ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ
ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Захист інформації у мережах мобільних операторів стандарту GSM»

на здобуття освітнього ступеня магістра
зі спеціальності __125 _____Кібербезпека та захист інформації»_____
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Артем КОБЕЦЬ

Виконав: здобувач вищої освіти групи СЗДМ 61
Артем КОБЕЦЬ

Керівник:_____Андрій КОТЕНКО_____
к.т.н., доцент (Ім'я, ПРІЗВИЩЕ)

Рецензент:_____
(Ім'я, ПРІЗВИЩЕ)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ
ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУРОБОТУ

КобецЮ Артему Валентиновичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Захист інформації у мережах мобільних операторів стандарту GSM»
керівник кваліфікаційної роботи _____Андрій КОТЕНКО к.т.н., доцент

затверджені наказом Державного університету інформаційно-комунікаційних технологій
від « 15 » жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи _____

3. Вихідні дані до кваліфікаційної роботи:
__Мережа зв'язку сигналами стандарту GSM_____
__Особливості використання сигналів GSM_____
__Принципи захисту інформації стандарту GSM_____

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1.__Особливості сигналів стандарту GSM_____
2.__Огляд існуючих методів захисту сигналів стандарту GSM_____
3.__Алгоритми шифрування сигналів стандарту GSM_____

5. Перелік графічного матеріалу: ___Презентаційний матеріал на 12 слайдах_____

6. Дата видачі завдання _____20.10.2024 ___ _____

рту GSM / Всеукраїнська конференція «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем», 5 листопада 2024 р. Державний університет інформаційно-комунікаційних технологій - Київ: 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка презентаційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ __Артем КОБЕЦЬ__
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ __Андрій КОТЕНКО_
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи: 74 стор., 13 рис., 18 джерел, 6 таблиць.

Об'єкт дослідження – Процес захисту інформації у мережах мобільних операторів.

Предмет дослідження – Захист інформації стандарту GSM.

Мета роботи – Підвищення захищеності інформаціїї в мережах стандарту GSM шляхом використання криптоалгоритму.

Методи дослідження – системний аналіз, чисельні методи.

Магістерська робота присвячена підвищенню якості захисту інформації в мережах стандарту GSM.

Проаналізовано існуючі методи захисту інформації стандарту GSM. Зроблено огляд криптоалгоритмів що можуть бути застосовані для захисту мовленевої інформації яка передається мережами стандарту GSM

Ґрунтуючись на проведеному досліджені розроблено рекомендації по підвищенню якості захисту інформації у мережах мобільних операторів стандарту GSM.

Галузь використання – кібербезпека стільникових мереж стандарту GSM.

Апробація:

А.В. Кобець Захист інформації у мережах мобільних операторів стандарту gsm. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.90 - 91.
https://duikt.edu.ua/uploads/p_2661_93669247.pdf

КРИПТОАЛГОРИТМ, БЕЗПЕКА МОБІЛЬНИХ СИСТЕМ, GSM, AES, СТІЙКІСТЬ КРИПТОАЛГОРИТМУ, ОБРОБКА ЗВУКОВОГО СИГНАЛУ, ВІДКРИТИЙ КЛЮЧ

ABSTRACT

The text part of the bachelor's (master's) qualification work: 74 pages, 13 figures, 18 sources, 6 tables.

Object of research – The process of information protection in mobile operator networks.

Subject of research – Information protection of the GSM standard.

Purpose of work – Increasing information security in GSM standard networks by using a crypto algorithm.

Research methods – system analysis, numerical methods.

The master's thesis is devoted to improving the quality of information protection in GSM standard networks.

Existing methods of information protection of the GSM standard are analyzed. A review of crypto algorithms that can be used to protect speech information transmitted by GSM standard networks is made

Based on the research conducted, recommendations have been developed to improve the quality of information protection in GSM standard mobile operator networks.

Field of application – cybersecurity of GSM standard cellular networks.

Approbation:

A.V. Kobets Information protection in networks of mobile operators of the GSM standard. All-Ukrainian scientific and practical conference: Current problems of security of information and telecommunication systems. Kyiv, November 3, 2024, Kyiv: RVC DUICT. – 024. P.90 - 91. https://duikt.edu.ua/uploads/p_2661_93669247.pdf

CRYPTOALGORITHM, MOBILE SYSTEMS SECURITY, GSM, AES, CRYPTOALGORITHM STABILITY, AUDIO SIGNAL PROCESSING, PUBLIC KEY

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ……..……..7
ВСТУП……..…….……8
1 РАДІОСИГНАЛИ GSM У СТІЛЬНИКОВИХ МЕРЕЖАХ.....……..…..9
1.1 Особливості розповсюдження радіосигналів у стільникових мережах зв'язку……..…9
1.2 Стільниковий телефон як об'єкт інформаційної безпеки…….……..…13
1.3 Шляхи захисту інформації у каналах стільникового зв'язку…….……16
2 ЗАХИСТ GSM СИГНАЛІВ……20
2.1 Напрями захисту GSM сигналів…..…….…….……..…20
2.2 Мобільні мережі другого покоління…….……..…22
2.3 Інформаційна безпека мереж другого покоління……..…..……28
2.4 Загальний огляд стандарту GSM……29
2.5 Інформаційна безпека стандарту GSM……..……34
3 ОГЛЯД АЛГОРИТМІВ ШИФРУВАННЯ СИГНАЛУ СТАНДАРТУ GSM.37
3.1 Типові алгоритми шифрування даних……..……37
3.2 Алгоритм шифрування AES ……...…..…..38
3.3 Алгоритм шифрування TwoFish……..…..49
4 РОЗРОБКА ДОДАТКУ ДЛЯ ШИФРУВАННЯ АЛГОРИТМОМ AES…..…60
ВИСНОВКИ……..……71
ПЕРЕЛІК ПОСИЛАНЬ……..……74

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

GSM	-	Global System for Mobile Communications
BS	-	Базова станція
NMT	-	Nordic Mobile Telephony
MS	-	рухливастанція.
MTX	-	Mobile Telephone eXchange
D-AMPS	-	цифрова система стільникового зв'язку другого покоління (2G), відома також під абревіатурою IS-54
ETSI	-	незалежна, некомерційна організація зі стандартизації в телекомунікаційній промисловості
AuC	-	AuthenticationCenter
EIR	-	EquipmentIdentityRegister
VLR	-	VisitorLocationRegister

ВСТУП

Актуальність дослідження. З широким розповсюдженням мобільних пристроїв стає актуальним захист циркулюючої у них інформації. Сучасні засоби мобільного зв'язку дають людині більше можливостей для обміну інформацією. Але разом з цим вони також можуть стати небезпечним інструментом для несанкціонованого отримання інформації сторонніми особами.

Виходячи з цього тема роботи є актуальною.

Об'єкт дослідження – Процес захисту інформації у мережах мобільних операторів.

Предмет дослідження – Захист інформації стандарту GSM.

Мета роботи – Підвищення захищеності інформаціїї в мережах стандарту GSM шляхом використання криптоалгоритму AES.

Наукові завдання:

- проаналізувати особливості сигналів стандарту GSM;
- провести огляд існуючих методів захисту інформації у мобільних стандартах;
- проаналізувати алгоритми шифрування сигналів стандарту GSM.

Методи дослідження – системний аналіз, чисельні методи.

Практичне значення одержаних результатів полягає у розробці алгоритму шифрування сигналів стандарту GSM для підвищення ефективності захисту інформації.

1 РАДІОСИГНАЛИ GSM У СТІЛЬНИКОВИХ МЕРЕЖАХ

1.1 Особливості розповсюдження радіосигналів у стільникових мережах зв'язку

Однією з проблем у вивченні поширення радіохвиль складається є опис процесу ослаблення потужності сигналу при віддалені приймального абонента від передавача.

Найбільш важливим є випадок, коли антена базової станції піднята досить високо над містом, а рухливий об'єкт, з яким здійснюється зв'язок, розташований поблизу поверхні землі.

Просторовий розподіл напруженості поля у міських умовах у поверхні землі відрізняється крайньою нерегулярністю. Сигнали, що передаються між центральною станцією і рухомим пунктом, схильні до глибоких завмирань, причому сусідні максимуми розташовані на відстанях порядку довжини несучої хвилі. Великі затінення, створювані будівлями, практично виключають можливість прямого проходження сигналу, тому його загасання значно більше, ніж в вільному просторі [1].

В даний час існує цілий ряд математичних моделей, що дають можливість розрахувати в міських умовах усереднене значення ослаблення радіосигналу в залежності від різних параметрів, що характеризують конкретні умови. Створені на сьогоднішній день моделі розрахунку зони покриття у радіомережах відрізняються за складністю (за кількістю чинників, які вонивраховують) і умовно діляться на три групи:

- статистичні,
- детерміновані,
- комбіновані.

Детерміновані і комбіновані моделі не отримали широкого застосування так як не можуть врахувати абсолютно всі фактори, що впливаютьна сигнал, а розра-

хунки виявляються занадто складними. хоча статистичні моделі не позбавлені недоліків (однорідність структури моделі, низькаточність, необхідність використовувати моделі не по-окремо, а кілька моделей в комплексі при великому розкиді значень змінних), вони найбільш активно використовуються для проведення розрахунків в силу простоти розрахунків.

На поширення радіохвиль на ділянках довжиною менше 1 км впливають будівлі і дерева, а не зміни відміток висоти. При цьому переважає вплив будівель, оскільки більшість радіоліній ближньоїзв'язку знаходяться в міських і приміських зонах [2]. Даний діапазон поширення радіохвиль особливо актуальний і до нині, зважаючи на високу щільность розміщення БС через значний трафік.

Використовувані в радіозв'язку дециметрові радіохвилі не огинають перешкоди, тобто поширюються в основному по прямій (рис. 1,1 верхня картинка), але відчувають численні відображення від навколишніх об'єктів і підстильної поверхні. Це пояснюється тим, що розмір першої зони Френеля залежить від довжини електромагнітної хвилі. Чим менша довжина хвилі – менше розмір першої зони і тим чутливіша вона буде до різних перешкод.

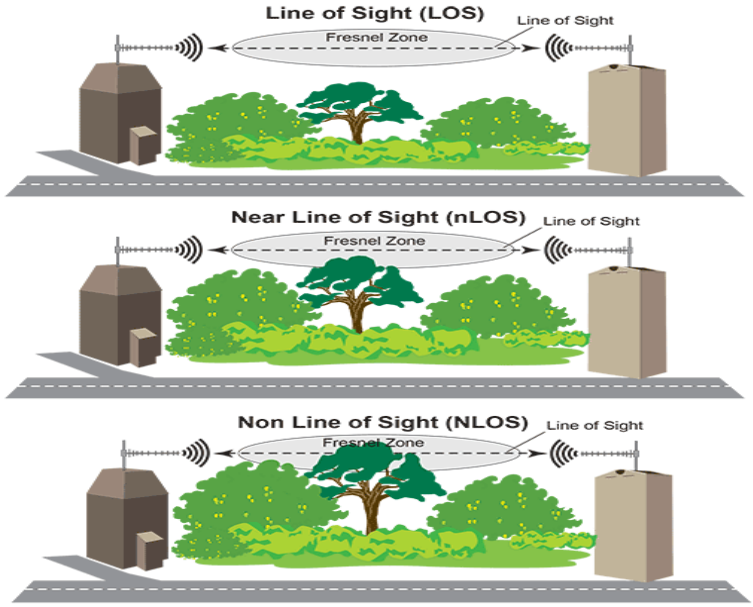


Рис. 1.1 Розповсюдження дециметрових хвиль

Умовою надійного радіозв’язку між двома абонентами є безперешкодне розповсюдження першої зони Френеля між ними ,оскільки основна енергія хвилі знаходиться у першій зоні Френеля.

Одним із наслідків багатопроменевого поширення є більш швидке, ніж у вільному просторі, спадання інтенсивності сигналу з відстанню. Інший наслідок -завмирання і спотворення результуючого сигналу.Область істотних відображень обмежується зазвичай порівняноневеликою ділянкою в околиці мобільної станції - близько кількохсотень довжин хвиль, тобто порядку декількох десятків або сотень метрів. При русі рухомий станції ця область переміщається разом з нею таким чином, що рухома станція весь час залишається поблизу центру області.

Навіть найменше, саме повільне переміщення призводить до зміни у часі умов багатопроменевого поширення і, як наслідок, до зміни параметрів сигналу. Поширення радіохвиль в подібних умовах характеризується трьома,частково самостійними ефектами:

- завмирання через багатопроменевого характеру поширення,
- затінення (або екранування),
- втрати при поширенні.

При складанні двох сигналів, що пройшли різними шляхами і мають різні фази, результуючий сигнал може бути як трохи вище середнього рівня, так і помітно нижче. Типова модель сухопутної системи рухомого радіозв'язку або лініїпередачі стільникового системи, включає в себе високо підняту антену базової станції і відносно короткий ділянки поширення по лінії прямої видимості (LOS). Присутні також безліч трас з перевідбиттям (тобто непрямий видимості - NLOS).

У більшості випадків має місце неповна ділянка поширення радіохвиль в межах прямої видимості між антеною базової станції, або точкою доступу, і антенами рухомих радіостанцій через природні і штучні перешкоди. При таких умовах траса радіопередачі, або радіолінія, може моделюватися як випадковим чином змінюющаяся траса поширення.

Для практичних розрахунків необхідно врахувати електричну неоднорідність тропосфери. Електрична неоднорідність тропосфери, що виявляється в рефракції радіохвиль, впливаєна всі параметри, від яких залежить поле в освітленій зоні. В межах суттєвої області для відображення поверхню землідосить рівна і плоска, модуль коефіцієнта відображення ≈1 ікоефіцієнт розходження ≈1.

Якщо розглядати великі відстані інтерференційна структура поля перестає існувати і величина поля зменшується пропорційно квадрату відстані. Чим більше відстань, тим повніша взаємна компенсація прямий і відбитої хвилі, що і викликає порівняно швидке убування поля. Поверхня землі ніколи не буває ідеально гладкою, навіть рівнинна місцевість вкрита великою кількістю хаотично розташованих нерівностей. Залежно від їх розмірів, електричних властивостей, кількості, а також від довжини хвилі, що розповсюджується, елементи рельєфу роблять різний вплив на поле в точці прийому.

Великі елементи рельєфу місцевості у вигляді, наприклад, гір або долин, пагорбів і ярів, будівель різноманітних за розмірами, формою і розташування на трасі, нерівності земної поверхні, істотно впливають на умови поширення хвилі. Чим менше довжина хвилі, тим цей вплив виражається більш різко. Затінення точки прийому перешкодою призводить, як правило, до значного ослаблення сигналу. Однак, в деяких випадках, як показують експерименти, напруженість в точці прийому може в кілька раз перевищувати значення напруженості поля за відсутності перешкоди.

Цей ефект називають ефектом посилення за рахунок перешкоди. при вдалому збігу обставин, Напруженість поля за перешкодою може перевищувати значення поля у вільному просторі. Якщо врахувати, що в реальності напруженість поля в точці прийому зазвичай менше напруженості поля у вільному просторі, то виграш в посиленні за рахунок перешкоди попорівняно з полем в його відсутність виходить ще більше і може досягати десятків дБ. Умови прийому сигналів в діапазоні 1880-1900 МГц істотно залежать від розташування прийомної антени щодо оточуючих її предметів.

Близько розташовані будівлі можуть, залежно від їх розташування, опинитися затінючими перешкодами або джерелами місцевих відбитих хвиль. Затінюча дію окремої перешкоди призводить до того, що поле за перешкодою з'являється в результаті двох процесів: дифракції та проникнення через перешкоди (дифракція в розглянутому діапазоні хвиль протікає з дуже великими втратами). проникнення через перешкоду типу стін будівель також супроводжується великими втратами за рахунок поглинання. Вимірювання показують, що напруженість поля за окремовартим цегляним будинком на 20-30 дБ нижче, ніж перед ним, а за залізобетонним будовою рівень сигналу падає на 30-40 дБ. В цілому всередині міської забудови є численні тіньові зони, де сигнал значно ослаблений. На поле в точці прийому впливають не тільки розглянуті чинники, а й багато інших. Зокрема, встановлено, що рівень сигналу істотнозалежить від розташування вулиць в місті. Уздовж радіально розташованих вулиць щодо базової станції, рівень сигналу на 10-20 дБ вище, ніж в перпендикулярних напрямках [1].

1.2 Стільниковий телефон як об'єкт інформаційної безпеки

Способів несанкціонованого доступу до інформації дуже багато, але найчастіше їх організація та технічне оснащення досить дорогі і складні. Крім того, більшість засобів знімання інформації неможливо придбати легально. Але в той же час у нас у всіх є доступ до дешевого, мініатюрного, високоякісного підслуховувального радіопристрою, здатному, по-перше, передавати акустичну інформацію на яку завгодно велику відстань.

