на аутентифікацію '(user authentication response)' в якому міститься параметр RES, який був обчислений UE.

MSC / VLR (SGSN) порівнює отриманий RES з тим, який був присланий з AUC, що є компонентом цього вектора. Якщо обидві послідовності однакові, то аутентифікація закінчується позитивно.

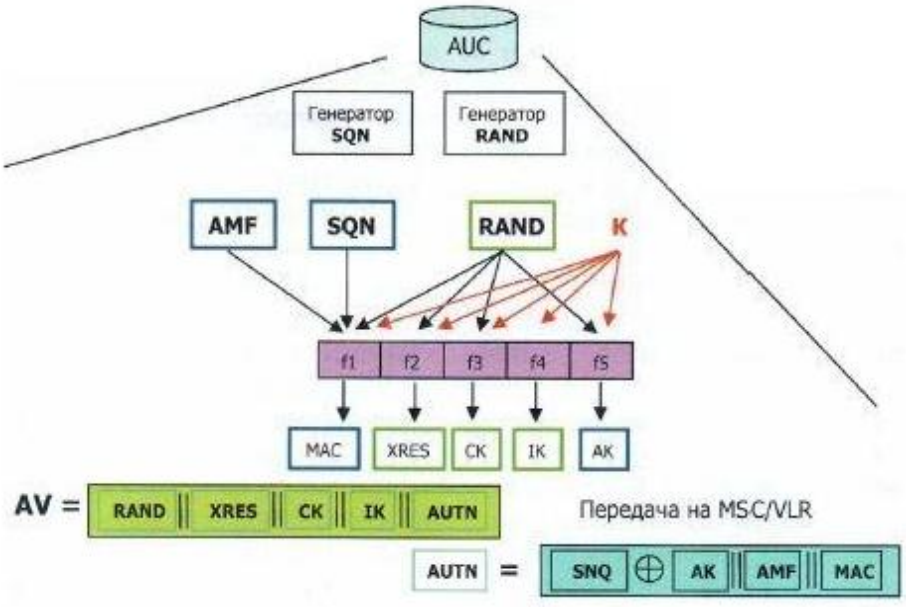


Рисунок – 2.11. Аутентифікації в AUC

Додатковим результатом успішної процедури аутентифікації, є наявність шифрування і цілісності захисту ключів, які будуть використовуватися USIM і RNC.

Процедура генерації векторів в AUC починається з генерації випадкового числа і вибору додаткових номерів SQN. Ці дві послідовності разом із ключем аутентифікації, який є постійним і секретним еталонним ключем для механізму безпеки і числом AMF є вхідними параметрами для алгоритмів F1-F5. Алгоритми F1-F5 не стандартизовані, але специфікації 3GPP надають тільки деякі основні вимоги та пропозиції. Так, наприклад, пропонується набір алгоритмів (званих MILENAGE) включених в специфікацію 3GPP TS 33.206. F1-F5 є власними специфічними алгоритмами домашньої мережі. Кожен з них є односторонньою функцією, яка означає, що її дуже просто вирахувати в одному напрямку (знаючи вхідні дані), але дуже складно в іншому (маючи вихідні дані, отримати вхідні дані). Іншою важливою властивістю є те, що з вихідних даних одного алгоритму немає ніякої інформації про вихідних даних інших алгоритмів. Можна припустити, що спроба перебрати всі можливі значення для отримання вхідних, вихідних параметрів односторонньої функції призведе до отримання необхідних значень. Але це практично неможливо, через низькість потужностей і велику довжину ключа шифрування.

В векторі AV міститися 5 параметрів: RAND, XRES, CK, IK і AUTH і тому, вони називаються 'квінтплетом', за аналогією з ктриплетом в GSM. У процесі аутентифікації ці п'ять параметрів періодично об'єднуються. AUTN отриманий складанням по модулю 2 номери SQN доданого до АК (XOR operational), з AMF і MAC.

Управління аутентифікацією в USIM показано на малюнку. Після отримання 'User authentication request', що включає RAND і AUTN, USIM спочатку застосовує алгоритм F5 для обчислення параметра АК. Потім АК разом з частиною AUTN використовується для отримання SQN. Перша перевірка яку робить USIM - з'ясовує, чи є правильним числом отриманий SQN і якщо це було збільшено з останньої спроби аутентифікації. Якщо ні, то можна

припустити, що зловмисник намагатиметься використовувати неправильний вектор. Крім цього, механізм, описаний вище захищає послану SQN у відкритому тексті. Якщо зловмисник зніме розширену SQN послідовність абонента, то він зможе отримати інформацію про це абонента і тоді може порушити його конфіденційність. Наступним кроком аутентифікації є обчислення вихідних даних за допомогою функцій F1-F4. Якщо обчислений параметр XMAC дорівнює отриманому MAC (в частині AUTN), то інформація UE є позитивною і RES може бути відправлений назад в мережу у вигляді 'Authentication Response Massage'. Користувацька аутентифікація запит / відповідь є частиною Non Access Stratum (NAS) повідомлень Mobility Management. Може трапитися так, що нумерація SQN закінчиться через синхронізації між терміналом і мережею і, як результат цього, - всі спроби аутентифікації будуть помилкові. У такому випадку передбачена спеціальна розсинхронізуюча процедура, протягом якої абонентський термінал інформує мережу про SQN і змінена послідовність SQN може бути вилучена.

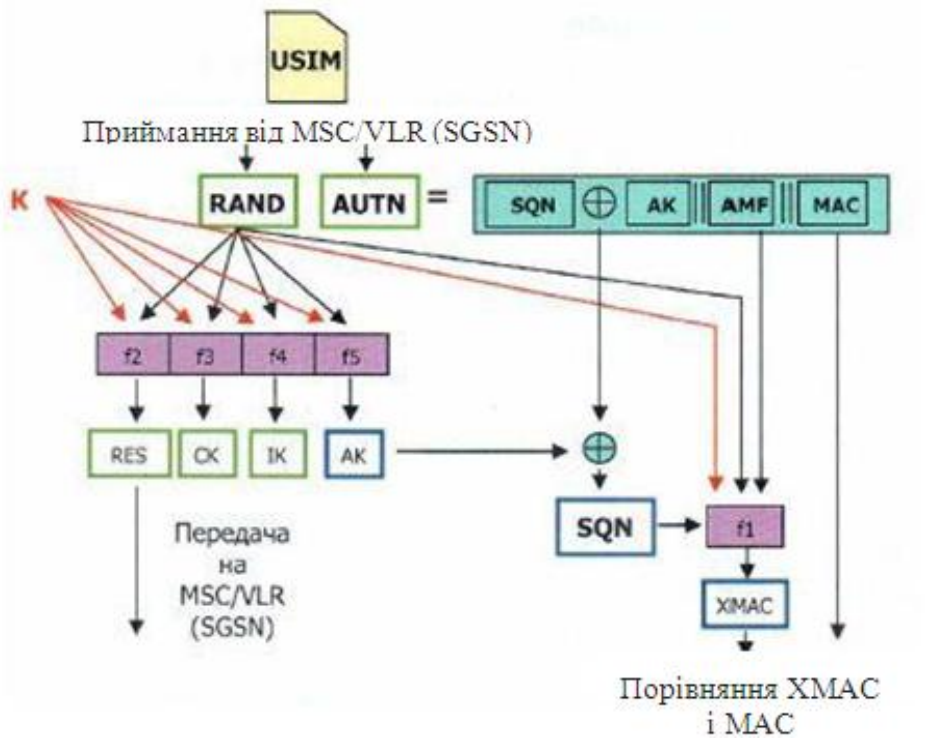


Рисунок 2.12 – USIM аутентифікація

Управління номером SQN здійснюється оператором. У кожного користувача є свій власний SQN генератор в мережі. В якості альтернативи, обчислення SQN може бути засноване на глобальному, загальному лічильнику для всіх користувачів.