По-друге, цей пристрій може бути видалено і негласно активований без будь-якої індикації, без відома власника («недекларіровані» можливості, про які не повідомляє виробник), навіть у вимкненому стані. Це пристрій - стільниковий телефон – мініатюрний радіопристрій, здатний передавати акустичну інформацію на будь-яку відстань по каналах стільникового зв'язку. В цьому випадку телефон переводиться в режим передачі з ініціативи його власника [2].

Також мобільний телефон використовується як засіб зв'язку, для виходу в ынтернет та для зберігання особистих даних, до яких належать повідомлення, фотографії, відео, дані банківських карток і рахунків та багато іншого. Шахраї, розуміючи все це, застосовують різні заходи для отримання персональних даних власника телефону, щоб досягти своєї головної мети - заволодіти його грошима.

Майже всі смартфони працюють на двох операційних системах Google Android та Apple iOS. Якщо iOS міститься лише у телефонах фірми Apple, то Android можливо абсолютно скрізь. Тому головний плюс iOS - вона не запускає програми які не схвалюються Apple.

Виділяють два основні рівні захисту смартфона [3]:

- фізичний захист. Сюди входять базові правила догляду мобільного телефону. Наприклад, не варто залишати його без нагляду, вводити код доступу на очах інших людей або банально носити смартфон в кишені. Адже хтось може «зламати» ваш девайс і використовувати його у власних інтересах, наприклад, спустошити рахунки, прив'язані до смартфону, отримати бажані дані або видалити потрібну вам інформацію. У гіршому випадку телефон буде вкрадено.

- захист «начинки» - операційної системи, додатків та інших програм. Існує безліч способів захисту смартфона на внутрішньому рівні. Найголовнішими з них, безперечно, є своєчасне оновлення операційної системи, використання багатофакторної аутентифікації та складних паролів.

Активувати блокування екрану

Встановіть PIN-код довжиною щонайменше 6 символів.

Не вмикайте мінімальний PIN-код із 4 символів, тому що його занадто легко вгадати та подивитися через плече. Якщо пристрій не має PIN-коду, що містить не менше 6 символів, перейдіть до наступного кроку, а краще змініть смартфон.

Біометрія.

Сьогодні сучасні смартфони мають форму сканера відбитків пальців і навіть сканера сітківки. Біометричні сканери краще, ніж ПІН-код або пароль, тому що

вони дозволяють дійсно кожному мати хорошу безпеку, хоча з моєї точки хороший ПІН-код все ж таки надійніше.

Встановіть антивірусну программу.

Ця порада насамперед відноситься до користувачів Android. Вам потрібна антивірусна програма, щоб ви були впевнені, що маєте мінімальний захист. Немає абсолютно ніякого виправдання, щоб не встановлювати антивірусний продукт, оскільки всі відомі виробники засобів забезпечення безпеки мають не тільки платну версію. А якщо хочете серйозно поставитися до цього питання, зверніть увагу на рейтинги таких відомих тестових сайтів, як AV-Test, AV Comparatives.

Використати шифрування.

Всі сучасні смартфони поставляються з можливістю шифрування телефону та SD-картки. Шифрування потрібне для того, щоб хтось не дивився ваші дані, якщо ваш телефон вкрадений, а картка прочитана в іншому телефоні.

Активація видаленних функцій, такі як «блокування» та «стирання».

«Блокування» призначене для того, щоб ніхто не міг використовувати ваш пристрій, якщо ви його втратите. очищення, щоб видалити особисті дані з пристрою.

Увімкнути автоматичне резервне копіювання.

Мобільні пристрої можуть бути вкрадені або втрачені (а потім ви їх «заблокуєте» та «видаєте» з них дані) або можуть бути пошкоджені. У таких випадках краще зберігати всі ваші дані (налаштування, облікові записи, документи, зображення) у безпечному місці, звідки ви можете відновити їх у будь-який час у їхньому початковому місці.

Не встановлюйте незрозумілі програми.

Не встановлюйте програми з магазинів програм, яким ви не довіряєте. Не вмикайте інсталяцію програм із SD-картки або інших закордонних магазинів.

Будьте підозрілі, якщо программа вимогає дозволи, які їй не потрібні.

Веб-загрози.

Навіть якщо ви знаходитесь на мобільному пристрої, ваші дані так само вразливі, як і на будь-якому іншому пристрої.

За замовчуванням майже всі браузери блокують спливаючі вікна, а також мають антифішингові веб-фільтри.

1.3 Шляхи захисту інформації у каналах стільникового зв'язку

Способи захисту інформації від витоку по каналах стільникового зв'язку наступні (рис. 1.2). Організаційно-режимні заходи, які повинні забезпечити вилучення стільникових телефонів. Тобто запобігають (або забороняють) спробу вносити стільникові телефони на об'єкт, що захищається, але ефективність таких заходів низька.

Проконтролювати виконання організаційно-режимних заходів складно через те, що стільниковий телефон має невеликі розміри і може бути закамуфльований практично під будь-який предмет побуту.

Технічні методи і засоби [4]:

- пасивне блокування сигналів стільникового зв'язку (екранування приміщень);
- акустичне зашумлення тракту передачі мовної інформації при спробі негласної дистанційнійактивації мікрофону трубки стільникового телефону.

Рис. 1.2 Рекомендації АНБ США по захисту інформації на смартфонах

Серед пасивних засобів захисту інформації від витоку по каналах стільникового зв'язку на першому місці стоять індикатори електромагнітного випромінювання і екранування приміщень. Акустичніпристрої захисту стільникових телефонів від негласної дистанційної активізації Строго кажучи, акустичні пристрої захисту стільникових телефонів від негласної дистанційної активізації (НДВ) призначені для захисту мовної інформації, що циркулює в місцях перебування власника стільникового телефону, в разі його негласної дистанційної активізації – зметою прослуховування через канал стільникового зв'язку. При цьому єдиною демаскуючою ознакою є зміна напруженості електромагнітного поля (передавач стільникового телефону несанкціоновано включається на передачу). Ця зміна фіксується індикатором електромагнітного поля, що входять до складу пристрою, який дає команду наавтоматичне включення акустичного Шумогенератора, розташованого усередині виробу в безпосередній близькості від мікрофона стільникового телефону.

Принцип роботи наступний. Трубка стільникового телефону розиіщується у внутрішній обсяг футляра або в стакан. У разі негласної дистанційної активації телефону в режим прослуховування єдиною демаскуючою є зміна напруженості електромагнітного поля (передавач стільникового телефону несанкціоновано включається на передачу). Ця зміна фіксується індикатором поля, що входить до складу пристрою, який дає команду на автоматичне включення акустичного шумогенератора, розташованого усередині виробу ізашумлює весь тракт передачі мовної інформації таким чином, що на приймальному кінці відсутні будь-які ознаки мови. У всіх описаних пристроях реалізований автоматичний контроль розрядки батареї. Ознакою розряду батарей є переривчастий звуковий сигнал частотою 2 кГц з періодом повторення 0,6 с, чутний на тлі шуму. Для доступу до елементів живлення відкрутити два гвинти в днище пристрою, вийняти електронний блок, потім витягти елементи живлення і замінити новими [5].

Індикатори електромагнітного випромінювання - вони сигналізують про перевищення рівня електромагнітного поля при переході стільникового телефону в

режим передачі (розмови). Але якщо вприміщенні знаходиться велика кількість людей, то визначити, хто конкретно ведепередачу,проблематично.

Екранування приміщень.

На стіни виставляються спеціальні екрануючі електромагнітні панелі з тонкими пластинами з нікель-цинкового сплаву, або можливо «фанерне» рішення: деревна маса замішується з нікель-цинковим ферритом і у вигляді начинки поміщається міждвома тонкими дерев'яними пластинами. Це надійний спосіб для окремо взятого приміщення, завдяки йому блокується випромінювання радіохвиль. Це є найбільш ефективним способом запобігання витоку мовної інформації по каналах стільникового зв'язку в даний час є застосування блокаторів (або заглушувачів)стільникових телефонів, які реалізуються на основі постановки різного роду електромагнітних завад.

Інструменти для злому і перехоплення GSM сигналів [6].

Ще в 2010 році булла зламана 64 бітна система криптозахисту A5/1 для захисту телефонних переговорів від прослуховування, перехоплення і розшифровки інших даних протоколу GSM. Було продемонстровано як за допомогою ключів і приймача налаштованого на GSM частоту 900 і 1800 мГц можна прослухати розмову по стільниковому телефону, а також отримати SMS та іншу службову інформацію. До недавнього часу у мережі не було точних інструкцій для повторення подібних комплексів для GSM перехоплення і прослуховування.

Складність перехоплення протоколу GSM полягала в наступному:

- райдужні таблиці (що застосовувались для перехоплення) займають обсяг близько 2 терабайт, не кожен зможе дозволити собі завантажити їх;
- безкоштовний доступ до таблиць був відкритий лише на деякий час. Дата центри блокували сервера з райдужними таблицями, вважаючи їх незаконними;
- обладнання, а саме приймач для прийому GSM сигналу на частотах 900 і 1800 мГц дістати складно, а якщо і можна, то за велику ціну.

- немає ніяких інструкцій з налаштування програмних модулів для перехоплення GSM і прослуховування розмов.

Висновок по розділу.

Встановлено, що стільникові станції для своєї роботи використовують частоту 1800 МГц. На розповсюдження таких ел. магнітних хвиль негативно впливають природні та штучні навколишні об’єкти.

Мобільний телефон є засобом несанкціонованого отримання інформації, оскільки виробник не задекоровує у вільний доступ усі можливості приладу.

Для захисту інформації у мережах GSM доцільно використовувати організаційні, технічні активні та пасивні засоби та заходи.

2 ЗАХИСТ GSM СИГНАЛІВ

2.1 Напрями захисту GSM сигналів

Серед програмних засобів захисту від прослуховування через мобільний пристрій відмітимо прооограму GSM SAFE.

GSM SAFE – по іншому це акустичний сейф, призначений для захисту від прослуховування через мобільні пристрої. Автоматичне спрацьовування GSM SAFE відбувається під час несанкціонованої віддаленої активації мобільного пристрою зв'язку. Він починає генерувати шуми в чутному діапазоні акустичних частот, що маскують мову.

Це робить неможливим прослуховування і запис розмови, а на самому пристрої виникне слабкий шум приладу і мерехтіння світлодіода. Звичайні дзвінки будуть проходити у штатному режимі. Прихований дзвінок буде відразу детектуватися у трубці і сторонній особі буде чутний лише шумовий сигнал.

Далі відмітимо програмний засіб GSM CASE.

Програма GSM CASE представляє собою акустичний кейс, що захищає від прослуховування через мобільний телефон шляхом його дистанційної активації. Принцип дії виробу – активація вбудованого генератора шуму детектором GSM-випромінювання. Як тільки телефон активується – вмикається генератор шуму, і телефон більше не може «підслуховувати». Легкий шум вказує на активацію телефону. Штатні дзвінки проходять у звичайному режимі, а при вийманні телефону з виробу генератор автоматично вимикається.

Наступний програмний засіб - GSM-Box.

Індикатор активації мобільних засобів зв'язку GSM-Box усуває можливість несанкціонованого доступу до мобільних засобів зв'язку.

Також існують контрольовані протоколи: GSM 900/1800, Wi-Fi, Bluetooth. GSMBOX - це, в першу чергу, відображаючий пристрій, який дозволяє визначити

несанкціоновану активність мобільного телефону, а також Bluetooth-обмін. У момент появи радіохвиль пристрій включить шумовий сигнал і засвітиться індикатор. Чутний шум при відсутності вхідного дзвінка або SMS свідчить про те, що відбувається якийсь обмін з базовою станцією. Якщо телефон розташувати мікрофоном у напрямку до динаміка GSM-Box, шум, що генерується пристроєм, глушить мікрофон, і прослуховування простору навколо телефону буде неможливим.

Для забезпечення конфіденційності телефонних розмов, що здійснюються незахищеним GSM каналом, використовуються системи безпеки на основі шифрування даних.

Принцип дії більшості пристроїв для захисту передачі даних і голосу засновано на додатковому шифруванні даних. Одним з таких засобів є скремблери.

Перевагою скремблерів є висока надійність захисту від будь-якого засобу прослуховування стільникових телефонів, у тому числі і від спеціального обладнання, встановленого у оператора. Недоліком є необхідність усім абонентам мати сумісні пристрої для приватної бесіди. Криптофони - це звичайні смартфони з додатковим програмним забезпеченням. Першими такі пристрої розробила німецька компанія Cryptophone, звідки і їх назва. Принцип дії криптофонів, як і скремблерів, полягає у наступному: сигнали з мікрофону оцифровуються, кодуються і відправляються в мережу стільникового зв'язку в зашифрованому вигляді. Вся різниця між криптофонами і скремблерами полягає у способі 2 реалізації цієї методики. Головною перевагою криптофона є використання двох алгоритмів шифрування AES і Twofish з ключами довжиною 256 біт, розподіленими за системою Діффі-Хелмана (з власним ключем завдовжки 4096 біт). Також існують криптографічні картки SECUSMART, які встановлюються у телефон і перетворюють його у повноцінний криптофон.

Перше покоління технології Мобільна телефонія – це група аналогових стандартів передавання, реалізована на початку 80-х років XX століття. Ідея створення системи радіозв'язку з'явилася вже в 40-вих роках XX століття в лабораторіях Bell Telephone Company у США. Перші комерційні мобільні системи

зв’язку появилися у 80-тих роках. Було опрацьовано кілька несумісних один з одним аналогових систем. Однак найбільше значення відіграло два з них:

– скандинавський NMT (Nordic Mobile Telephone System) система використовується, наприклад, у країнах ПівнічноїЄвропи, Східної Європи та Росії;

– розроблена у Сполучених Штатах, AMPS (Advanced Mobile Phone System,) в Європі відома як TACS (Total Access Communications System).

Використання аналогової технології спричинило ряд недоліків, таких як низький рівень безпеки, обмежені дані, відсутність міжнародного роумінгу. Найбільший розвиток телефонії першого покоління відбувався у 90-х роках XX- століття у Фінляндії та Швеції, де щільність абонентів становила приблизно 5%. В інших країнах, щільність не перевищувала2%.

2.2 Мобільні мережі другого покоління

Розроблений у США аналоговий стандарт Advanced Mobile Phone System (AMPS) отримав такого широкого поширення, що пряма заміна його цифровим виявилася практично неможливою. Вихід був знайдений у розробці дворежимної аналого-цифрової системи, що дозволяє поєднувати роботу аналогової і цифрової системи в одному і тому ж діапазоні. Такий новий стандарт отримав найменування D-AMPS, або IS-54 (IS - скорочення від Interim Standard, тобто «проміжний стандарт»).

Його практичне застосування почалося в 1993 році. У Європі ситуація ускладнювалася наявністю безліччю несумісних аналогових систем. Тут виходом виявилася розробка єдиного загальноєвропейського стандарту GSM (GSM 900 – робоча частота 900 МГц).

Стандарт D-AMPS додатково удосконалився за рахунок введення нового типу каналів управління [7]. Справа в тому, що цифрова версія IS-54 зберегла структуру каналів управління аналогового AMPS, що обмежувало можливості системи. Нові чисто цифрові канали управління введені у версії IS-136, яка була розроблена

в 1994 році і почала застосовуватися в 1996 році. При цьому була збережена сумісність з AMPS і IS-54, але підвищена ємкість каналу керування і помітно розширені функціональні можливості системи. Стандарт GSM, продовжуючи удосконалюватися технічно (послідовно вводяться фази 1, 2 і 2 +), в 1989 році пішов на освоєння нового частотного діапазону 1800 МГц. Це напрям відомий під назвою системи персонального зв'язку.

Відмінність останньої від вихідної системи GSM 900 не стільки технічна, скільки маркетингова за технічної підтримки: ширша робоча смуга частот у поєднанні з меншими розмірами сот дозволяє будувати стільникові мережі значно більшої місткості, і саме розрахунок на масову систему мобільного зв'язку з відносно компактними, легкими, зручними і недорогими абонентськими терміналами був закладений в основу цієї системи.

Відповідний стандарт (у вигляді доповнень до вихідного стандарту GSM 900) був розроблений в Європі в 1990-1991 роках. Система отримала назву DCS 1800 (Digital Cellular System - цифрова система стільникового зв'язку; спочатку використовувалася також назва PCN – Personal Communications Network, що в буквальному перекладі означає «мережа персональної зв'язку») і почала використовуватися з 1993 році. У 1996 році було прийнято рішення іменувати її GSM 1800.