Шифрування в UMTS (User Services Identity Module) застосовується як для користувача даних, так і для високих рівнів сигналізації, і здійснюється між UE і RNC. Після користувальницької аутентифікації ключ шифрування вже знаходиться в UE і в MSC / VLR (SGSN). До того як почнеться шифрування, параметр СК повинен бути переданий з CN в RNC. Це справляє протокол RANAP. Потім, у процесі встановлення з'єднання, RNC може включити шифрування відправкою повідомлення Security Mode Command (RRC) на термінал.

Шифрування в UMTS відбувається на другому рівні (L2), на рівні MAC (Media Access Control) або на рівні Radio Link Control (RLC). Точне місце розташування функції шифрування залежить від типу з'єднання та контролюється вищими рівнями, іменованими прозорими RLC сполуками. Якщо трафік передається прозоро через RLC, то шифрування відбувається в рівні MAC. Для непрозорих типів з'єднань це відбувається в RLC рівні. Шифрування виконується на індивідуальних логічних каналах.

Механізм шифрування ґрунтується на технології потокового шифрування. Незашифрований блок шифрується додаванням біта за бітом до ключа потокового блоку, з випадково вибраної маскою. Дешифрування на приймальному кінці відбувається по такому ж шляху, з такою ж маскою. Це відбувається, тому що додавання по модулю два з однієї і тієї ж маскою двічі в результаті дає вихідну послідовність на виході.

Існують 4 види вхідних даних для алгоритму шифрування окремо від СК (128 біт) і даних які шифруються.

Чотири види даних:

– Count-c - Номер шифрувальної послідовності. Це 32-бітний лічильник, який збільшує кожен блок даних. 'Count - з' містить 2 різних

лічильника: Hyper Frame Number (HFN) і Connection Frame Number (CFN) або RLC Sequence Number (RLC-SN). Мета COUNT-C гарантувати, що для кожного блоку даних буде використана різна маска шифрування.

– Bearer- 5 бітний ідентифікатор радіоканалу. Він використовується, щоб гарантувати, що для одних і тих же користувачів одночасно є безліч синхронних каналів, де маска шифрування завжди різна. Ризик наявності однакових масок для різних каналів пояснюється фактом, що Count-c використовується незалежно для кожного радіоканалу.

– Direction - один біт, що показує чи використовується шифрування в Uplink і в Downlink.

– Length - 16 бітний параметр, який визначає необхідну довжину маски для незашифрованому послідовності.

Беручи до уваги верхні 4 параметри, може виникнути таке запитання: для чого, для кожного блоку даних буде використовуватися своя відмінна маска? Відповідь закликає нас повернутися до особливості операції XOR, якщо однакове число додано 2 рази, то воно має результатом додавання 0. Якщо 2 блоку даних зашифровані різними масками і були додані один до одного, то будуть отримані однакові результати, то є два нерозшифрованих блоку даних. Сума двох блоків даних, якщо вона була прослухана зловмисником, може бути порівняно легко розкладена на прості компоненти.

Алгоритм шифрування для генерації масок називається F8. Він повністю стандартизований і доступний як блок функцій шифрування званий KASUMI, який працює на 64 бітних блоках даних і використовує 128-бітний ключ. Шифрування, незважаючи на те, що воно рекомендовано, є необов'язковим у UMTS.

Аналогічно шифруванню, захист цілісності використовується між UE і RNC. Вона завжди використовує рівень управління радіо ресурсу, і, отже захищена тільки сигналізація. У реальності, через деяких процедур перевірки, кількість інформації (даних) переданої протягом всього RRC з'єднання, а також обсяг інформації користувача є повністю захищеними.

Можливий варіант замінити справжні дані на невірні, але не зможливо додати або видалити що-небудь невизначеним способом.

Безпека в четвертому поколінні мобільного зв’язкувийшла ще на новий рівень захисту. Який включає захищений зв'язок (Security Association, SA) - одностороннє з'єднання для забезпечення захищеної передачі даних між пристроями мережі.

SA бувають двох типів:

- Data Security Association, захищений зв'язок для даних;
- Authorization Security Association, захищений зв'язок для авторизації.

Захищений зв'язок для даних

Захищений зв'язок для даних буває трьох типів:

- Первинна (основна) (Primary SA);
- Статична (Static SA);
- Динамічна (Dynamic SA).

Первинний захищений зв'язок встановлюються абонентською станцією на час процесу ініціалізації. Базова станція потім надає статичний захищений зв'язок. Що стосується динамічних захищених зв'язків, то вони встановлюються і ліквідуються в міру необхідності для сервісних потоків. Як статична, так і динамічна захищені зв'язки можуть бути однією для декількох абонентських станцій.

Захищений зв'язок для даних визначається:

- 16-бітовим ідентифікатором зв'язку;
- Методом шифрування, застосовуваним для захисту даних в з'єднанні;
- Двома Traffic Encryption Key (TEK, ключ шифрування трафіку), що тече і той, який буде використовуватися, коли у поточного TEK закінчиться термін життя;
- Двома двобітніми ідентифікаторами, по одному на кожен TEK;
- Часом життя TEK. Може мати значення від 30 хвилин до 7 днів. Значення за замовчуванням 12:00;

- Двома 64-бітними векторами ініціалізації, по одному на TEK (потрібно для алгоритму шифрування DES);

- Індикатором типу зв'язку (первинна, статична чи динамічна).

Абонентські станції зазвичай мають один захищений зв'язок для даних для вторинного частотного каналу управління (secondary management channel); і або один захищений зв'язок даних для з'єднання в обидві сторони (uplink і downlink), або один захищений зв'язок для передачі даних для підключення базової станції до абонентської і одну - для зворотного. Абонентська станція і базова станція поділяють один захищений зв'язок для авторизації. Базова станція використовує захищений зв'язок для авторизації для конфігурації захищеного зв'язку для даних(рис.2.13).

Захищений зв'язок для авторизації визначається:

- Сертифікатом X.509, що ідентифікує абонентську станцію, а також сертифікатом X.509, що ідентифікує виробника абонентської станції.

- 160-бітовим ключем авторизації (authorization key, AK). Використовується для аутентифікації при обміні ключами TEK.

- 4-бітовим ідентифікатором ключа авторизації.

- Часом життя ключа авторизації. Може приймати значення від 1 дня до 70 днів. Значення за замовчуванням 7 днів.

- 128-бітовим ключем шифрування ключа (Key encryption key, KEK). Використовується для шифрування і розподілу ключів TEK.

- Ключем HMAC для низхідних повідомлень (downlink) при обміні ключами TEK.

- Ключем HMAC для висхідних повідомлень (uplink) при обміні ключами TEK.

- Списком data SA, для яких дана абонентська станція авторизована.

KEK обчислюється таким чином:

1. Проводиться конкатенація шістнадцятирічного числа 0x53 з самим собою 64 рази. Виходять 512 біт.

2. Праворуч приписується ключ авторизації.

3. Обчислюється хеш-функція SHA-1 від цього числа. Виходять 160 біт на виході.

4. Перші 128 біт беруться як KEK, інші відкидаються.

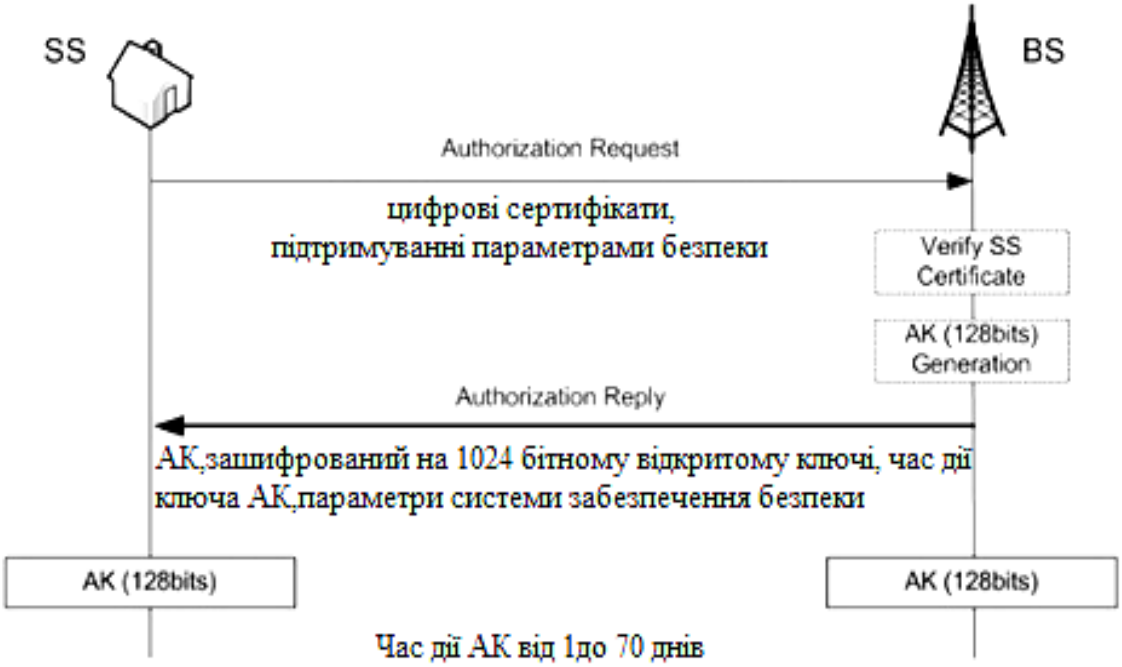


Рисунок – 2.13 – Процедура аутентифікації

Ключі HMAC обчислюються наступним чином:

1. Проводиться конкатенація шістнадцятирічного числа 0x3A (uplink) або 0x5C (downlink) з самим собою 64 рази.

2. Праворуч приписується ключ авторизації.

3. Обчислюється хеш-функція SHA-1 від цього числа. Виходять 160 біт на виході. Це і є ключ HMAC.

Для шифрування переданих даних необхідний спеціальний ключ, званий TEK. Цей ключ вибирається базової стації випадково, проте при його передачі на абонентську станцію використовується ключ AK, а також два додатково вироблених ключі: ключ шифрування ключів - KEK і ключ аутентифікації повідомлень - HMAC key. Ключ TEK шифрується одним із таких способів:

- За допомогою алгоритму 3DES на ключі KEK, при цьому довжина ключа KEK дорівнює 112 біт;

- За допомогою системи шифрування RSA, відкритий ключ береться з цифрового сертифікату X.509;

- За допомогою алгоритму AES на ключі KEK, довжина якого в цьому випадку дорівнює 128 біт.

При обміні повідомленнями хеш-функція HMAC-SHA1, що окрім контролю цілісності забезпечує захист від підміни (оскільки використовує ключ АК, відомий тільки АС і БС) (рис. 2.15)Для шифрування повідомлень стандарт передбачає використання алгоритму DES в режимі CBC або алгоритм AES в режимі CCM. Сам процес шифрування показаний на рис. 2.16 для алгоритму DES.