У США діапазон 1800 МГц виявився зайнятий іншими користувачами, але була знайдена можливість виділити смугу частот у діапазоні 1900 МГц, яка отримала в Америці ім'я діапазону систем персонального зв'язку (PCS – Personal Communications Systems), на відміну від діапазону 800 МГц, за яким збережено назву стільникового.

Освоєння діапазону 1900 МГц почалося з кінця 1995 р.; робота в цьому діапазоні передбачена стандартом D-AMPS (версія IS-136, але аналогового AMPS в діапазоні 1900 МГц вже немає), і розроблена відповідна версія стандарту GSM («американський» GSM 1900 - стандарт IS-661).

Стандврт Digital Advanced Mobile Phone System (D-AMPS) - цифрова система стільникового зв'язку другого покоління, відома також під абревіатурою IS-54. Цей стандарт набув найбільшого поширення в Північній Америці, переважно в США та Канаді.

Принцип роботи.

Виклик мобільної станції (вхідне з'єднання).

Процедура встановлення вхідного виклику в системах стандарту AMPS виконується наступним чином. Якщо в центр комутації мобільного зв'язку надходить заявка на встановлення зв'язку з рухомим абонентом від абонента телефонної мережі загального користування або іншого рухомого абонента, тобто заявка на вхідний дзвінок, то він проводовим каналом передавання даних дає команду всім базовим станціям, що знаходяться в зоні обслуговування, викликати необхідного рухомого абонента. Цей виклик каналом управління транслюється на рухому станцію, яка, отримавши його, перевіряє можливість доступу в зворотний канал керування з допомогою прапора "вільно / зайнято", наявного в прийнятому повідомленні. Якщо зворотний канал керування вільний, то абонентська станція видає в центр комутації мобільного зв'язку MSC через базову підтверджуюче повідомлення, яке містить особистий номер рухомого абонента.

Центр комутації, прийнявши це повідомлення, аналізує інформацію, що надійшла, визначає номер базової станції, яка обслуговує в даний момент часу абонента, і, тим самим, визначає його місце розташування. Потім він вибирає вільний розмовний канал на даній базовій станції BTS і займає його, вказуючи в інформаційній частині каналу керування, що цей канал "зайнятий". Процедура вхідного виклику відбувається протягом 1 - 4 мс, що зовсім не помітно для користувача. Реалізація такої процедури дозволяє знизити до мінімуму ймовірність конфліктної ситуації при занятті каналу керування декількома абонентами одночасно.

Після виконання процедури встановлення вільного каналу зв'язку і його заняття з центру комутації по розмовному каналу посилається повторний виклик на базову станцію з вказівкою номера виділеного радіоканалу і номера спеціального

позасмугового сигналу SAT (Supervisory Audio Tone). Як якості сигналу SAT в одній клітинці системи стільникового зв'язку може використовуватися сигнал однієї з трьох тональних частот: 5970, 6000 або 6030 Гц, який необхідний для контролю за виконанням команд і якістю зв'язку в розмовному каналі. Даний сигнал виходить за рамки стандартного каналу тональної частоти (300 - 3100 Гц), пригнічується фільтрами абонентських станцій і тому його не чути.

Отримавши інформацію від центру комутації, абонентська станція перестроюється на частоту вільного розмовного каналу і по ньому ретранслює виділений сигнал SAT. При його розпізнаванні на базовій станції приймається рішення про готовність дуплексного радіоканалу "базова станція - абонент", про що повідомляється в центр комутації відповідним сигналом.

Далі виробляється комутація наземної телефонної лінії між центром MSC і базовою станцією радіоканалу - між станцією BTS і мобільною станцією MS, яка відповідною командою приводиться в готовність.

Якщо абонент вільний, то від нього по призначеному розмовному каналу на базову станцію передається тональний сигнал ST (SignallingTone) частотою 8 кГц, який переривається при знятті трубки абонентського апарата. По сигналу ST базова станція повідомляє в центр комутації про готовність абонентського термінала, і центр MSC посилає абоненту сигнал виклику (дзвінок).

При перериванні сигналу ST центр комутації підключає весь розмовний тракт, передає в канал сигнал SAT і стежить за результатами контролю якості зв'язку. По завершенні розмови від абонентського терміналу передається сигнал ST і сигнал про перебудову на частоту каналу управління, тому базова станція повідомляє в центр комутації мобільного зв'язку про закінчення сеансу зв'язку, після чого комутаційне обладнання звільняється.

Сигнал SAT постійно передається в каналі зв'язку під час розмови. У тому випадку, якщо виявлено переривання цього сигналу, абонентська станція включає таймер і, якщо сигнал SAT не буде виявлений після закінчення певного часу, перемикається на частоту каналу керування. На цьому сеанс зв'язку закінчується.

Слід зазначити, що на відміну від алгоритму вхідного дзвінка системи NMT у даному алгоритмі контроль достовірності прийнятих повідомлень частково перенесений на блок управління абонентської станції. Наприклад, з його допомогою визначається відповідність між прийнятим номером розмовного каналу і номером каналу управління, який обслуговує дану групу розмовних каналів.

Виклик з рухомий станції (вихідні повідомлення).

Вихідний від рухомого абонента виклик може бути призначений як для абонента телефонної мережі загального користування, так і для іншого рухомого абонента системи стільникового зв'язку. Для створення вихідного виклику користувач набирає на радіотелефоні номер абонента; цей номер передається на базову станцію і далі транслюється в центр комутації по каналу передавання даних. Після аналізу інформації і виділення вільного розмовного каналу в діючих системах стільникового зв'язку організовується тестування стану каналів, встановлюється з'єднання і в бік абонента надсилається виклик. При відповіді абонента підключається весь розмовний тракт.

У системах стільникового зв'язку стандарту AMPS управління при вихідному виклику засновано на застосуванні сигналів SAT і ST. Як і в системі стандарту NMT, номер абонента записується в запам'ятовуючий пристрій абонентської станції, яка потім перевіряє стан зворотного каналу керування на зайнятість, тобто визначає можливість доступу в прямий канал управління.

Отримавши доступ, абонентська станція передає вихідний виклик, в якому містяться номери абонентів якого викликають і який викликає. Базова станція транслює вихідне повідомлення по каналу передавання даних в центр комутації, де здійснюється перевірка на несанкціонований доступ абонента до даної мережі. Якщо абонент має право доступу, то центр комутації ініціює протягом 1 - 4 мс стан зворотного каналу керування як "зайнято", виділяє вільний розмовний канал і передає сигнал SAT. Одночасно з цим встановлюється з'єднання з абонентом і йому передається виклик. Отримавши номери розмовного каналу і сигналу SAT, станція

яка викликає налаштовується на частоту розмовного каналу і передає по ньому через базову станцію в центр комутації мобільного зв'язку відповідний сигнал SAT, після отримання якого здійснюється перевірка розмовного тракту MSC - BTS-MS. Далі центр комутації очікує відповіді абонента, що викликається і, при знятті ним трубки, підключає розмовний тракт і веде контроль за якістю мови. Обмін повідомленнями в режимі "естафетного передавання" (хендовер)

Однією з основних проблем при розробці систем стільникового зв'язку є забезпечення безперервного зв'язку під час пересування абонента по зоні обслуговування. Для її вирішення використовується принцип естафетного передавання.

У системах стандарту AMPS протокол обміну повідомленнями подібний протоколу системи стандарту NMT і відрізняється лише тим, що контроль за якістю передавання ведеться за допомогою сигналу SAT. В процесі естафетної передавання абонента від однієї базової станції до іншої апаратура рухомого абонента повідомляється про номер сигналу SAT спеціальним повідомленням.

При наближенні рухомої станції до межі осередку значення відношення сигнал/шум зменшується. Тому базова станція BTS1 може видати в центр комутації сигнал "погіршення якості", за яким центр комутації ідентифікує шести найближчих до абонента базових станцій і дає їм команду виміряти рівень сигналу SAT 1 в даному радіоканалі. Центр комутації порівнює отримані результати і вибирає нову комірку з більш високим рівнем сигналу, наприклад, клітинку 2, в базову станцію якій передається номер нового розмовного каналу і номер SAT2. Це повідомлення транслюється на рухому станцію в розмовному каналі, по якому ведеться сеанс зв'язку. Підтвердженням отримання інформації є короткочасне (на 50 мс) переривання сигналу SAT2, зафіксувавши яке, BTS1 посилає сигнал виконання на центр комутації. У новому розмовному каналі абонентський термінал передає в центр комутації сигнал готовності. Останній робить відповідну перекомутацію каналів, звільняючи базову станцію BTS1, і підключає новий розмовний тракт. Контроль за якістю передавання ведеться за сигналом SAT2, дискретна інформація передається

в розмовному каналі методом бланкування, при якому мовні сигнали перериваються. Вся процедура естафетної передавання займає близько 250 мс, тому для абонента момент перемикання непомітний.

2.3 Інформаційна безпека мобільних мереж другого покоління

До стандарту D-AMPS війшли нові алгоритми: аутентифікації – CAVE (Cellular Authentication, Voice Privacyand Encryption) і шифрування – CMEA (Cellular Message Encryption Algorithm). На відміну від AMPS у цьому стандарті застосовується інтерлівінг для подолання швидких завмирань.

Алгоритми аутентифікації:

Для захисту від несанкціонованого доступу в системах AMPS і D-AMPS використовується система аутентифікації A-KEY [8]. Власне A-KEY представляє собою 8-байтове число-ключ, яке зберігається в стільниковому телефоні абонента і є унікальним для кожного абонента. A-KEY вводиться при продажі телефону клієнта і зберігається в базі. A-KEY 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 A-KEY (постійний ключ) за допомогою хеш-функції CAVE (Cellular Authenticationand Voice Encryption), що використовує в якості вхідних параметрів AKEY, ESN, MIN телефону, а також випадкове число, прислане по ефіру від базової станції, генерується часової ключ, званий SSD_A (теж 8 байт). Цей ключ надалі і використовується при аутентифікації для генерації відповідного значення. Постійна A-KEY не використовується при аутентифікації і служить тільки для розрахунку тимчасового ключа. При встановлення 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 - AuthenticationCenter, який, в свою чергу, незалежно від телефону генерує відповідь

число (всі параметри телефону, у тому числі і A-KEY, 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. 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 A-KEY, 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.

2.4 Загальний огляд стандарту GSM

GSM (від *Groupe Spécial Mobile*, пізніше перейменована в Global Systemfor Mobile Communications) – глобальний цифровий стандарт для мобільного сотового зв’язку, з розділенням частотного каналу по принципуTDMA і середним ступінем безпеки. Розроблений під керівництвом Європейського інституту телекомунікаційних стандартів в кінці 80-х років. ETSI були успішно стандартизовані система стільникового зв'язку GSM і система професійного мобільного радіозв'язку TETRA,стандарт радіотелефонів DECT.

ETSI був створений CEPT в 1988 році і був офіційно визнаний Європейською Комісією і секретаріатом EFTA. ETSI офіційно відповідальний за стандартизацію інформаційних і телекомунікаційних технологій в межах Європи.

GSM відноситься до мережі другого покоління (2 Generation), хоч на 2010 рік він умовно знаходиться в фазі 2,75 G завдяки багаторазовим розширенням. Сотові телефони випускаються для чотирьох діапазонів частот: 850 МГц, 900 МГЦ, 1800МГц, 1900 МГц.

В залежності від кількості діапазонів, телефони поділяються на класи і варіацію частот в залежності від регіону використання.

Однодіапазонні – телефон може працювати на одній з частот. В наш час не випускаються, але є можливість ручного виборучастоти в деяких моделях телефонів, наприкладMotorola C115, або з допомогою інженерного меню телефона.

Дводіапазонні (Dual Band) – для Європи, Азії, Африки, Австралії 900/1800 і 850/1900 для Америки і Канади.

Тридіапазонні (Tri Band) – для Європи, Азії, Африки, Австралії 900/1800/1900 і 850/1800/1900 для Америки і Канади.

Чотирьох діапазонні (Quad Band) – підтримують всі діапазони 850/900/1800/1900.

В стандарті GSM застосовується GMSK – модуляція з величиною нормованої полоси ВТ – 0,3, де В – ширина полоси фільтра по рівню мінус 3 дБ, Т – тривалість одного біта цифрового повідомлення. GSM на сьогоднішній день являється найбільш поширеним стандартом зв’язку. По даних асоціації GSM (GSMA) на даний стандарт приходитися 82 % світового ринку мобільного зв’язку, 29 % населення земноїкулівикористовують глобальні технології GSM. В GSMA в теперішній час входять операторибільше ніж 210 країн і територій.

Відповідно до рекомендації CEPT 1980 р., що стосується використання спектра частот рухомого зв'язку в діапазоні частот 862-960 Мгц, стандарт GSM на цифрову загальноєвропейську (глобальну) стільникову систему наземного рухомого зв'язку передбачає роботу передавачів у двох діапазонах частот: 890-915 Мгц (для передавачів рухомих станцій - MS), 935-960 Мгц (для передавачів базових станцій – BTS. У стандарті GSM використовується вузько смуговий багатостанційний доступ з часовим поділом каналів (NS TBMA). У структурі TDMA кадру міститься 8 часових позицій на кожній з 124 несучих.Для захисту від помилок у радіоканалах при передавання інформаційних повідомлень застосовується блокове і згортальне кодування з перемежовуванням. Підвищення ефективності кодування з перемежо-

ваннями при малій швидкості переміщення рухомих станцій досягається повільним переключенням робочих частот (SFH) у процесі сеансу зв'язку зі швидкістю 217 стрибків у секунду.

У стандарті GSM обрана гаусова частотна маніпуляція з мінімальним частотним зсувом (GMSK) [9]. Опрацювання мови здійснюється в рамках прийнятої системи переривчастої передавання мови (DTX), що забезпечує включення передавача тільки при наявності мовного сигналу і відключення передавача в паузах і наприкінці розмови[9]. В якості мовно-перетворюючого пристрою обрано мовний кодек з регулярним імпульсним збудженням, довгостроковим пророкуванням і лінійним предикативним кодуванням із пророкуванням (RPE/LTR-LTP-кодек). Загальна швидкість перетворення мови - 13 кбіт/с. У стандарті GSM досягається високий ступінь безпеки передавання повідомлень; здійснюється шифрування повідомлень по алгоритму шифрування з відкритим ключем (RSA). В цілому система зв'язку, що діє в стандарті GSM, розрахована на її використання в різних сферах. Вона надає користувачам широкий діапазон послуг і можливість застосовувати різноманітне устаткування для передаваннямовних повідомлень і даних, викличних і аварійних сигналів; підключатися до телефонних мереж загального користування (PSTN), мережам передавання даних (PDN) і цифровим мережам з інтеграцією служб (ISDN).

Основні характеристики:

- частоти передавання рухомої станції і прийому базової станції, МГц 890-915;
- частоти приймання рухомої станції і передавання базової станції, МГц 935-960;
- дуплексний рознесення частот приймання і передавання, МГц 45;
- швидкість передавання повідомлень у радіоканалі, кбіт/с 270, 833;
- швидкість перетворення мовногокодека, кбіт/с 13;
- ширина смуги каналу зв'язку, кГц 200;
- максимальна кількість каналів зв'язку 124;

- максимальна кількість каналів, що організовані в базовій станції 16-20;
- вид модуляції GMSK;
- індекс модуляції BT 0,3;
- ширина смуги передмодуляційногогаусового фільтра, кГц 81,2;
- кількість стрибків по частоті в секунду 217;
- вид мовногокодека RPE/LP;
- максимальний радіус стільника, км до 35.

Функціональна побудова та інтерфейси, прийняті в стандарті GSM, ілюструються структурною схемою на (рис. 2.1). Найпростіша частина структурної схеми - переносний телефон, складається з двох частин: самої "трубки" - ME (Mobile Equipment – мобільне обладнання) і смарт-картки SIM (Subscriber Identity Module - модуль ідентифікації абонента), яку отримують при заключенні контракту з оператором [10]. Сотовий телефон має особистий номер - IMEI (International Mobile EquipmentIdentity – міжнародний ідентифікатор мобільного устаткування), який може передаватись по мережі. SIM, в свою чергу, вміщає так званий IMSI (International Mobile Subscriber Identity–міжнародний ідентифікаційний номер підписувача). Отже – IMEI відповідає конкретному телефону, а IMSI - відповідає абоненту.

"Центральною нервовою системою " мережі являється NSS (Network and Switching Subsystem – підсистема мережі і комутації), а компонент, виконуючий функції "мозку" називається MSC (Mobileservices Switching Center - центр комутації). Якраз останній всі називають "комутатор". MSC в мережі може бути і не один (в даному випадку досить влучна аналогія з багатопроцесорними комп’ютерними системами) - наприклад,московський оператор Білайн ввів другий комутатор (виробництва Alcatel). MSC займається маршрутизацією викликів, формуванням даних для білінгової системи, управляє багатьма процедурами і багато інше.

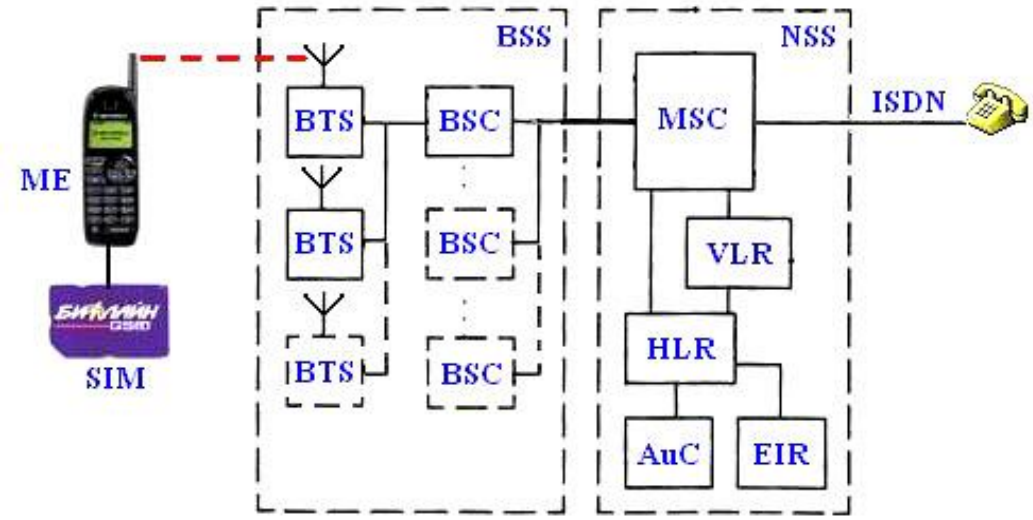


Рис. 2.1 Структурна схема стандарту GSM

Наступними по важливості компонентами мережі, які також входять в NSS є HLR (Home Location Register - реєстр особистих абонентів) і VLR (Visitor Location Register - реєстр переміщення). HLR, грубо кажучи, представляє собою базу даних про всіх абонентів, що заключили з мережею контракт. В ній зберігається інформація про номери користувачів (під номером розуміється, по-перше IMSI, а по-друге, так званий MSISDN – Mobile Subscriber ISDN, телефонний номер в його звичайному розумінні), доступні послуги і багато інше.

На відміну від HLR, який в системі один, VLR`і в може бути декілька-кожен з них контролює свою частину мережі. В VLR зберігаються дані про абонентів, які знаходяться на його території. Як тільки користувач покидає зону дії якого-небудь VLR, інформація про нього копіюється в новий VLR, а зі старого видаляється. Фактично між тим, що є про абонента в VLR і в HLR, дуже багато спільного.

Принципова відмінність HLR від VLR є така що в першому знаходиться інформація про всіх в мережі, незалежно від їх місця знаходження, а в другому – дані тільки про тих, хто знаходиться на відомому цьому VLR території. В HLR для кожного абонента постійно присутня ссилка на цей VLR, який з ним (абонентом) на даний час співпрацює (при цьому сам VLR може належати чужій мережі).

NSS містить ще два компоненти - AuC (AuthenticationCenter - центр авторизації) і EIR (Equipment Identity Register - реєстр ідентифікації обладнання). Перший блок використовується для процедур встановлення авторизації абонента, а другий, відповідає за допуск до експлуатації в мережі тільки тих сотових телефонів яким дозволено. Виконуючою частиною сотової мережі, являється BSS (Base Station Subsystem – підсистема базових станцій). Якщо продовжувати аналогію з людським організмом, то цю підсистему можна назвати кінцівками тіла. BSS складається з кількох "рук" і "ніг" - BSC (BaseStationController - контролер базових станцій), а також багатьох "пальців" - BTS (BaseTransceiverStation - базова станція). Базові станції можна спостерігати всюди ,фактично це просто приємно-передавальне обладнання, яке вміщає від одного до 16 випромінювачів. Кожен BSC контролює цілу групу BTSi відповідає за управління і розділення каналів, рівнів сили базових станцій і тому подібне. BSC в мережі не один, а ціла множина (базових станцій взагалі сотні).

2.5 Інформаційна безпека стандарту GSM

Сотові системи зв’язку першого покоління, такі як NMT, TACS і AMPS, мали невеликі можливості в плані безпеки, і це призвело до суттєвого рівня шахрайської діяльності, яка шкодить і абонентам і мережевим операторам. Безліч інцидентів великого значення висунуло на перший план чутливість аналогових телефонів до підслуховування ліній радіозв'язку. Система 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 місце знаходження користувача для того хто підслуховує.

Мережі третього покоління 3G працюють на частотах дециметрового діапазону (близько 2 ГГц), швидкість передавання даних становить понад 2 Мбіт/с. Такі мережі надають можливість організувати відеозв'язок, дивитись на мобільному телефоні фільми й телепрограмми та ін. В світі існує два стандарти 3G: UMTS (чи W-CDMA) та CDMA-2000. UMTS більш розповсюджений в основному в Європі, CDMA2000 – в Азії та США. За даними Wireless Intelligence, на кінець 2006 року в світі нараховувалось 364 млн. абонентів 3G, з них 93,5 млн були підключені до мереж UMTS та 271,1 млн. – до CDMA2000. Найбільший оператор – японський NTT DoCoMo (40 млн абонентів).

Вирішення цієї проблеми (сумісність стандартів та глобальний роумінг) абсолютно аналогічне сьогоднішньому – розробка багатомодових терміналів, що можуть працювати в двох і більше стандартах.

Термін 3G використовується для опису сервісів мобільного зв’язку стандартів наступного покоління, які забезпечуються більш високу якість звуку, а також високошвидкісний інтернет-звязок та мультимедійні сервіси [11]. Мобільні мережі третього покоління (3G) відрізняються від мереж другого покоління (2G), таких як наприклад цифровий стандарт мобільного звязку GSM, зв'язок перехідного покоління (2.5G) GRPS набагато більшою швидкістю передавання даних, а також більш широким набором і високою якістю послуг, що надаються.

В грудні 2006 компанія ЗАТ «Телесистеми України» оголосив про запуск з січня 2007 року мережі 3G під торговою маркою «PEOPLEnet» стандарту CDMA2000 1xEV-DO (800 мГц) rev0. В 2008 році поступово переходить на EV-DO revA , в цьому стандарті також працюють Інтертелеком, який з квітня 2008 році перейшов

на CDMA2000 EV-DO revA (800 мГц), CDMA UKRAINE (з 2007 року CDMA2000 EV-DO rev0, а з 2008 року - RevA) (800 мГц), та МТС Україна з липня 2007 CDMA2000 EV-DO revA (450 мГц).

1 листопада 2007 державне підприємство Укртелеком запускає мережу мобільного звязку 3G під брендом «Utel». Мережа «Utel» працює в стандарті UMTS 2100 з надбудовою HSDPA (3,5G). Якщо в базовій версії UMTS забезпечує пікові швидкості від 2-х мегабіт за секунду для статичних об'єктів поблизу соти, та 384 Кб/с для мобільних абонентів, то для пристроїв, що підтримують HSDPA швидкості в теорії можуть досягати 14,4 Мбіт/с. На практиці ж, реальні швидкості рідко перевищують 3 мегабіти, а в умовах високих, щільних забудов та завантаженості мережі, ще менше.

3 ОГЛЯД АЛГОРИТМІВ ШИФРУВАННЯ СИГНАЛУ СТАНДАРТУ GSM

3.1 Типові алгоритми шифрування даних

Сучасна криптографія для забезпечення конфіденційного передавання інформації передбачає можливість використання значного розмаїття симетричних алгоритмів шифрування. До типових симетричних алгоритмів, призначених для шифрування інформації типу “дані”, можна зарахувати алгоритми DES, 3DES, IDEA, AES, Twofish, Blowfish, CAST-5 (CAST-128) та інші, які можуть бути використані як самостійно, так і у режимах типу ECB, CBC, OFB та CFB.

Типовою областю застосування цих алгоритмів є передавання даних, які є нечутливими або малочутливими до часових затримок. Тому єдиною проблемою, яка виникає під час передавання такого типу інформації, є надійність алгоритму, яка визначається рядом критеріїв: довжиною ключа, кількістю раундів шифрування, довжиною блока даних відкритого тексту та математичною складністю реалізації раунду шифрування.

Але в сучасних телекомунікаційних мережах щораз частіше виникає потреба передавати у захищеному вигляді дані іншого типу, зокрема зашифровані мультимедійні дані в реальному часі. Для передавання таких даних виникає суперечлива задача: з одного боку, необхідно забезпечити високу криптографічну надійність, яка, як правило, досягається за рахунок використання складних математичних операцій алгоритму, а з іншого боку – потрібно досягти високої швидкості передавання, а отже, і незначних часів затримок, які переважно обмежуються швидкістю криптографічних перетворень на сторонах передавання та приймання. Крім того, на аналіз цієї задачі накладається ще одне додаткове обмеження, а саме: криптографічні алгоритми реалізовуються у вигляді програмного або апаратного забезпечення і час затримки на обробку типового інформаційного блока сталий для вибраного алгоритму шифрування, вплинути на який неможливо.

Тому єдиним розв’язанням цієї задачі є підбір алгоритму, режиму роботи та його відповідної реалізації – апаратної або програмної, яка б задовольняла вимоги стосовно конфі- денційної надійності та часових затримок передавання. Також необхідно зауважити, що передавання і приймання мультимедійних даних відбувається, як правило, з використанням персональних комп’ютерів.

3.2 Алгоритм шифрування AES

Вперше AES-шифрування згадується ще в 2000 році, коли на конкурсі вибору наступника системи DES, яка була стандартом у США з 1977 року, переможцем став алгоритм Rijndael [12].

У 2001 році AES-система була офіційно прийнята в якості нового федерального стандарту шифрування даних і з тих пір використовується повсюдно.

Еволюція алгоритмів включала в себе декілька проміжних стадій, які в основному були пов'язані із збільшенням довжини ключа.

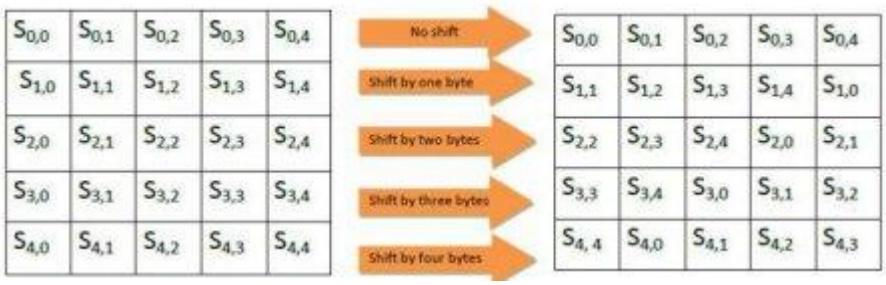
Сьогодні розрізняють три основних типи: AES-128-шифрування, AES-192 і AES-256. Назва говорить сама за себе.

Цифрове позначення відповідає довжині застосовуваного ключа, вираженої в бітах. Крім того, AES-шифрування відноситься до блокового типу, який працює безпосередньо з блоками інформації фіксованої довжини, шифруючи кожен з них, на відміну від потокових алгоритмів, що оперують окремими символами відкритого повідомлення, переводячи їх в зашифрований вид. У AES довжина блоку складає 128 біт. Якщо говорити науковою мовою, ті ж алгоритми, які використовує AES-256 шифрування, розуміють операції на основі полиноминального подання операцій і кодів при обробці двовимірних масивів (матриць).

Алгоритм роботи досить складний, проте включає в себе використання декількох базових елементів. Спочатку застосовується двовимірна матриця, цикли перетворення (раунди) (табл. 3.1), раундовий ключ і таблиці початкової і зворотного підстановки.

Таблиця 3.1

Цикли перетворення двораундових ключів



Процес шифрування даних складається з декількох етапів:

- обчислення всіх раундових ключів;
- підстановка байтів з допомогою основної таблиці S-Box;
- зрушення у формі з використанням розрізняємих величин;
- змішування даних усередині кожного стовпця матриці (форми);
- складання форми і раундового ключа. Дешифрування проводиться в зворотному порядку, але замість таблиці S-Box застосовується таблиця зворотних постановок, яка була згадана вище.

Таблиця 3.2

Кількість можливих комбінацій ключів залежно від його довжини

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^9
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

У табл 3.2 привелено залежність кількісті можливих комбінацій ключів залежно від довжини ключа.

Якщо навести приклад, при наявності ключа довжиною 4 біта для перебору потрібно всього 16 стадій (раундів), тобто необхідно перевірити всі можливі комбінації, починаючи з 0000 і закінчуючи 1111. Природно, такий захист зламується досить швидко. Але якщо взяти ключі побільше, для 16 біт потрібно 65536 стадій, а для 256 біт – 11 x 10 77 . І як було заявлено американськими фахівцями, на вибір правильної комбінації (ключа) піде близько 149 трильйонів років.

Rijndael представляє собою ітеративний блочний шифр, що має змінну довжину блоків і різні довжини ключів. Довжина ключа і довжина блоку можуть бути незалежно один від одного 128, 192 або 256 біт.

Стан, Ключ шифрування і Число Циклів

Різноманітні перетворення працюють з проміжним результатом, називаемим Станом (State).

Визначення: проміжний результат шифрування назвемо Станом (State).

Стан можна представити у вигляді прямокутного масиву байтів. Цей масив має 4 рядки, а число стовпців позначено як Nb і дорівнює довжині блоку, поділеній на 32.

Ключ шифрування також представлений у вигляді прямокутного масиву з чотирма рядками. Число стовпців позначено як Nk і дорівнює довжині ключа, поділеній на 32. Це показано на рис 3.1.

У деяких випадках ключ шифрування показаний як лінійний масив 4-байтових слів. Слова складаються з 4 байтів, які знаходяться в одному стовпці (при поданні у вигляді прямокутного масиву).

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

Рис. 3.1 Приклад подання Стану (Nb = 6) і Ключа шифрування (Nk = 4)

Вхідні дані для шифру ("відкритий текст", якщо використовується режим шифрування ECB) позначаються як байти стану в порядку a0,0, a1,0, a3,0, a0,1, a1,1, a3,1, a4,1. Після завершення дії шифру вихідні дані виходять з байтів стану в тому ж порядку.

Таблиця 3.3

Число циклів (Nr) як функція від довжини ключа і довжини блоку

Nr	Nb = 4	Nb = 6	Nb = 8
Nk = 4	10	12	14
Nk = 6	12	12	14
Nk = 8	14	14	14

Циклове перетворення складається з чотирьох різних перетворень. На мові програмування Сі це виглядає наступним чином:

```
Round (State, RoundKey)
{
ByteSub(State); // заміна байтів
ShiftRow(State); // зсув рядків
MixColumn(State); // замішування стовпців
AddRoundKey(State, RoundKey); // додавання циклового ключа
}
```

Останній цикл шифру трохи відрізняється. Ось як він виглядає:

```
FinalRound(State, RoundKey)
{
ByteSub(State); // заміна байтів
ShiftRow(State); // зсув рядків
AddRoundKey(State, RoundKey); // додавання циклового ключа
}
```

У наведеній записі, "функції" - Round, ByteSub і т.д. виконують свої дії над масивами, покажчики (тобто State, RoundKey) на які їм передаються.

Як можна помітити, останній цикл відрізняється від простого циклу тільки відсутністю замішування стовпців. Кожне з наведених перетворень пояснено далі.

Заміна байтів (ByteSub).

Перетворення ByteSub є нелінійну заміну байт, виконувану незалежно з кожним байтом стану [14]. Таблиці заміни (або S-блоки) є інвертіруемимі і побудовані з композиції двох перетворень:

Перше - отримання зворотного елемента щодо множення в полі GF (28), описаного в розділі 2.1. '00' переходить сам у себе.