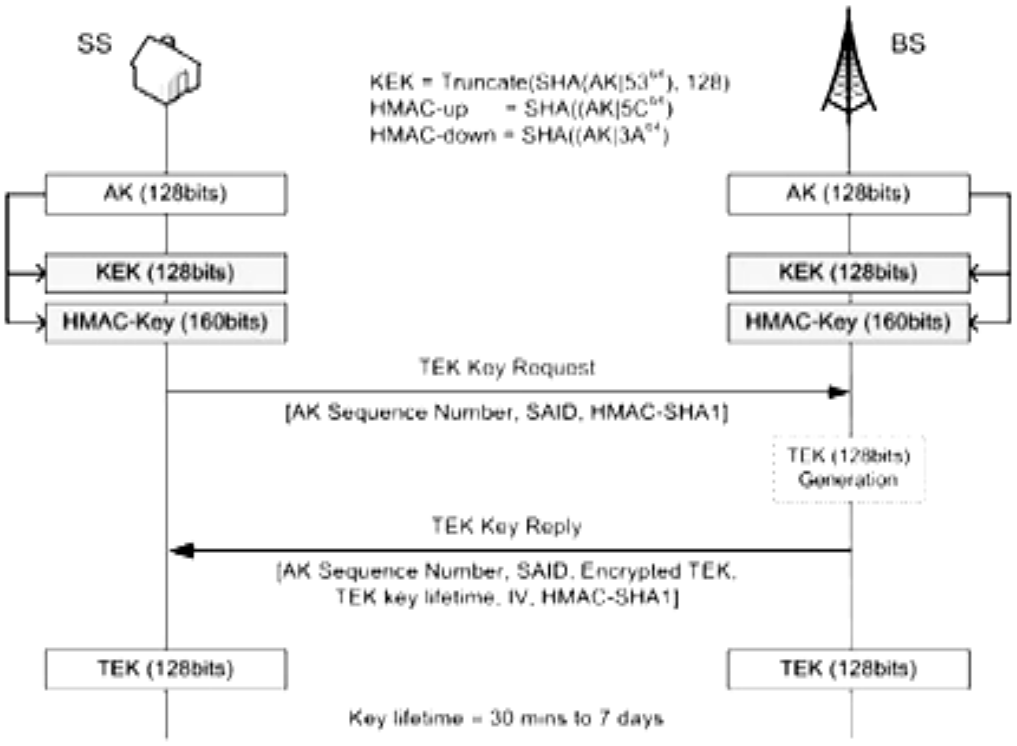


Рисунок – 2.14 – Передача ключа шифрування даних

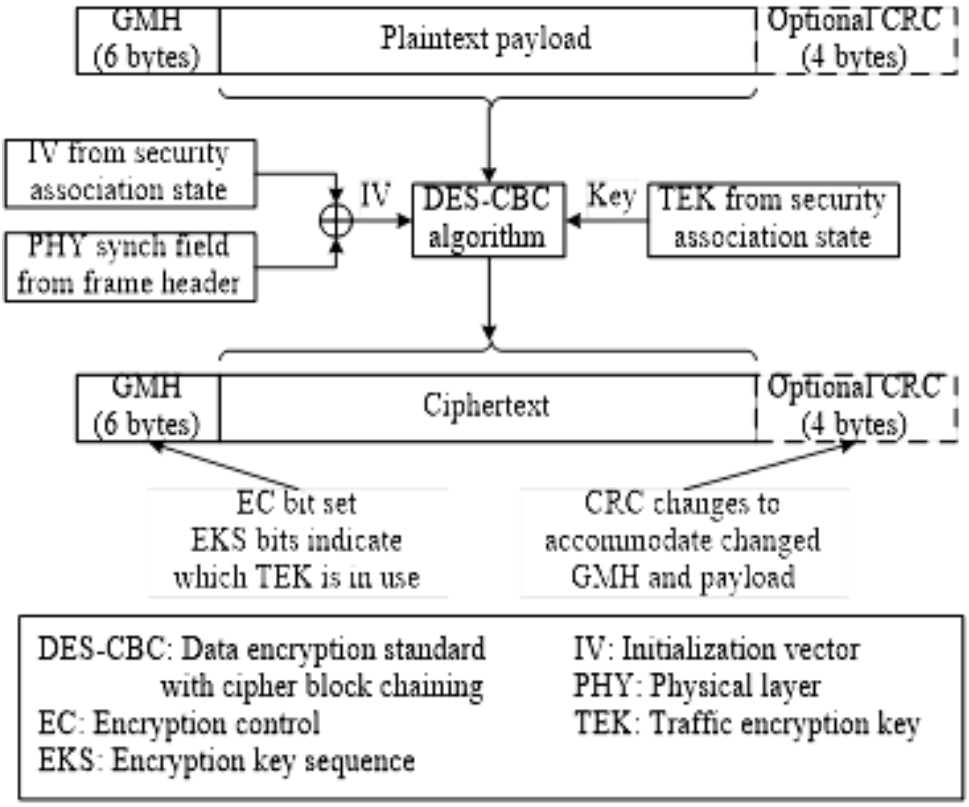
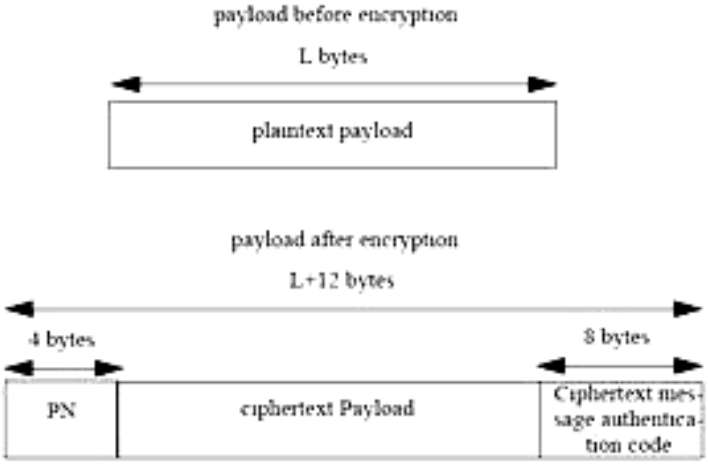


Рисунок – 2.15 – Процес шифрування даних за допомогою алгоритму DES у режимі CBC



Рисунок–2.16 – Структура шифрованого повідомлення при використанні алгоритму AES PN – номер пакета

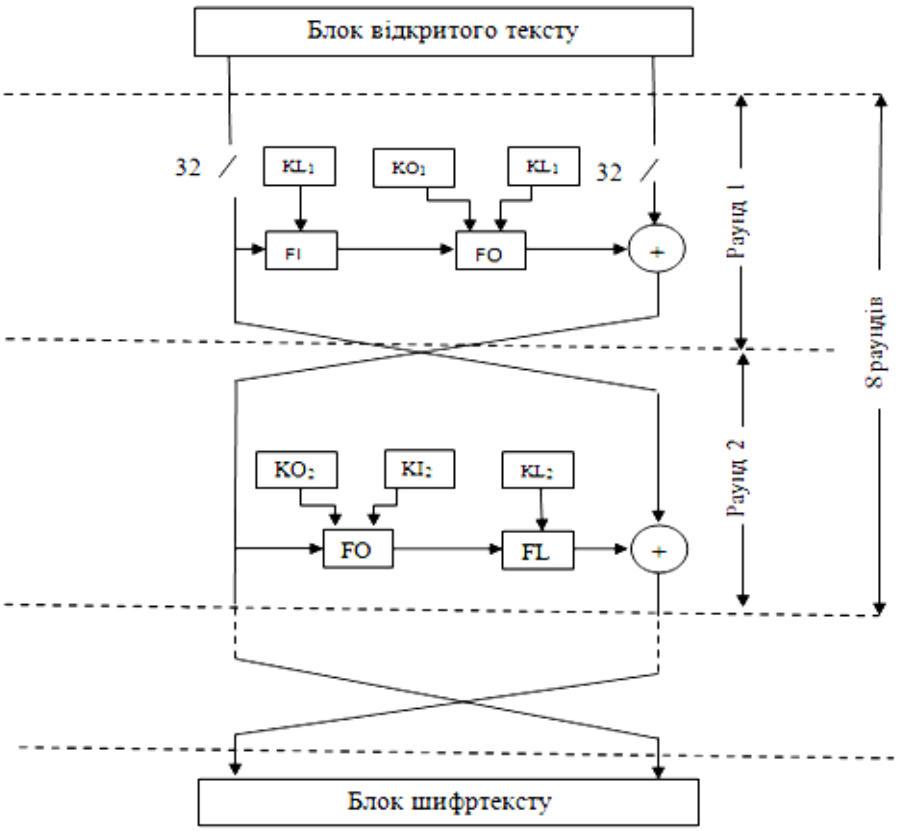
Недоліками можна вважати дефіцит обладнання, повністю відповідає всім вимогам і стандартам, які розробляються і приймаються організацією WiMAX - Forum. Устаткування, що випускається для WiMAX різними

виробниками, не сумісно один з одним і технічними характеристиками істотно відрізняються від тих, що були закладені в стандарт.

Обмеження використання частот введені ГОС. Комісією з розподілу частот. Після введення цих обмежень радіус дії і потужність базових станцій в діапазонах, в яких працює WiMAX, сильно обмежили, і в великому місті, чисельність населення якого більше 1 млн. Людина, радіус дії не повинен перевищувати 3 км. Пристрої з підтримкою WiMAX дороги Поки дуже обмежене мережі.

2.3 Структура алгоритму kasumi.

Алгоритм KASUMI має незвичайну структуру - він заснований на схемі Фейстеля . Спочатку 64-бітний шифруючий блок даних розбивається на два 32-бітових субблока, після чого виконується 8 раундів наступних перетворень рисунок 2.17.



Рисунок–2.17 – Структура алгоритму KASUMI.