Таблиця 3.4

Застосування описаного S-блоку до всіх байтам стану позначено як ByteSub (State). Малюнок 2 ілюструє застосування перетворення ByteSub до стану

y_0		1	1	1	1	1	0	0	0	x_0	+	0
y_1		0	1	1	1	1	1	0	0	x_1		1
y_2		0	0	1	1	1	1	1	0	x_2		1
y_3		0	0	0	1	1	1	1	1	x_3		0
y_4	=	1	0	0	0	1	1	1	1	x_4		0
y_5		1	1	0	0	0	1	1	1	x_5		0
y_6		1	1	1	0	0	0	1	1	x_6		1
y_7		1	1	1	1	0	0	0	1	x_7		1

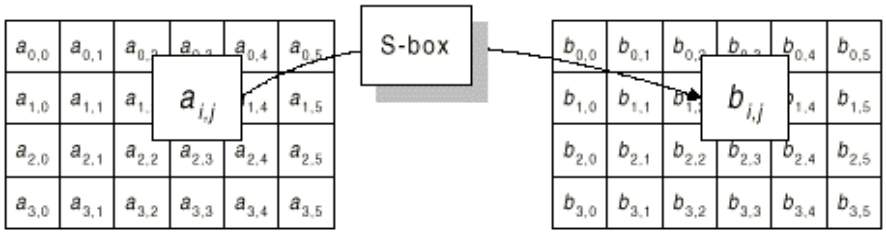


Рис. 3.2 Перетворення зсуву рядків (ShiftRow)

Останні 3 рядки стану циклічно зсуваються на різне число байт. Рядок 1 зсувається на C1 байт, рядок 2 - на C2 байт і рядок 3 - на C3 байт. Значення зрушень C1, C2 і C3 залежать від довжини блоку Nb. Їх величини наведені в таблиці 3.5.

Таблиця 3.5
Величина зсуву для різної довжини блоків

Nb	*C1*	*C2*	*C3*
4	1	2	3
6	1	2	3
8	1	3	4

Операція зсуву останніх 3 рядків стану на певну величину позначена як ShiftRow (State). На рис. 3.3 показано вплив перетворення на стан.

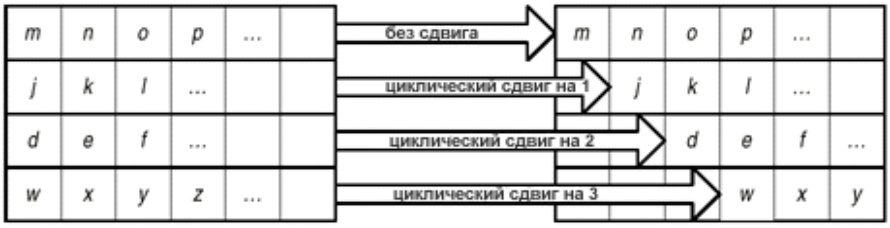


Рис. 3.3 Перетворення замішування стовпців (MixColumn).

У цьому перетворенні стовпці стану розглядаються як многочлени над GF (28) і множаться по модулю x4 + 1 на многочлен c (x), що виглядає в такий спосіб:

$$c(x) = 0{,}3x^3 + 0.1x^2 + 0.1x + 0.2$$

Як описано в розділі 2.2, це може бути представлено у вигляді матричного множення. Нехай b (x) = c (x) a (x),

Таблиця 3.6
Застосування операції (2.1)стовпчиків стану

b0		02	03	01	01	a0
b1		01	02	03	01	a1
b2	=	01	01	02	03	a2
b3		03	01	01	02	a3

Застосування цієї операції до всіх чотирьох стовпчиках стану позначено як MixColumn (State). На (рис 3.4) демонструє застосування MixColumn до стану.

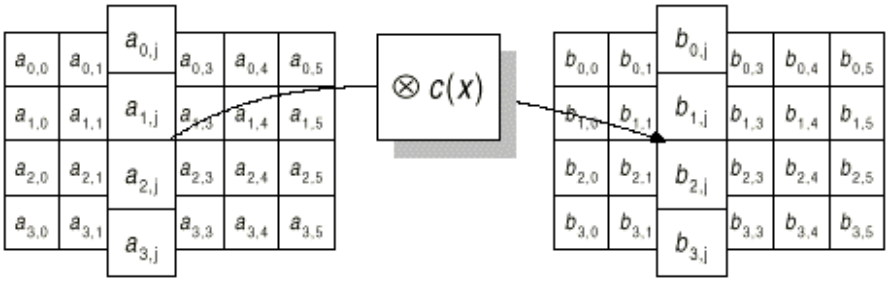


Рис. 3.4 MixColumn діє на стовпці стану.

Додавання циклового ключа

У даній операції циклової ключ додається до стану за допомогою простого EXOR. Циклової ключ виробляється з ключа шифрування за допомогою алгоритму вироблення ключів (key schedule). Довжина циклового ключа дорівнює довжині блоку Nb.

Перетворення, що містить додавання за допомогою EXOR циклового ключа до стану, позначено як AddRoundKey (State, RoundKey). Воно проілюстровано на (рис. 3.7).

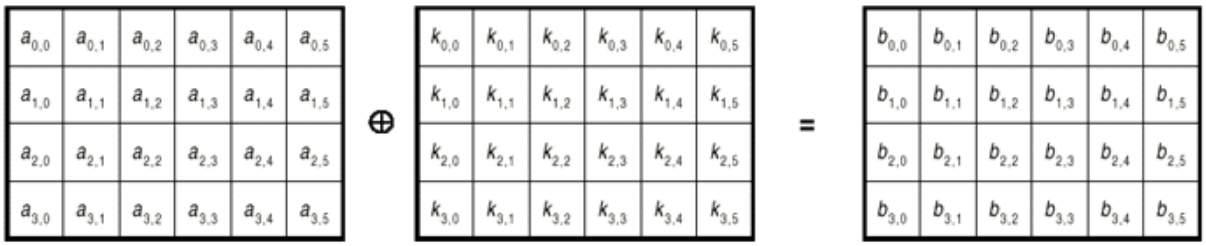


Рис. 3.5 Перетворення що містять додавання за допомогою EXOR

При додаванні ключа циклової ключ складається за допомогою EXOR зі станом.

Алгоритм вироблення ключів (Key Schedule)

Циклові ключі виходять з ключа шифрування за допомогою алгоритму вироблення ключів. Він містить два компоненти: розширення ключа (Key Expansion) і вибір циклового ключа (Round Key Selection). Основоположні принципи алгоритму виглядають наступним чином:

- Загальна кількість біт циклових ключів дорівнює довжині блоку, помноженої на число циклів плюс 1 (наприклад, для довжини блоку 128 біт і 10 циклів потрібно 1 408 біт циклового ключа).
- Ключ шифрування розширюється в Розширений Ключ (ExpandedKey).
- Циклові ключі беруться з Розширеного ключа наступним чином: перший циклової ключ містить перші Nb слів, другий - такі Nb слів і т.д.

Розширення ключа (Key Expansion) (рис. 3.8).

Розширений ключ являє собою лінійний масив 4-ох байтових слів і позначений какW [Nb * (Nr + 1)]. Перші Nk слів містять ключ шифрування. Всі інші слова визначаються рекурсивно з слів з меншими індексами. Алгоритм вироблення ключів залежить від величини Nk: нижче приведена версія для Nk рівного або меншого 6 і версія для Nk більшого 6.

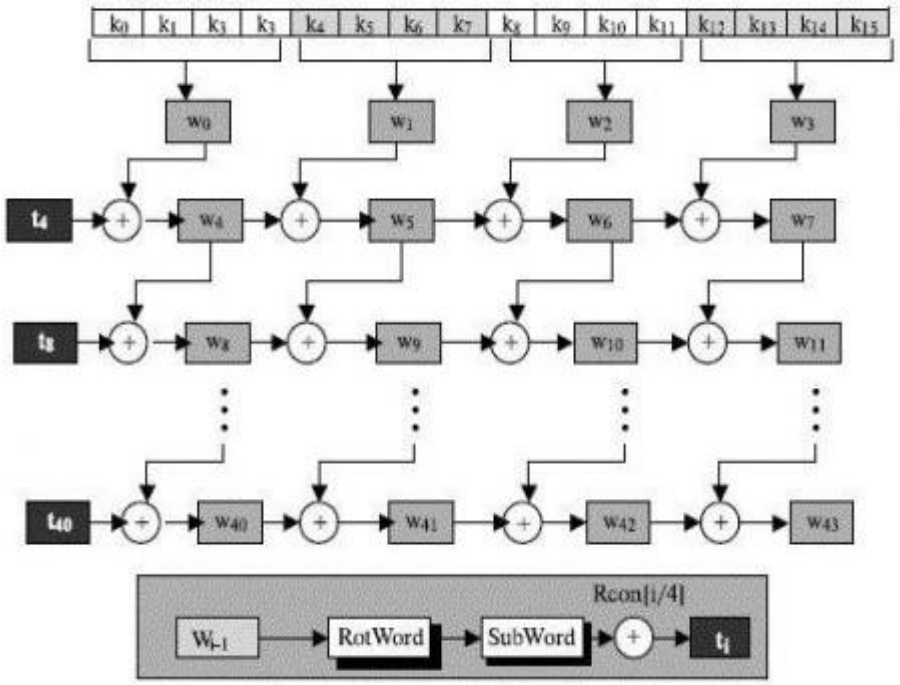


Рис. 3.8 Розширення ключа

Для *Nk*<6 или *Nk*=6 маемо:

```
KeyExpansion(CipherKey,W)
{
for (i = 0;  i < Nk;  i++) W[i] = CipherKey[i];
for (j = Nk;   j < Nb*(Nk+1);   j+=Nk)
   {
   [j] = W[j-Nk] ^ SubByte( Rotl( W[j-1] ) ) ^ Rcon[j/Nk];
   for (i = 1;   i < Nk   &&  i+j < Nb*(Nr+1);   i++)

W[i+j] = W[i+j-Nk] ^ W[i+j-1];}
}
```

Як можна помітити, перші Nk слів заповнюються ключем шифрування. Кожне наступне слово W [i] виходить за допомогою EXOR попереднього слова W [i-1] і слова на Nk позицій ранееW [i-Nk]. Для слів, позиція яких кратна Nk, перед

EXOR застосовується перетворення до W [i-1], а потім ще додається цикловая константа. Перетворення містить циклічний зсув байтів в слові, позначений як Rotl, потім слід SubByte - застосування заміни байт.

Для *Nk*>6 маємо:

```
KeyExpansion(CipherKey,W)
{
for (i=0; i<Nk; i++) W[i]=CipherKey[i];
for (j=Nk; j<Nb*(Nk+1); j+=Nk)
   {
   W[j] = W[j-Nk] ^ SubByte(Rotl(W[j-1])) ^ Rcon[j/Nk];
   for (i=1; i<4; i++)   W[i+j] = W[i+j-Nk] ^ W[i+j-1];
   W[j+4] = W[j+4-Nk] ^ SubByte(W[j+3]);
   for (i=5; i<Nk; i++) W[i+j] = W[i+j-Nk] ^ W[i+j-1];
   }
}
```

Відмінність для схеми при Nk> 6 полягає в застосуванні SubByte для кожного 4-го байта з Nk.

Циклова константа незалежний від Nk і визначається наступним чином:
Rcon[i] = (RC[i], '00' , '00' , '00'), где

RC[0]='01'

RC[i]=xtime(Rcon[i-1])

Вибір циклового ключа.
і-ий циклової ключ виходить з слів масиву циклового ключа від W [Nb * i] і доW [Nb (i + 1)]. Це показано на (рис. 3.6).

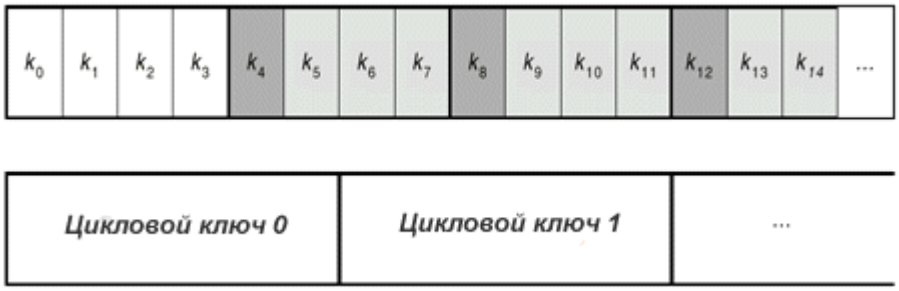


Рис. 3.6 Розширення ключа і вибір циклового ключа для Nb = 6 і Nk = 4

Зауваження: Алгоритм вироблення ключів можна здійснювати і без використання массівaW [Nb * (Nr + 1)]. Для реалізацій, в яких істотно вимога до займаної пам'яті, циклові ключі можуть обчислюватися на льоту за допомогою використання буфера з Nk слів.

Шифр.

Шифр Rijndael складається з:

- Початкового додавання циклового ключа;
- Nr-1 циклів;
- заключного циклу.

На мові Сі це виглядає наступним чином:

```
Rijndael (State, CipherKey)
{
KeyExpansion(CipherKey, ExpandedKey); // Расширение ключа
AddRoundKey(State, ExpandedKey);  // Добавление циклового ключа
For ( i=1 ; i<Nr ; i++) Round(State,ExpandedKey+Nb*i); // циклы

FinalRound(State, ExpandedKey+Nb*Nr); // заключительный цикл
}
```

Якщо попередньо виконана процедура розширення ключа, то Rijndael буде виглядати наступним чином:

```
Rijndael (State, CipherKey)
{
AddRoundKey(State, ExpandedKey);
For ( i=1 ; i<Nr ; i++) Round(State,ExpandedKey+Nb*i);
FinalRound(State, ExpandedKey+Nb*Nr);
}
```

Зауваження: Розширений ключ повинен завжди виходити з ключа шифрування і ніколи не вказується прямо. Немає ніяких обмежень на вибір ключа шифрування.

3.3 Алгоритм шифрування TwoFish

Алгоритм Twofish - симетричний алгоритм блочного шифрування з розміром блоку 128 біт і довжиною ключа до 256 біт (рис. 3.10). Число раундів 16. Розроблено групою фахівців на чолі з Брюсом Шнайером. Був одним з п'яти фіналістів другого етапу конкурсу AES. Алгоритм розроблений на основі алгоритмів Blowfish, SAFER і Square. Відмінними рисами алгоритму є використання попередньо обчислюваних і залежних від ключа S-box'ов і складна схема розгортки підключей шифрування. Половина n-бітного ключа шифрування використовується як власне ключ шифрування, інша - для модифікації алгоритму (від неї залежать S-box'и) [15].

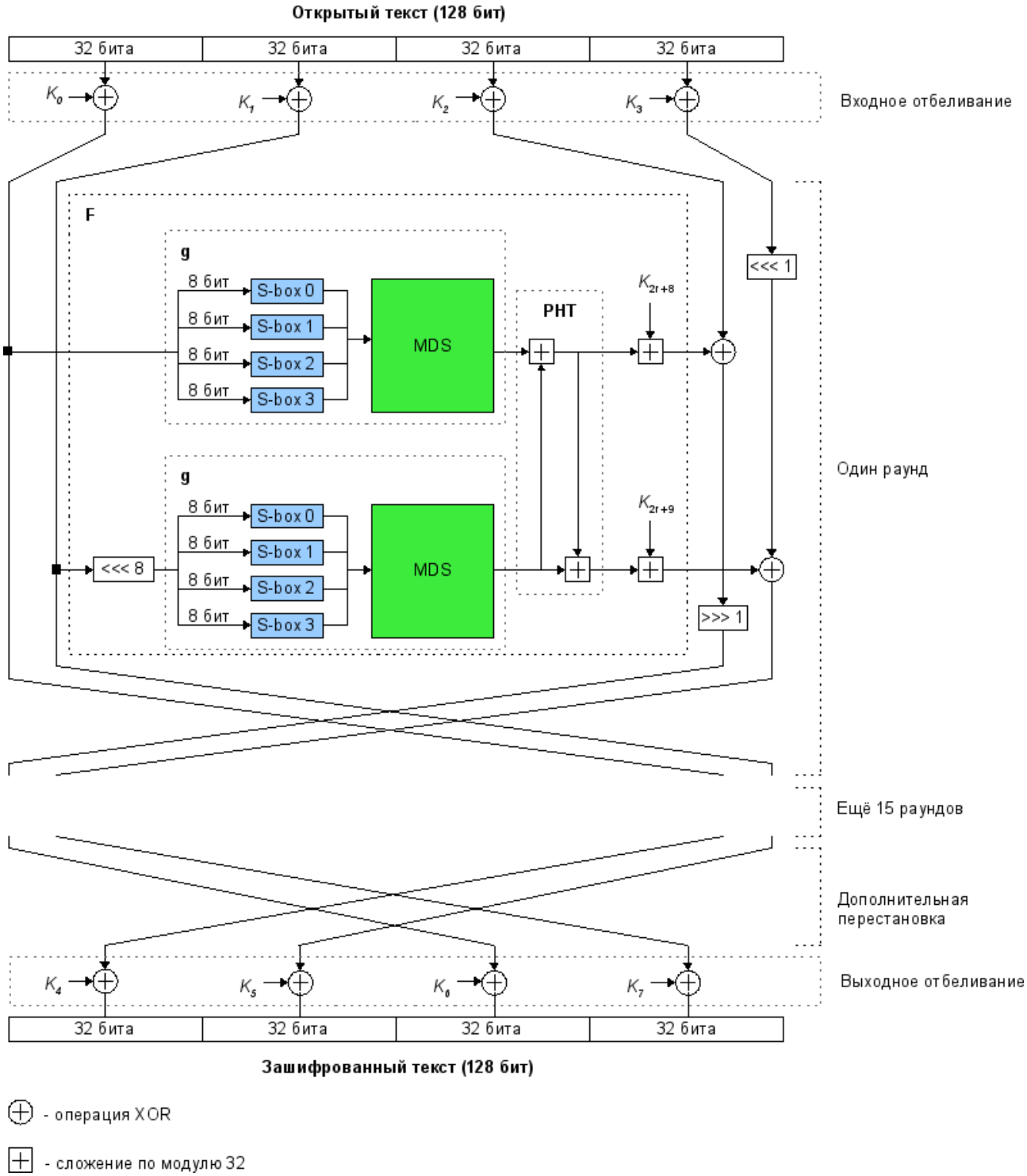


Рис. 3.7 Структура алгоритму TwoFish

Параметри алгоритму.

Розмір ключа: 256.

Розмір блоку: 128.

Число раундів: 16.

Twofish розроблявся спеціально з урахуванням вимог і рекомендацій NIST для AES [16]:

- 128-бітний блоковий симетричний шифр;
- Довжина ключів 128, 192 і 256 біт;
- Відсутність слабких ключів;
- Ефективна програмна (в першу чергу на 32-бітних процесорах) і апаратна реалізація;
- Гнучкість (можливість використання додаткових довжин ключа, використання в потоковому шифруванні, хеш-функціях і т. д.);
- Простота алгоритму - для можливості його ефективного аналізу.

Однак саме складність структури алгоритму і, відповідно, складність його аналізу на предмет слабких ключів або прихованих зв'язків, а також досить повільне час виконання в порівнянні з Rijndael на більшості платформ, зіграло не на його користь.

Алгоритм Twofish виник в результаті спроби модифікувати алгоритм Blowfish для 128-бітового вхідного блоку. Новий алгоритм повинен був бути легко реалізованим апаратно (в тому числі використовувати таблиці меншого розміру), мати більш досконалу систему розширення ключа (key schedule) і мати однозначну функцію F.В результаті, алгоритм був реалізований у вигляді змішаної мережі Фейстеля з чотирма гілками, які модифікують один одного з використанням криптоперетворень Адамара (Pseudo-Hadamar Transform, PHT).

Можливість ефективної реалізації на сучасних (для того часу) 32-бітних процесорах (а також в смарт-картах і подібні пристрої) - один з ключових принципів, яким керувалися розробники Twofish. Наприклад, у функції F при обчисленні PHT і складання з частиною ключа K навмисно використовується додавання, замість традиційного xor. Це дає можливість використовувати команду LEA сімейства процесорів Pentium, яка за один такт дозволяє обчислити перетворення Адамара (Правда в такому випадку код доводиться компілювати під конкретне значення ключа).Алгоритм Twofish не запатентований і може бути використаний будь-ким

без будь-якої плати або відрахувань. Він використовується в багатьох програмах шифрування, хоча і отримав менше поширення, ніж Blowfish.

Опис алгоритму.

Twofish розбиває вхідний 128-бітний блок даних на чотири 32-бітних подблока, над якими, після процедури вхідного відбілювання (input whitening), проводиться 16 раундів перетворень. Після останнього раунду виконується вихідне відбілювання (output whitening).

Відбілювання (whitening)

$$(T_0 + 2T_1 + K_{2r+9}) mod 2^{32}$$

Відбілювання - це процедура xor'a даних з підключенням перед першим раундом і після останнього раунду. Вперше ця техніка була використана в шифрі Khufu / Khare і, незалежно, Рональдом Ривестом (Ron Rivest) в алгоритмі шифрування DESX. Joe Killian (NEC) і Phillip Rogaway (Каліфорнійський університет) показали, що відбілювання дійсно ускладнює завдання пошуку ключа повним перебором (exhaustive key-search) в DESX. Розробники Twofish стверджують, що в Twofish відбілювання також істотно ускладнює завдання підбору ключа, оскільки криптоаналитик не може дізнатися, які дані потрапляють на вхід функції F першого раунду.

Проте, виявилися і негативні сторони. Цікаве дослідження провели фахівці дослідницького центру компанії IBM. Вони виконали реалізацію алгоритму Twofish для типової смарт-карти з CMOS-архітектурою і проаналізували можливість атаки за допомогою диференціального аналізу споживаної потужності (DPA - Differential Power Analysis). Атаці піддавалася саме процедура вхідного відбілювання, оскільки вона безпосередньо використовує xor подключей з вхідними даними. В

Внаслідок дослідники показали, що можна повністю обчислити 128-бітний ключ проаналізувавши всього 100 операцій шифрування довільних блоків.

Функція g - основа алгоритму Twofish. На вхід функції подається 32-бітове число X, яке потім розбивається на чотири байти x0, x1, x2, x3. Кожен з вийшов байтів пропускається через свій S-box. (Слід зазначити, що S-box'и в алгоритмі не фіксовані, а залежать від ключа). Утворені 4 байта на виходах S-box'ов інтерпретуються як вектор з чотирма компонентами. Цей вектор множиться на фіксовану матрицю MDS (maximum distance separable) розміром 4x4, причому обчислення проводяться в поле Галуа GF (28) по модулю неприводимого многочлена x8 + x6 + x5 + x3 + 1

MDS матриця - це така матриця над кінцевим полем K, що якщо взяти її в якості матриці лінійного перетворення f (x) = (MDS) x з простору Kn в простірKm, то будь-які два вектори з простору Kn + m виду (x, f (x)) будуть мати як мінімум m + 1 відмінностей в компонентах. Тобто набір векторів виду (x, f (x)) утворює код, що володіє властивістю максимальної рознесених (maximum distance separable code). Таким кодом, наприклад, є код Ріда-Соломона.

У Twofish властивість максимальної рознесених матриці MDS означає, що загальна кількість мінливих байт вектора a і вектора b = (MDS) a не менш п'яти. Іншими словами, будь-яка зміна тільки одного байта в a призводить до зміни всіх чотирьох байтів в b.

Криптоперетворень Адамара (Pseudo-Hadamar Transform, PHT)

Криптоперетворень Адамара - оборотне перетворення бітової рядки довжиною 2n. Рядок розбивається на дві частини a і b однакової довжини в n біт. Перетворення обчислюється таким чином:

$$a = a + b(mod 2^n) \quad ($$

$$a = a + 2b(mod 2^n) \quad ($$

Ця операція часто використовується для «розсіювання» коду (наприклад в шифрі SAFER).

У Twofish це перетворення використовується при змішуванні результатів двох g-функцій (n = 32).

Циклічний зсув на 1 біт

У кожному раунді два правих 32-бітних блоку, які xor-ятся з результатами функції F, додатково циклічно зсуваються на один біт. Третій блок зсувається до операції xor, четвертий блок - після. Ці зрушення спеціально додані, щоб порушити вирівнювання по байтам, яке властиво S-box'ам і операції множення на MDS-матрицю. Однак шифр перестає бути повністю симетричним, так як при шифрування і розшифровки зрушення слід здійснювати в протилежні сторони.

Генерація ключів.

Twofish розрахований на роботу з ключами довжиною 128, 192 і 256 біт. З вихідного ключа генерується 40 32-бітових подключей, перші вісім з яких використовуються тільки в операціях вхідного і вихідного відбілювання, а решта 32 - в раундах шифрування, по два підключа на раунд. Особливістю Twofish є те, що вихідний ключ використовується також і для зміни самого алгоритму шифрування, так як використовувані в функції g S-box'и не фіксовані, а залежать від ключа.

Для формування раундовий подключей вихідний ключ M розбивається з перестановкою байт на два однакових блоку Mo і Me. Потім за допомогою блоку Mo і функції h шифрується значення 2 * i, а за допомогою блоку Me шифрується значення 2 * i + 1, де i - номер поточного раунду (0 - 15). Отримані зашифровані блоки змішуються криптоперетворень Адамара, і потім використовуються в якості раундових подключей.

Технічні подробиці.

Розглянемо більш докладно алгоритм формування раундовий підключів, а також залежність від ключа функції g (рис. 3.11). Як для формування подключів, так і для формування функції g в Twofish використовується одна основна функція: h (X, L0, L1, ..., Lk). Тут X, L0, L1, ..., Lk - 32 бітні слова, а k = N / 64, де N - довжина вихідного ключа в бітах. Результатом функції є одне 32-бітове слово.

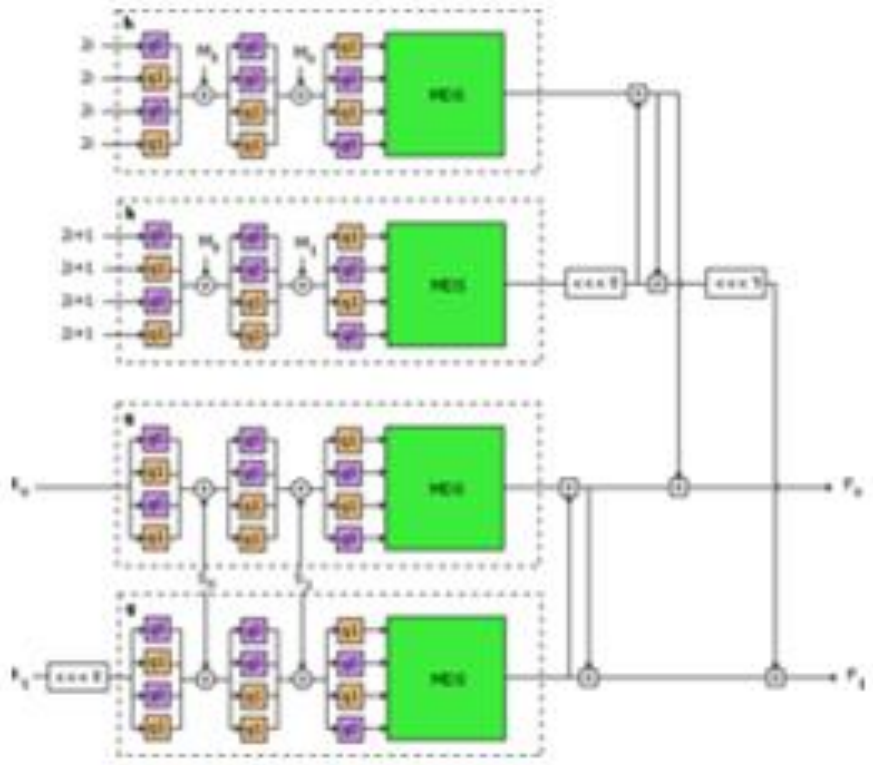


Рис. 3.8 Схема одного раунду шифрування для 128-бітного ключа

Функція h (рис. 3.9).

Функція виконується в k етапів. Тобто для довжини ключа 256 біт буде 4 етапи, для ключа в 192 біта - 3 етапу, для 128 біт - 2 етапи.

На кожному етапі вхідний 32-бітове слово розбивається на 4 байта, і кожен байт піддається фіксованою перестановці бітів q0 або q1.

Результат представляється у вигляді вектора з 4 байтів і множиться на MDS матрицю. Обчислення проводяться в поле Галуа GF (28) по модулю неприводимого многочлена x8 + x6 + x5 + x3 + 1.

Матриця MDS має вигляд:

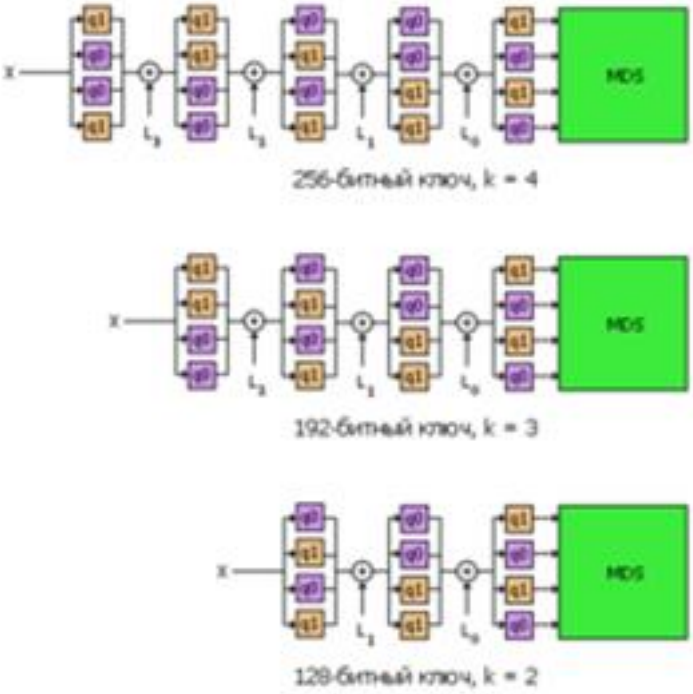


Рис. 3.9 Функція h для різних довжин ключа

Перестановки q0 і q1

q0 і q1 - фіксовані перестановки 8 бітів вхідного байта x.

Байт x розбивається на дві 4-бітові половинки a0 і b0, над якими проводяться наступні перетворення:

$$a_0 = \frac{x}{16} b_0 = x \mathrm{mod} 16$$

$$a_1 = a_0 \oplus b_0 b_1 = a_0 \oplus ROR_4(b_0, 1) \oplus 8a_0 \mathrm{mod} 16$$

$$a_2 = t_0[a_1] b_2 = t_1[b_1]$$

$$a_3 = a_2 \oplus b_2 b_3 = a_2 \oplus ROR_4(b_0, 1) \oplus 8a_2 mod 16$$

$$a_4 = t_2[a_3] b_4 = t_3[b_3]$$

$$y = 16b_4 + a_4$$

де:

ROR4- 4-бітний циклічний зсув вправо, а t0, t1, t2, t3 - табличні заміни 4-бітних чисел.

Для q0 таблиці мають вигляд:

t0 = [8 1 7 D 6 F 3 2 0 B 5 9 E C A 4]

$$t1 = [\ E\ C\ B\ 8\ 1\ 2\ 3\ 5\ F\ 4\ A\ 6\ 7\ 0\ 9\ D\ ]$$

$$t2 = [\ B\ A\ 5\ E\ 6\ D\ 9\ 0\ C\ 8\ F\ 3\ 2\ 4\ 7\ 1\ ]$$

$$t3 = [\ D\ 1\ 7\ D\ 6\ F\ 3\ 2\ 0\ B\ 3\ 0\ 8\ 5\ C\ A\ ]$$

Для q1 таблиці мають вигляд:

$$t0 = [\ 2\ 8\ B\ D\ F\ 7\ 6\ E\ 3\ 1\ 9\ 4\ 0\ A\ C\ 5\ ]$$

$$t1 = [\ 1\ E\ 2\ B\ 4\ C\ 3\ 7\ 6\ D\ A\ 5\ F\ 9\ 0\ 8\ ]$$

$$t2 = [\ 4\ C\ 7\ 5\ 1\ 6\ 9\ A\ 0\ E\ D\ 8\ 2\ B\ 3\ F\ ]$$

$$t3 = [\ B\ 9\ 5\ 1\ C\ 3\ D\ E\ 6\ 4\ 7\ F\ 2\ 0\ 8\ A\ ]$$

Генерація ключів.

Нехай M - вихідний ключ, N - його довжина в бітах. Генерація подключей відбувається наступним чином:

- вихідний ключ розбивається на 8 * k байтів m0, ..., m8k - 1, де k = N / 64;

- ці 8 * k байтів розбиваються на слова по чотири байти, і в кожному слові байти переставляються в зворотному порядку.