Над оброблюваним субблоком виконуються залежні від ключа операції FL і FO (у зазначеній послідовності - в непарних раундах, в парних - навпаки).Результат цих операцій накладається побітової логічною операцією XOR на необроблений субблок. Після цього субблоки міняються місцями. Оброблюваний операції FL(рис.2.18) субблок розбивається на два 16-бітових фрагмента, над якими виконуються наступні дії :

$$R' = R \oplus ((L[\&KL]_{1}(i,2)) <<< 1);$$

$$L' = L \oplus ((R'|KL_{i,2}) <<< 1).$$

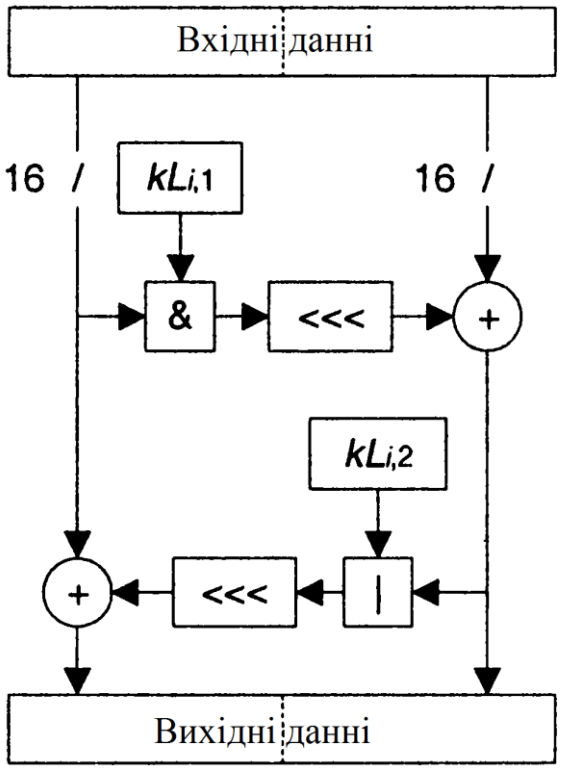
R і L вхідні значення лівого і правого фрагменту відповідно;

R` і L` вихідні значення

$KL_{i,1}$ і $KL_{i,2}$ фрагменти ключа і-го раунду для операції FL.

& і | - побітові логічні операції “і” та “або” відповідно;

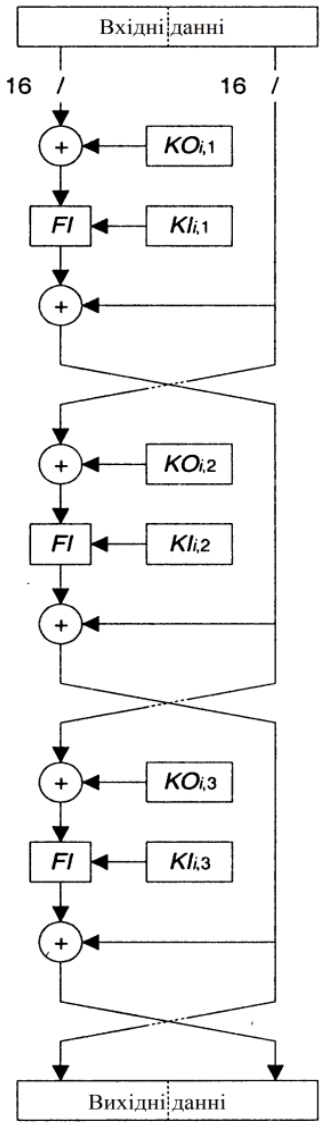
<<<1- побітове циклічне зміщення операнда на 1 біт в ліво



Рисунок–2.18 – Операція FL.

Операція FO більш цікава - вона являється вкладеною схемою Фейстеля рис 2.19. Як і раніше ,вхідне значення розбивається на два 16- бітних фрагмента, після чого виконуються три раунди наступних дій:

1. На лівий фрагмент операції XOR накладається фрагмент ключа раунду $KO_{i,j}$ (j- номер раунду операції FO).
2. Виконується залежна від ключа операція FL.
3. На лівий фрагмент накладається операція XOR значення правого фрагменту.
4.Фрагменти міняються місцями.



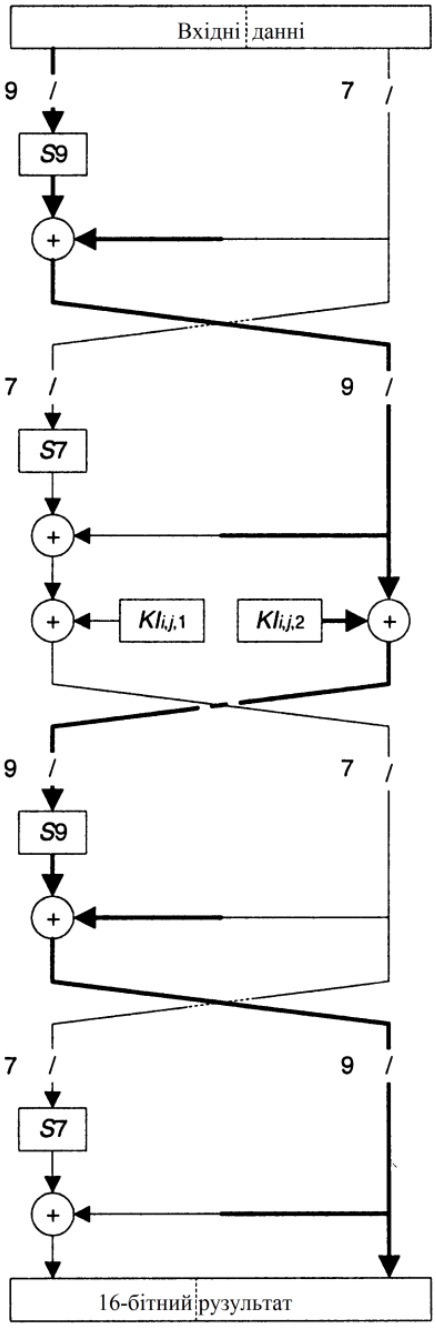
Рисунок–2.19 – Операція FO.

Операція FI також представляє собою схему Фейстеля , це вже третій рівень вкладеності. Відмінно від схеми Фейстеля на двох верхніх рівнях , дана

схема являється не збалансованою: оброблювальні 16-ти бітні фрагменти діляться на дві частини :9- бітну ліву і 7-бітну праву. Потім виконується 4 раунда ,які складаються з наступних дій(рис.2.20) :

Ліва частина пропускається через таблицю зміни. 9-бітна частина (в не парних раундах) обробляється таблицею S9, а 7-бітна (в парних раундах)-таблицею S7. Ці таблиці повність наведені в дипломній роботі в розділі 3.2 .

Крім того, враховувати той факт ,що алгоритм KASUMI призначений попередньо для апаратної реалізації ,в том числі в пристроях, маючих обмежений ресурс, біти вихідного значення таблиць замін можуть вираховуватись із бітів вхідного значення. В цих обчисленнях використовуються тільки побітові логічні операції ‘і’ або XOR; Формули обрахунку приведені в розділі 3.1 схема шифрування.На ліву частину операції XOR накладається текуче значення правої частини. При цьому,якщо справа 7-бітова частина , вона доповнюється нулями з ліва ,а у 9-бітовій частині видаляються зліва два біта. В другому раунді на ліву частину операцією XOR накладається фрагмент ключа раунду $KI_{i,j,1}$,а на праву – фрагмент $KI_{i,j,2}$.В інших раундах ці дії не виконуються. Після цього ліва і права частина міняються місцями.