У підсумку виходить 2 * k 32-бітних слова Mi:

$$M_i = \sum_{j=0}^{3} m_{(4i+j)} 2^{8j} \qquad i = 0, \ldots\ldots, 2k$$

Отримані 2 * k 32-бітних розбиваються на два вектора Me і M0 розміром в k 32-бітних слів:

$$M_e = (M_0, M_2, \ldots\ldots M_{2k-2})$$

$$M_o = (M_1, M_3, \ldots\ldots, M_{2k-1})$$

Підключи для і-го раунду обчислюються за формулами:

$$p = 2^{24} + 2^{16} + 2^8 + 2^0$$

$$A_i = h(2ip, M_e)$$

$$B_i = ROL(h\big((2i+1)p, M_0\big), 8)$$

$$K_{2i} = (A_i + B_i) mod 2^{32}$$

$$K_{2i+1} = ROL((A_i + 2B_i) mod 2^{32}, 9)$$

Функція g і S-box'и.

Функція g визначається через функцію h:

Вектор S, як і вектора Me і Mo, теж формується з вихідного ключа і складається з k 32-бітних слів. Вихідні байти ключа розбиваються на k груп по вісім байт. Кожна така група розглядається як вектор з 8-ю компонентами і множиться на фіксовану RS матрицю розміром 4x8 байт. В результаті множення виходить вектор, що складається з чотирьох байт. Обчислення проводяться в поле Галуа GF (28) по модулю неприводимого многочлена x8 + x6 + x3 + x2 + 1.

RS-матриця має вигляд:

$$RS = \begin{pmatrix} 01 & A4 & 5587 & 5A & 58DB & 9E \\ A4 & 56 & 82F3 & 1E & C668 & E5 \\ 02 & A1 & FCC1 & 47 & AE3d & 19 \end{pmatrix}$$

Вивчення Twofish зі скороченими числом раундів показало, що алгоритм має великий запас міцності, і, в порівнянні з іншими фіналістами конкурсу AES, він виявився найстійкішим. Однак його незвичайна структура і відносна складність породили деякі сумніви в якості цієї міцності.

Нарікання викликало поділ вихідного ключа на дві половини при формуванні раундовий подключей. Криптографи Fauzan Mirza і Sean Murphy припустили,

що такий поділ дає можливість організувати атаку за принципом «розділяй і володарюй», тобто розбити задачу на дві аналогічні, але більш прості. Однак реально подібну атаку провести не вдалося.

На 2008 рік кращим варіантом криптоанализа Twofish є варіант усіченого диференціального криптоаналізу, який був опублікований Shiho Moriai і Yiqun Lisa Yin в Японії в 2000 році. Вони показали, що для знаходження необхідних диференціалів потрібно 251 підібраних відкритих текстів. Проте дослідження носили теоретичний характер, ніякої реальної атаки проведено не було. У своєму блозі творець Twofish Брюс Шнайер стверджує, що в реальності провести таку атаку неможливо.

4 РОЗРОБКА ДОДАТКУ ДЛЯ ШИФРУВАННЯ ЗА АЛГОРИТМОМ AES

Структура додатку.

Для вирішення даної задачі було вибрано мову програмування Java і середовище розробки Eclipse Neon.

Умовно програму можна розділити на 7 класів:

Клас Aes Encription відповідає безпосередньо за зашифрування сигналу.

Клас Audiorecorder відповідає за захоплення звуку з мікрофону.

Клас CriptoException обробляє можливі помилки при роботі крипто алгоритму і виводить коди помилок.

Клас DecriptionForm відповідає користувацький інтерфейс для процесу розшифрування.

Клас EncriptionForm відповідає за користувацький інтерфейс для процесу за шифрування.

Клас SoundCapture відповідає за обробку захопленого звуку.

Використані технології.

Для розробки користувацького інтерфейсу було використано Java бібліотеку.

Розробка користувацького інтерфейсу.

Swing — інструментарій для створення графічного інтерфейсу користувача (GUI) мовою програмування Java. Це частина бібліотеки базових класів Java (JFC, Java Foundation Classes).

Swing розробляли для забезпечення функціональнішого набору програмних компонентів для створення графічного інтерфейсу користувача, кращого за застарійлий інструментарій AWT. Компоненти Swing підтримують специфічні look-and-feel модулі, що динамічно підключаються. Завдяки ним можлива емуляція графічного інтерфейсу платформи (тобто до компоненту можна динамічно підключити інші, специфічні для даної операційної системи вигляд і поведінку). Основним недоліком таких компонентів є відносно повільна робота, хоча останнім часом це не

вдалося підтвердити через зростання потужності персональних комп'ютерів. Позитивна сторона — універсальність інтерфейсу створених програм на всіх платформах.

На початку існування Java класів Swing не було взагалі. Через слабкі місця в AWT (початковій GUI системи Java) було створено Swing. AWT визначає базовий набір елементів керування, вікон та діалогів, які підтримують придатний до використання, але обмежений у можливостях графічний інтерфейс. Однією з причин обмеженості AWT є те, що AWT перетворює свої візуальні компоненти у відповідні їм еквіваленти, що не залежать від платформи, які називаються рівноправними компонентами. Це означає, що зовнішній вигляд компонентів визначається платформою, а не закладається в Java. Оскільки компоненти AWT використовують «рідні» ресурси коду, вони називаються ваговитими (англ. highweigh).

Використання «рідних» рівноправних компонентів породжує деякі проблеми. По-перше, у зв'язку із різницею, що існує між операційними системами, компонент може виглядати або навіть вести себе по-різному на різноманітних платформах. Така мінливість суперечила філософії Java: «написане один раз, працює скрізь». По-друге, зовнішній вигляд кожного компонента був фіксованим (оскільки усе залежало від платформи), і це неможливо було змінити (принаймні, це важко було зробити). По-третє, використання ваговитих компонентів тягнуло за собою появу нових обмежень. Наприклад, ваговитий компонент завжди має прямокутну форму і є непрозорим [17].

Незабаром після появи початкової версії Java, стало очевидним, що обмеження, властиві AWT, були настільки незручними, що потрібно було знайти кращий підхід. У результаті з'явились класи Swing як частина бібліотеки базових класів Java (JFC). В 1997 році вони були включені до Java 1.1 у вигляді окремої бібліотеки. А починаючи з версії Java 1.2, класи Swing (а також усі останні, що входили до JFC) стали повністю інтегрованимими у Java.

Розробка классів DecriptionForm і EncriptionForm.

Пакет javax.crypto визначає класи і інтерфейси для різних криптографічних операцій. Рисунок 4.1 показує ієрархію класів цього пакета. Центральний клас Cipher, який використовується для шифрування і дешифрування даних. Cipher Input Stream і Cipher Output Stream класи утиліти, які використовують Cipher об'єкт для шифрування і дешифрування потокових даних. Sealed Object ще один важливий клас утиліта, яка використовує Cipher об'єкт для шифрування довільносеріалізованого об'єкту Java.

Ієрархія класів пакету jaxax.crypto.

Клас Key Generator створює об'єкти Secret Key, які використовуються для шифрування і дешифрування. Secret Key Factory кодує і декодує Secret Key об'єкти. Клас KeyAgreement дозволяє двом або більше сторінам домовитися про SecretKey таким чином, що зловмисник не може визначити ключ. Клас Mac обчислює код аутентифікації повідомлення (MAC), який може забезпечити цілісність передачі даних між двома сторонами, які поділяють SecretKey. MAC фактично є цифровим підписом, за винятком того, що він заснований на секретному ключі, а не публічній / приватній парі ключів.

Як пакет java.security, пакет javax.crypto є постачальником, так що довільні криптографічні реалізації можуть бути підключені до будь-якої версії Java. Різні класи в цьому пакеті це посилання, які закінчуються на «Spi». Ці класи визначають інтерфейс сервіс-провайдера і повинні бути реалізовані кожен своїм криптографічним провайдером, який забезпечує реалізацію конкретної криптографічної служби або алгоритму.

Цей пакет є частиною Cryptography Extension (JCE Java). BC розподіляє ОКО в межах Сполучених Штатів і Канади, але, на жаль, правила експорту США N забороняють експорт криптографічних технологій в інші країни. Якщо ви не є резидентом Сполучених Штатів або Канади, ви повинні отримати і використовувати реалізацію третьої сторони ОКО, розроблену за межами Сполучених Штатів.

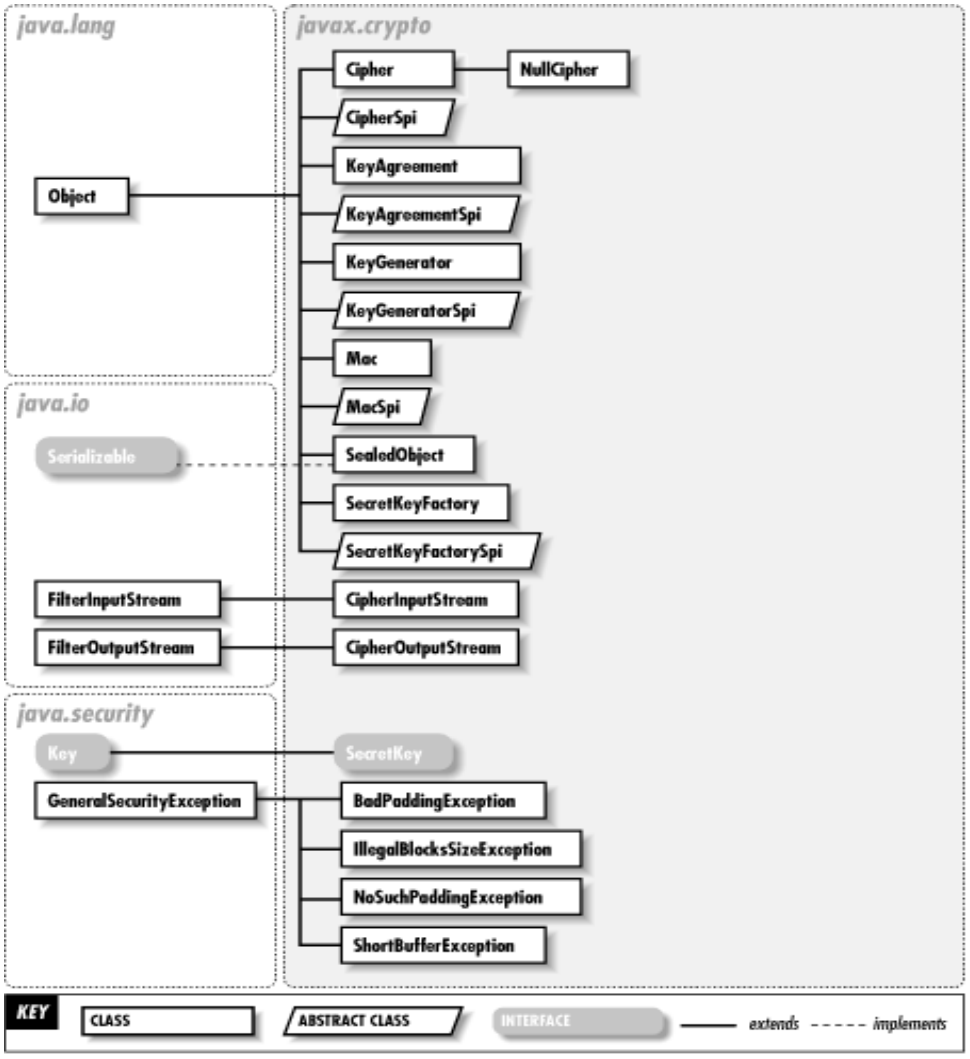


Рис. 4.1 Ієрархія классів Java

ОКО поширюються з криптографічним постачальником під назвою «SunJCE», який включає в себе широкий набір реалізацій шифру, KeyAgreement, Mac та інших класів. Установка розширення ОКА не те ж саме, проте, воно може бути встановленне так само як і SunJCE.

security.provider.2=com.sun.crypto.provider.SunJCE

Цифра 2 в рядку вище, визначає порядок переваг постачальника; Ви можете використовувати інший номер.

Якщо постачальник SunJCE не статично встановлений, як зазначено вище, його можна встановити динамічно:

```
import java.security.*;
Provider sunjce = new com.sun.crypto.provider.SunJCE();
Security.addProvider(sunjce);
```

Класс Cipher.

Цей клас забезпечує функціональність криптографічного шифру для шифрування і дешифрування. Він утворює ядро рамок Java Cryptographic Extension (JCE).

Для того, щоб створити Cipher об'єкт, додаток викликає метод GetInstance шифру, і передає ім'я запитуваного перетворення до нього.

Перетворення є рядком, що описує операцію (або набір операцій), які будуть виконуватися на даному вході. Перетворення завжди включає ім'я криптографічного алгоритму, а також може супроводжуватися режимом зворотного зв'язку і схемою доповнення.

Перетворення має вигляд:

«Алгоритм / режим / заповнення», або «Алгоритм».

(В останньому випадку використовуються значення конкретного постачальника за замовчуванням для режиму і схеми заповнення). Наприклад, наступне є допустимим перетворенням:

```
Cipher c = Cipher.getInstance("AES/CBC/PKCS5Padding");
```

Використання режимів, такі як CFB і OFB, блокові шифри можуть шифрувати дані в одиницях менших, ніж фактичний розмір блоку шифру. При запиті такого режиму, можна додатково вказати кількість біт, що підлягає обробці, в той час, додаючи це число до назви режиму, як показано в «DES / CFB8 / NoPadding» і перетвореннях «DES / OFB32 / PKCS5Padding». Якщо такий номер не вказано, використовується постачальник конкретних за замовчуванням. Таким чином, блокові

шифри можуть бути перетворені в байт-орієнтованих потокові шифри, використовуючи режим 8-бітний такий, як CFB8 або OFB8.

Режими, такі як шифрування з перевіркою достовірності Associated Data (AEAD) забезпечують гарантії як для конфіденційних даних і додаткові пов'язані з ним дані (ACP), які не зашифровані.

Режим GCM має вимогу єдиності, при використанні в шифруванні з заданим ключем. Таким чином, після кожної операції шифрування з використанням режиму GCM, абоненти повинні повторно ініціалізувати об'єкти шифрів з параметрами ГКР, який має інше значення .

Розробка класу SoundCapture.

Java Sound API є низькорівневим API для здійснення і контролю вхідних і вихідних звукових засобів, в тому числі аудіо та даних цифрового інтерфейсу музичних інструментів (MIDI). Java Sound API забезпечує явний контроль над можливостями, які зазвичай потрібний для звукового входу і виходу, в рамках, що сприяє розширюваності і гнучкості.

Java Sound API задовольняє потреби широкого кола розробників додатків. Потенційні області застосування включають в себе:

рамки комунікації, такі як конференц-зв'язок і телефонія

Кінцеві користувачі системи доставки контенту, такі як медіа-плеєри і мобільні телефони, використовують потоковий контент

Інтерактивні прикладні програми, такі як ігри та веб-сайти, які використовують динамічний вміст

Створення і редагування контенту

Інструменти, набори інструментів і утиліти

Java Sound API забезпечує найнижчий рівень підтримки звуку на платформі Java. Він надає прикладні програми з великою кількістю контролю над звуковими операціями, і є розширюваним. Наприклад, Java Sound API поставляє механізми

для установки, доступу та управління системних ресурсів, таких як аудіо-змішувачі, MIDI синтезатори, інші аудіо або MIDI-пристрої, зчитувачі та записувачі файлів і конвертори звукових форматів. Java Sound API не включає в себе складні звукові редактори або графічні інструменти, але він надає можливості, на яких можуть бути побудовані такі програми. Він підкреслює, низькорівневе управління понад те, що зазвичай очікується від кінцевого користувача.

Java Sound API включає в себе підтримку для цифрового аудіо і даних MIDI. Ці два основних модулі функціональних можливостей надаються у вигляді окремих пакетів:

javax.sound.sampled - Цей пакет визначає інтерфейси для захоплення, мікшування і відтворення цифрового (відібраного) аудіо.

javax.sound.midi - Цей пакет надає інтерфейси для MIDI-синтезу, секвенування і передачі аудіо.

Дві інші пакети дозволяють постачальникам послуг (на відміну від розробників додатків) створювати користувацькі програмні компоненти, які розширюють можливості реалізації в Java Sound API:

javax.sound.sampled.spi

javax.sound.midi.spi

Ця сторінка представляє семпл-аудіо системи, MIDI системи і пакети SPI.

Біліотека Javax.sound.sampled

Javax.sound.sampled пакет що обробляє цифрові звукові дані, які Java Sound API посилається як зразки аудіо. Зразки - це послідовні знімки сигналу. Мікрофон перетворює звуковий сигнал в відповідний аналоговий електричний сигнал, і аналого-цифровий перетворювач перетворює цей аналоговий сигнал в цифрову форму. На наступному рис 4.2. показаний короткий момент в запису звуку.