Рисунок–2.20 – Операція FI.

З вище поданого зрозуміло що в алгоритмі виконується багато простих операцій,скомбінованих доволі оригінальним чином.

РОЗДІЛ 3
СТВОРЕННЯ ПРОГРАМИ НА ОСНОВІ МОДИФІКОВАНОГО БЛОЧНОГО ШИФРУ KASUMI

3.2. Криптоаналіз і модифікація алгоритму алгоритму.

Надійність криптоалгоритму визначається його криптостійкістю. Виділяють поняття теоретичної криптографічної стійкості, яка вказується розробниками шифру і, як правило, є кількістю можливих варіантів значень ключа при методі повного перебору. Також, виокремлюють поняття практична криптографічна стійкість алгоритму шифрування, яка визначається на основі застосування відомих, більш ефективних, аніж повний перебір методів.

При розробці алгоритм Kasumi був підданий первинному аналізу командою розробників . А після того, як специфікація алгоритму була визначена, Kasumi було надано для дослідження трьом незалежним групам спеціалістів-криптологів. В результаті аналізу всі групи фахівців зробили висновок про те, що, по-перше, не виявлено яких-небудь атак на алгоритм KASUMI, здійсненних на практиці: по-друге, алгоритм повністю відповідає його передбачуваним застосуванням.

Коли криптоаналітики не можуть знайти недоліки повно функціональної версії досліджуваного алгоритма,виконується аналіз обрізаних версій, перш за все варіантів алгоритма з зменшеною кількістю раундів. Про крипто стійкість алгоритму можна зробити висновок при наявності достатньої кількості криптоаналітичних робіт, присвячених його обрізаним версіям.

Досліджуючи алгоритм є варіант атаки на пов'язаних ключах на пяти раундову версію KASUMI. Для успішного здійснення даної атаки потрібна

наявність приблизно 2^{26} обраних відкритих текстів і близько 2^{26} тестових операції шифрування. Цю атаку можна здійснити завдяки тому, що процедура розширення ключа алгоритму KASUMI істотно спрощена з метою спростити апаратну реалізацію алгоритму і прискорити процес розгортки ключа шифрування. Алгоритм KASUMI з оригінальною процедурою розширення ключа подібній атаці не схильний. Аналогічна атака можлива і на 6-раундовую версію KASUMI; для неї необхідно наявність такої ж кількості обраних 2^{26} відкритих текстів і близько 2^{26} спроб шифрування. Також успішну атаку можливо провести методом диференціального крипптоанализа 5-раундну версію алгоритму, яка розкривається при наявності 2^{32} обраних відкритих 2^{32} текстів виконанням операцій шифрування. Є такі атаки на скорочені версії алгоритму (за винятком атаки на алгоритм без функції FL) досить складно здійсненні на практиці.

З недоліків можна виділити процедуру розширення ключа Kasumi яка виконується довше ніж в інших відомих методах шифрування ,але незважаючи на це алгорим вважається досить сильним.

Для виправлення цього недоліку модифікується набір фрагментів розширеного ключа щоб «набирались» по мірі виконання перетворень з масивів K1..K8 і K1'.. K8'. А 16-бітний фрагмент $KI_{i,j}$ ділився на 7 бітний

фрагмент $KI_{i,j1}$ і 9 бітний $KI_{i,j,2}$.Таким чином розширення ключа може проводитися «на льоту », тобто в процесі виконання шифрування, що є безперечним плюсом алгоритму, особливо в умовах обмежених ресурсів оперативної пам'яті.Тим самим скорочується час виконання даної процедури.

Для забезпечення захисту в 3g мережі, алгоритм kasumi вводжу в якоті ядра в алгоритм f8 який використовується для шифрування даних що передаються в 3G мережі.

Алгоритм f8 представляє собою алгоритм потокового шифрування, в якому блоковий шифр kasumi використаю для генерації псевдовипадкової послідовності (гами шифру).Отримана послідовність S накладається на шифровані дані операцією XOR:

$$C = M \oplus S$$

де M- шифруюче повідомлення, а C- отриманий в результаті шифрування шифрований текст.

Одержувач шифртекста генерує таку ж псевдовипадкову послідовність, яку накладає повторно для отримання вихідної інформації:

$$M = C \oplus S$$

Структура алгоритму f8 з введенням шифрування kasumi приведена на рисунку 3.1. Алгоритм f8 є досить простим.Спочатку формується 64 бітове початкове значення алгоритму, що складається з наступних даних:

- 32-бітний номер генеруючої послідовності;
- 5-бітове значення, специфічне для конкретного користувача;
- біт, що визначає напрямок (вхідні або вихідні) передачі шифрованих даних;

– доповнення бітовими нулями до 64 бітів.

Після цього виконується шифрування алгоритмом kasumi (на рисунку 3.1 позначено як Е) початкового значення на ключі, що є результатом застосування операції XOR до ключа шифрування К1 (унікальному для кожного користувача) і константі С1, використовуючу для модифікації ключа.Після цього для шифрування кожного 64-бітного блоку шіфрується дані (повного або неповного) наступним чином генерується гамма шифру.

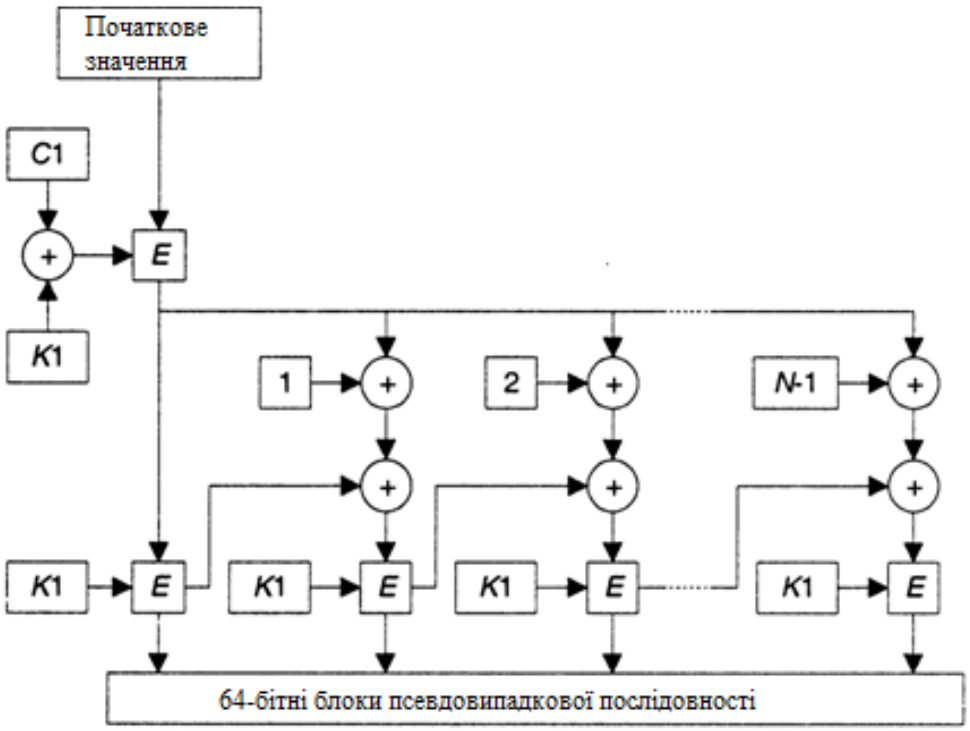


Рисунок – 3.1 –Алгоритму f8 з введенням шифрування kasumi.

На результат кроку 2 операцій XOR накладається 64- бітове значення, що відповідає номеру поточного блоку (від 0 до N-1, де N- необхідна кількість блоків).До результату попередньої дії застосовується операція XOR з попереднім блоком гами шифру; при генерації першого блоку гами ця дія не виконується.Виконується шифруфання результату попередньої операції на ключі К1. Вихідне значення і є вираховуваним блоком гами шифру

Практична частина передбачала створення програми шифрування модифікованим шифром Kasumi в якості ядра для алгоритму f8 . Дана прогрма

реалізована в інтегрованому середовищі розробки Microsoft Visual C++, результат роботи поданий в додатку Б.Лістинг програми додаток А.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ

4.1.Поняття про електробезпеку.

Сучасне виробництво нерозривно пов'язане з використанням електроенергії. В умовах експлуатації потужних енергосистем, електричних машин та апаратів, розвитку обчислювальної техніки і приладобудування, роботизації та комп'ютеризації виробництва важливого значення набуває проблема в електробезпеці — захисті електротехнічного персоналу та інших осіб, які обслуговують електроустаткування від ураження електричним струмом.

Аналіз загальної кількості виробничих нещасних випадків свідчить, що кількість електротравм становить 1,0-1,5%, а в енергетиці навіть 3-5%. Але серед нещасних випадків зі смертельним наслідком електротравми становлять 20-40% на виробництві, а в енергетиці до 60%, займаючи одне з перших місць. При цьому 60-85% смертельних уражень електричним струмом відбувається в електроустановках напругою до 1000 В (127-380 В).

Електротравматизм порівняно з іншими видами травматизму має деякі відмінні особливості.

Перша особливість полягає у тому, що організм людини не має органів, за допомогою яких можна дистанційно визначити наявність напруги, як, наприклад, теплову, світлову енергію, деталі, які рухаються. Тому захисна реакція організму виявляється тільки після потрапляння під напругу.

Друга особливість електротравматизму полягає в тому, що струм, який проходить крізь людину, діє не тільки в місцях контактів та на шляху протікання крізь організм, а й викликає рефлекторну взаємодію, спричиняючи

порушення нормальної діяльності окремих органів (серцево-судинної системи, системи дихання).

Третьою особливістю є можливість отримання електротравми, не маючи безпосереднього контакту зі струмопровідними частинами - переміщення по землі поблизу пошкодженої установки (у випадку замикання на землю), ураження через електричну дугу.

Четверта особливість електротравматизму — це те, що у більшості випадків для розслідування, обліку та аналізу доступні тільки електротравми з тяжкими та смертельними наслідками.

Електробезпечність у приміщенні лабораторії пропоную забезпечити наступними технічними способами і засобами захисту:

- для зменшення накопичення статичної електрики застосовувати зволожувачі і нейтралізатори, антистатичне покриття підлоги;
- забезпечити приєднання металевих корпусів устаткування до жили, що заземлює. Заземлення корпуса ПК забезпечити підведенням жили, що заземлює, до розеток. Опір заземлення 4 Ом, згідно (ПУЗ) для електроустановок з напругою до 1000 В.

Також організаційними заходами:

- своєчасне проведення інструктажів з техніки безпеки;
- заборонених використання непередбачених у лабораторії електричних приладів, таких як електричні чайники, обігрівачі.
-

4.2 Організація захисного заземлення.

Одними з важливіших заходів з забезпечення електробезпеки є організація захисного заземлення, занулення та захисного відключення. Для розрахунків захисного заземлення можна використати характеристики пристрою, які наведені в таблиці 4.1.

Таблиця 4.1 – Характеристики пристрою захисного заземлення

Передостання цифра	d, м	l, м	h, м	Остання цифра	a, м	b, м	Тип ґрунту	Вологість ґрунту
0	0,05	2,3	0,8	0	4,5	0,06	Ж	В
1	0,05	2,4	0,8	1	2,0	0,04	А	В
2	0,05	2,5	1,0	2	3,0	0,04	Б	В
3	0.10	2,6	0,5	3	4,0	0,05	В	С
4	0,10	2,7	0,9	4	5,0	0,05	Г	С
5	0,05	2,8	0,6	5	6,0	0,06	Д	Н
6	0,05	2,9	0,4	6	7,0	0,06	Ж	Н
7	0,10	3,0	1,2	7	8,0	0,04	З	В
8	0,10	2,0	0,7	8	9,0	0,04	А	С
9	0,05	2,2	1,0	9	2,5	0,06	Г	Н

У непарних варіантах заземлювачі розташовані по контуру, в парних – в ряд.Вид ґрунту: А – пісок, Б – супісок, В – кам‘янистий грунт, Г – суг-линок, Д – глина, Ж – чорнозем, З – садова земля. Вологість ґрунту: В – велика, С – середня, Н – низька.

Методика розрахунку захисного заземлення . Розрахунок системи захисного заземлення, яка виконана з вертикальних труб, з'єднаних стрічковою шиною та розташованих по контуру будівлі.

Характеристики пристрою: довжина труби 2,4 м; діаметр труби 0,05 м; відстань між трубами 2,4 м; заглиблення пристрою 0,8 м; ширина смуги 0,8 м.

Захисне заземлення розташовано в III кліматичній зоні, тип ґрунту – чорнозем.Розрахунок захисного заземлення здійснюється у такій послідовності:

- визначають розрахунковий питомий опір ґрунту;
- розраховують опір розтіканню струму одного вертикального заземлювача;
- визначають необхідну кількість заземлювачів та орієнтовне їх розташування по периметру приміщення або в ряд з визначенням відстані

між ними (відстань між заземлювачами та розташування їх в ряд або по контуру можуть бути задані(табл. 4.1);

- розраховують опір розтіканню з'єднувальної шини;

- розраховують загальний опір заземлюючого пристрою з урахуванням з'єднувальної шини.

Розрахунковий питомий опір ґрунту визначають за формулою:

$$\rho_p = \rho \times \varphi$$

де ρ – питомий опір ґрунту за вимірами або орієнтовно за даними (табл.4.2).

Таблиця 4.2

Питомий опір ґрунтів і води та кліматичного коефіцієнту

Грунт, вода	Питомий опір, Ом м·			Кліматичний коефіцієнт		
	При вологості 10-12% до маси ґрунту	Межі коливань	Рекомендоване для приблиз-них розрахун-ків	φ_1	φ 2	φ 3
1	2	3	4	5	6	7
Глина	40	8-70	60	1,6	1,3	1,2
Гравій, щебінь	–	–	2000	–	–	–
Кам‘яний грунт	–	500-800	4000	–	–	–
Пісок	700	400-2500	500	2,4	1,56	1,2
Садова земля	40	30-60	50	–	1,3	1,2
Суглинок	100	40-150	100	2	1,5	1,4
Супесок	300	150-400	300	2	1,5	1,4
Торф	20	10-30	20	1,4	1,1	1
Чернозем	200	9-53	30	–	1,32	1,2
Вода:	–	–	–	–	–	–
у струмках	–	10-60	–	–	–	–
грунтовая	–	20-70	–	–	–	–
морська	–	0,2-1	–	–	–	–
ставкова	–	40-50	–	–	–	–
річна	–	10-100	–	–	–	–

φ_1 -при великій вологості ґрунту; φ_2 – при середній вологості ґрунту; φ_3 – при сухому грунті.

$$\rho_р = \rho \times \varphi = 30 \times 1,5 = 450 \text{м} \times \text{м}$$

де φ – коефіцієнт сезонності, що залежить від кліматичних зон та виду заземлювача.

Опір розтіканню струму одного вертикального стрижневого (трубчатого) заземлювача при заглибленні визначаєтьсяза формулою:

де l – довжина заземлювача, м;

d – діаметр заземлювача, м;

h – заглиблення заземлювача, м;

t – відстань від поверхні землі до середини заземлювача, м.

$$t = h + \frac{l}{2} = 0,8 + \frac{2,4}{2} = 2\text{м}.$$

Орієнтовна кількість вертикальних заземлювачів :

$$n' = \frac{R_{од}}{R_н},$$

де $R_н$ – найбільший допустимий опір заземлюючого пристрою (згідно з «Правилами устройства електроустановок» $R_н$= 4 Ом).

$$n' = \frac{R_{од}}{R_н} = 14,\frac{5}{4} = 3,625 \approx 4 шт.$$

Шляхом розташування отриманої кількості заземлювачів на плані визначають орієнтовно відстань між ними та коефіцієнт використання вертикальних заземлювачів ήв залежно від кількості стрижнів і відношення відстані між ними до їх довжини. Необхідна кількість заземлювачів з урахуванням коефіцієнта використання $ή_в$:

де L — довжина шини, м;

b – ширина шини, м;

$ή_ш$–коефіцієнт використання шини, м.

Довжина шини визначається за формулою:

$$L=1,5a\ n,$$

де а – відстань між заземлювачами, м.

Визначаємо коефіцієнт використання та довжину шини:

$$ή_ш=0,74,\quad L=1,05\times 2,4\times 5 = 12,6$$

Загальний опір складного заземлюючого пристрою, Ом:

$$R = \frac{1}{\frac{\eta_ш}{R_ш} + \frac{n\eta_в}{R_{од}}} \leq R_н$$

Якщо загальний опір більший від нормативного, необхідно збільши-ти кількість заземлювачів або змінити їх розташування.

Розраховане значення опору заземлюючого пристрою менше норма-тивного (1,3 Ом < 4 Ом), отже пристрій спроектовано вірно.

Розрахунок занулення полягає у визначенні, окрім необхідної кілько-сті заземлювачів і загального опору заземлюючого пристрою за формулами (55) – (60), ще потрібної площі перерізу нульового проводу шляхом визначення необхідного його опору, за яким електроустаткування вимкнеться при виникненні струму короткого замикання у випадку пошкодження
ізоляції та замиканні на корпус.

Порядок розрахунку:

– визначають опір робочого заземлення нульової точки трансформатора (генератора) за формулами (55) – (60);

– визначають силу струму короткого замикання при замиканні фази
на корпус та перевіряють надійність захисного пристрою;

–визначають найбільший опір нульового проводу, при якому електрообладнання вимкнеться при появі струму короткого замикання;

– розраховують потрібну площу перерізу нульового проводу за формулою.

Для надійного спрацювання захисту повинна виконуватись така умова:

$$I_k \geq kI_{ном.},$$

де $I_к$ - сила струму короткого замикання при замиканні фази на кор-пус, А;

k – коефіцієнт перевищення (при використанні плавкої вставки запобіжника k = 3, для вибухонебезпечної зони k = 4; при використанні автомата k = 1,4 при номінальному струмі меншому за 100 А; k = 1,25 при номі-нальному струмі більшому за 100 А; для вибухонебезпечної зони k = 6);

$I_{ном}$ – номінальний струм плавкої вставки запобіжника або струм спрацювання автомата (табл. 4.3).

Таблиця 4.3

Значення номінального струму для деяких запобіжних пристроїв.

Тип запобіжного пристрою	Номінальний струм, А
НПИ 15	6, 10, 15
НПН 60М	20, 25, 35, 45, 60
ПН2-100	30, 40, 50, 60, 80, 100
ПН2-250	80, 100, 120, 150, 200, 250
ПН2-400	200, 250, 300, 350, 400
ПН2-600	300, 400, 500, 600
ПН2-1000	500, 600, 750, 800, 1000

Сила струму короткого замикання при замиканні фази на корпус визначається за формулою:

$$I_k = \frac{U_{\text{ф}}}{\frac{R_{\text{тр}}}{3} + R_{\text{п}}},$$

де $U_ф$ – фазова напруга,

$R_{тр}$ – опір трансформатора (за довідковими даними відповідно до типу трансформатора –тфлиця 4.4;

Таблиця 4.4

Повній опір масляних трансформаторів

Потужність трансформатора, кВА	Опір трансформатора (Ом), при схемі з‘єднання обмоток	
	зіркою	трикутником
25	3,11	0,906
40	1,949	0,562
63	1,237	0,360
100	0,799	0,226
160	0,487	0,141
250	0,312	0,090
400	0,195	0,056
630	0,129	0,042
1000	0,081	0,027

де $R_п$– опір петлі фаза – нуль, Ом.

Необхідний опір (найбільший) нульового проводу, при якому електрообладнання вимкнеться при появі струму короткого замикання:

,

Потрібна площа перерізу нульового проводу, мм^2:

$$S = \frac{\rho_п l_п}{2R_N},$$

де $\rho_п$ -питомий опір проводів, Ом мм^2 / м (мідних – 0,018; алюмінієвих – 0,028);

$l_п$ -довжина петлі фаза – нуль, м.

При розрахунку занулення необхідні дані тип трансформатора, схема з‘єднання обмоток, матеріал проводів, довжина петлі фаза - нуль.

ВИСНОВКИ

Метою даної роботи було проаналізувати мобільні стандарти які використовуються у світі, як відбувається в них захист інформації,а також провести криптоаналіз і модифікувати шифрування Kasumi а також програмно реалізувати шифрування.

Сьогодні досить актуальною є проблема безпеки інформації. Поняття «безпека» охоплює широке коло інтересів як окремих осіб, так і цілих держав. У наш мобільний час важливе місце відводиться проблемі інформаційної безпеки, забезпечення захисту конфіденційності інформації.

Для захисту інформації на рівні прикладного та системного ПЗ використовуються системи розмежування доступу до інформації, системи ідентифікації та автентифікації, системи аудиту та моніторингу, системи антивірусного захисту. Основним методом шифрування інформації – є криптографічний. На сучасному етапі розвитку науки і техніки саме криптографія дає можливість забезпечити безпечний обмін інформацію.

У даній роботі було проаналізовано методи та алгоритми шифрування в мобільному зв’язку їх основні характеристи . А також проведено криптоаналіз шифрування Kasumi і введення його в якоості ядра в алгоритм шифрування f8 який використовується для шифрування даних в мобільному зв’язку третього покоління. Реалізовано програмно шифрування алгоритму f8 з включеням в ядрого , шифрування Kasumi. Дана прогрма реалізована в інтегрованому середовищі розробки Microsoft Visual C++.