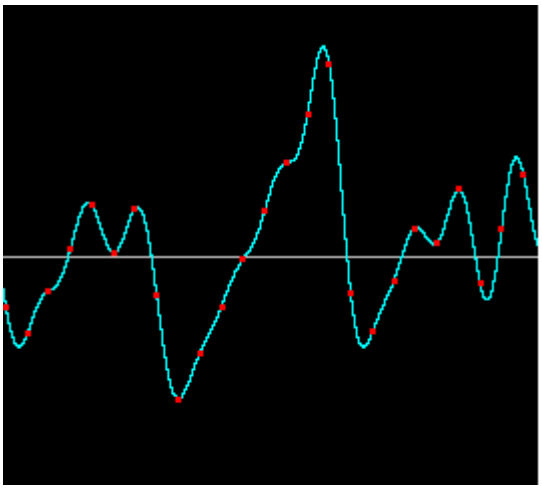


Рис. 4.2 Графік ділянки звуку

Цей графік ділянки звукового тиску (амплітуди) на вертикальній осі, а час по горизонтальній осі. Амплітуда аналогової звукової хвилі вимірюються періодично з певною швидкістю, що виводить дискретні вибірки (червоні точки на кресленні), які включають цифровий аудіосигнал. Центральна горизонтальна лінія вказує на нульову амплітуду; Точки вище ліній є позитивними значеннями вибірок, і нижче - негативними. Точність цифрового наближення аналогового сигналу залежить від його частоти дискретизації і його квантування, або число біт, що використовуються для представлення кожного зразка. В якості точки відліку, звук записаний для зберігання на компакт-дисках дискретизируется 44100 раз в секунду, і представлені 16 бітами на вибірку.

Термін «Аудіодані» використовується тут трохи вільно. Звукова хвиля може бути обрана через дискретні інтервали і в той же час залишається в аналоговій формі. Для Java Sound API, «Аудіодані» є еквівалентом терміну «цифрове аудіо.»

Як правило, зразки аудіо на комп'ютері походять від запису звуку, але звук може бути замість цього синтетично згенерованим (наприклад, для створення звуків кнопковим телефоном). Термін «вибірка аудіосигналу» відноситься до типу даних, а не його походження.

Java Sound API не приймає на себе певну конфігурацію аудіо апаратних засобів; він призначений для забезпечення різних видів аудіо компонентів, які будуть

встановлені в системі інадавати доступ до API. Java Sound API підтримує загальні функціональні можливості, такі як вхід і вихід з звукової карти (наприклад, для запису і відтворення звукових файлів), а також змішування декількох потоків аудіо. На рис. 4.3 наведено приклад типової аудіо архітектури:

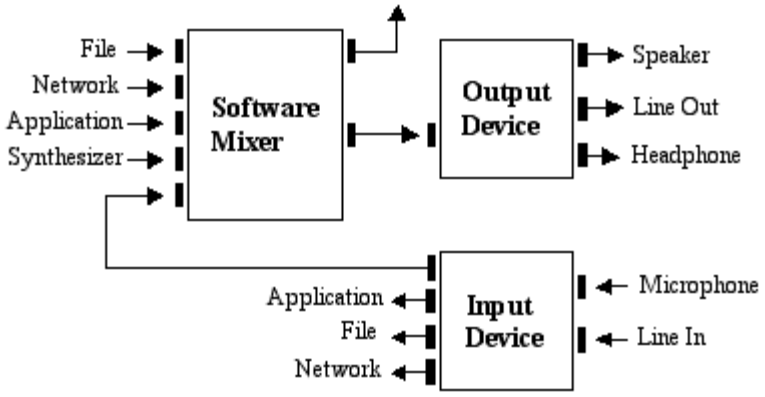


Рис. 4.3 Приклад аудіо архітектури

У цьому прикладі пристрій, звукова карта має різні вхідні і вихідні порти, а також змішування в програмному забезпеченні. Змішувач може отримати дані, які були прочитані з файлу, отримані з мережі, згенеровані прикладною програмою, або отримані за допомогою синтезатора MIDI. Змішувач поєднує в собі всі свої аудіо входів в єдиний потік, який може бути переданий на пристрій виведення для рендерингу [18].

Пакет javax.sound.midi містить API-інтерфейси для транспортування і послідовності MIDI-подій, а також для синтезу звуку з цих подій.

У той час як Аудіодані пряме уявлення самого звуку, дані MIDI можна розглядати як ынструмент для створення звуку. MIDI, на відміну від аудіо, не описує звук безпосередньо. Замість цього, він описує події, які впливають на звуки (або дії), що виконуються за допомогою MIDI-сумісного пристрою або приладу, наприклад, синтезатор. MIDI дані аналогічні подіям клавіатури і миші в графічному ко-

ристувальницькому інтерфейсі . У разі MIDI, події можна розглядати як дії, на музичній клавіатурі, поряд з діями на різних педалей, слайдерів, перемикачів і кнопок на певному музичному інструменті. Ці події повинні насправді не відбуваються з апаратним музичним інструментом; вони можуть бути змодельовані в програмному забезпеченні, і вони можуть бути збережені в MIDI-файли. Програма, яка може створювати, редагувати і виконувати ці файли, називається секвенсор. Багато комп'ютерних звукових карт включають в себе MIDI-керований музичний синтезатор, на які секвенсори можуть відправляти MIDI-події. Синтезатори також можуть бути повністю реалізовані в програмному забезпеченні. Синтезатори інтерпретують MIDI-події, які вони отримують і виробляють аудіовихід. Зазвичай звук синтезований з даних MIDI є музичним звуком (на відміну від мови, наприклад). MIDI синтезатори також здатні генерувати різні види звукових ефектів.

Деякі звукові карти включають в себе MIDI вхідні і вихідні порти, до яких можуть бути підключені зовнішні MIDI-апаратні пристрої (такі як синтезатори клавіатури або інших інструментів). Від вхідного порту MIDI, прикладна програма може отримувати події, що генеруються зовнішнім MIDI-обладнанням. Програма може зіграти музичну вистава за допомогою внутрішнього синтезатора комп'ютера, зберегти його на диск в якості MIDI-файлу, або зробити його нотний запис. Програма може використовувати порт MIDI виходу для відтворення на зовнішній інструмент або для управління інших зовнішніх пристроїв, таких як записуюче обладнання.

Провайдер інтерфейса послуг.

У javax.sound.sampled.spi і javax.sound.midi.spi пакети містять API, які дозволяють розробникам програмного забезпечення створювати нові аудіо або MIDI-ресурси, які можуть бути надані окремо користувачеві і «вставленими» в існуючуреалізацу Java Sound API. Ось деякі приклади послуг (ресурсів), які можуть бути додані таким чином:

Файл парсер, який може зчитувати або записувати новий тип аудіо або MIDI-файлу

Конвертер, який перетворює між різними форматами звукові дані.

У деяких випадках програмні інтерфейси і можливостей апаратних пристроїв, таких як звукові карти, можуть мати одного і тогож постачальника,як програмного , так і апаратного забезпечення. В інших випадках, існують послуги виключно в програмному забезпеченні. Наприклад, синтезатор або змішувач може бути інтерфейсом з чіпом на звуковій карті, або він може бути реалізований без апаратної підтримки взагалі.

Реалізація Java Sound API містить базовий набір послуг, але інтерфейс постачальника послуг, (SPI) пакети дозволяють третім сторонам створювати нові послуги. Ці сторонні сервіси інтегровані в систему таким же чином- Клас AudioSystem і клас MidiSystem як координатори, щонадають прикладним програмам доступ до служб явно або неявно. Часто існування служби повністю прозоро для прикладної програми, яка використовує його. Механізм сервісу-провайдер надає перевагу користувачам прикладних програм, заснованих на Java Sound API, оскільки нові звукові функції можуть бути додані до програми, не вимагаючи нового випуску JDK або середовища виконання, і, в багатьох випадках, навіть не вимагаючи нового випуску самої прикладної програми.

Висновок по розділу.

Показано практичне застосування алгоритму шифрування AES. У якості предметної сторони використовується мовна інформація.

ВИСНОВКИ

Показано особливості розповсюдження електромагнітних коливань діапазону, що відповідає стільниковому зв’язку. На розповсюдження електромагнітних хвиль суттєво впливають штучні та природні геометричні перепони.

Розглянуто методи захисту GSM сигналу що використовуються в мережі GSM, а також методи захисту що можуть використовуватись додатково. Розглянуто алгоритми шифрування GSM сигналу Rijndael і TwoFish.

Розроблено додаток на мові програмування java для шифрування сигналу алгоритмом AES. Для підвищенні захищеності інформаціїї в мережах стандарту GSM за допомогою криптоалгоритму AES, у роботі використовуються сучасні бібліотеки для обробки звуквого сигналу які використовуються в мові прогамування Java.

Як результат у роботі проведено аналіз криптоалгоритмів що використовуються в мережах GSM та можуть бути використані додатково, розроблено додаток на мові програмування java що використовує додаткові засоби для обробки сигналу що дозволить зменшити кількість викривлень сигналу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. С. Панасенко, "Алгоритми шифрування" :BHI,2009.-213с.

2. Alan G. Konheim **"**Computer Security and Cryptography**":**WILEY,2007.-346с

3. Брюс Шнайер "Прикладна криптографія":WILEY,2007.-514с.

4. С.Г. Баричев, Р.Е. Серов "Основи Сучасної Криптографії" :WILEY,2007.-145с.

5. Попов В.І. "Основи стільникового зв'язку стандарту GSM" :Эко-Трендз,2005 173с.

6. Джим Гейер "Беспроводные сети" :Вильямс,2005. 192с.

7. Кашкаров.А "Электронные устройства для глушения беспроводных сигналов(GSM,WI-FI,GPSи некоторых радиотелефонов)":Litres, 2017 - 604 с.

8. Кашкаров А. «Мобільник» і конфіденційність // Радіомір. 2005 - 12 с.

9. Ленков С.В., Перегудов Д. А., Хорошко В.А. Методы и средства защиты информации. – К., АРИЙ, 2008, Том I – 464с., Том II – 344 с.

10. Гулак Г., Горбенко И., Олейников Р. и др. Основные принципы проектирования, оценка стойкости и перспективы использования в Украине алгоритма шифрования AES// Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – Київ. – 2003. – №7 – С. 14-25.

11. Мухачев В.А., Хорошко В.А. Методы практической криптографии. К.: ООО «ПолиграфКонсалтинг», 2005. –215с.

12. Горбенко І.Д., Гулак Г.М., Олійников Р.В. та інш. Аналіз властивостей алгоритмів блокового симетричного шифрування (за результатами міжнародного проекту NESSIE)// Радіотехніка. Всеукраїнський міжвідомчий науково-технічний збірник, вип. 141, - Харків: ХНУРЕ, 2005. – С. 7-24.

13. Гулак Г., Горбенко И., Михайленко М., Гитис Ю. Блочный симметричный алгоритм SHACAL-2// Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – Київ. – 2003. – №7 – С. 86-100.

14. Кузнецов Г.В., Фомічов В.В., Сушко С.О., Фомічова Л.Я. Математичні основи криптографії. – Дніпропетровськ: НГУ, 2004. – 389 с.

15. NIST Special Publications 800-22. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, 2000.

16. Mecanismes cryptographiques Version 1.10. Crypto DCSSI @sgdn.pm.gouv.fr, 2006.

17. Feldman P. A practical scheme for non-interactive verifiable secret sharing // Proc. 28th Annu. Symp. on Found. of Comput. Sci. 1987. P. 427-437.

18. Фоменков Г.В. http://www.citforum.ru/cryptography/fortezza/.shtm.

ДОДАТКИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кваліфікаційна робота здобувача освітнього ступеня «МАГІСТР»

ЗАХИСТ ІНФОРМАЦІЇ У МЕРЕЖАХ МОБІЛЬНИХ ОПЕРАТОРІВ СТАНДАРТУ GSM

Спеціальність: 125 – Кібербезпека та захист інформації
Виконав: Артем КОБЕЦЬ
Керівник: к.т.н., доц. Андрій КОТЕНКО

Київ – 2025

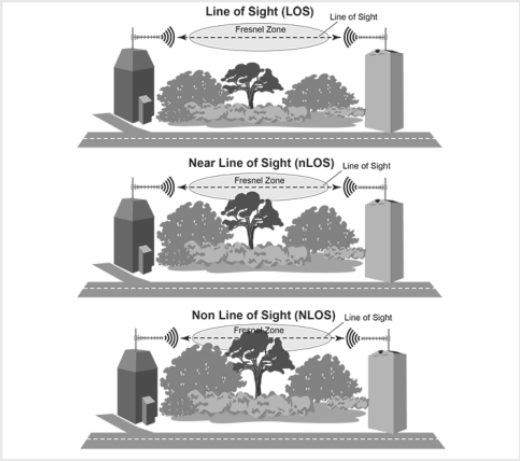
АКТУАЛЬНІСТЬ, МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

- Актуальність теми зумовлена широким поширенням мобільних пристроїв і зростанням ризиків несанкціонованого доступу до інформації у стільникових мережах.
- Об’єкт дослідження – процес захисту інформації у мережах мобільних операторів.
- Предмет дослідження – захист інформації стандарту GSM.
- Мета роботи – підвищення захищеності інформації в мережах стандарту GSM шляхом використання криптоалгоритму AES.
- Завдання: проаналізувати особливості сигналів стандарту GSM; розглянути існуючі методи захисту; дослідити алгоритми шифрування сигналів стандарту GSM.

ЗДОБУТІ РЕЗУЛЬТАТИ РОБОТИ

1	**РОЗДІЛ 1**	Проаналізовано радіосигнали GSM у стільникових мережах і особливості захисту інформації у каналах зв’язку.
2	**РОЗДІЛ 2**	Розглянуто напрямки захисту GSM сигналів, архітектуру та безпекові механізми стандарту GSM.
3	**РОЗДІЛ 3**	Проведено огляд типових алгоритмів шифрування даних, зокрема AES і Twofish.
4	**РОЗДІЛ 4**	Розроблено додаток для шифрування сигналу алгоритмом AES на мові програмування Java.
5	**ВИСНОВКИ**	Сформовано висновки та практичні рекомендації щодо підвищення захищеності інформації у мережах GSM.

ОСОБЛИВОСТІ РОЗПОВСЮДЖЕННЯ GSM СИГНАЛІВ



- У стільникових мережах рівень сигналу суттєво змінюється залежно від відстані до базової станції та умов забудови.
- Для міських умов характерні затінення будівлями, багатопроменевість і завмирання сигналу.
- Для оцінювання покриття застосовують статистичні, детерміновані та комбіновані моделі розрахунку.

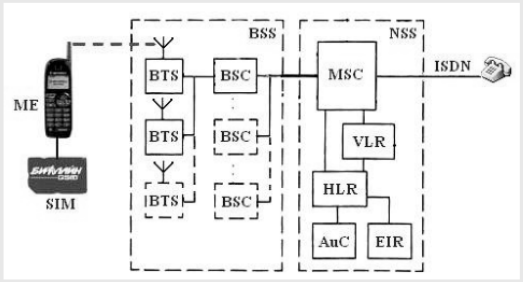
ШЛЯХИ ЗАХИСТУ ІНФОРМАЦІЇ У КАНАЛАХ СТІЛЬНИКОВОГО ЗВ’ЯЗКУ

- Організаційно-режимні заходи передбачають обмеження використання смартфонів на об’єктах, де обробляється конфіденційна інформація.
- Технічні заходи включають екранування приміщень, акустичне зашумлення та контроль доступу до мобільних пристроїв.
- Практичні рекомендації охоплюють захист додатків, керування дозволами, регулярні оновлення та вимкнення непотрібних інтерфейсів.

НАПРЯМИ ЗАХИСТУ GSM СИГНАЛІВ

- Розглянуто програмно-технічні засоби GSM SAFE, GSM CASE та GSM-Box, які виявляють або блокують несанкціоновану активацію мобільного пристрою.
- Захист може реалізовуватися через генерацію маскувального шуму, екранування та контроль випромінювань.
- Додатково використовуються контрольовані протоколи GSM 900/1800, Wi-Fi та Bluetooth для виявлення загроз.

ЗАГАЛЬНИЙ ОГЛЯД СТАНДАРТУ GSM



- GSM — цифровий стандарт мобільного зв’язку другого покоління з розподілом доступу за принципом TDMA.
- Архітектура мережі містить підсистему базових станцій BSS, комутаційну підсистему NSS, а також MS, BTS, BSC, MSC, HLR, VLR, AuC та EIR.
- Стандарт підтримує роботу в діапазонах 850, 900, 1800 і 1900 МГц та широко використовується в мобільних мережах.

ІНФОРМАЦІЙНА БЕЗПЕКА СТАНДАРТУ GSM

- Система GSM включає механізми автентифікації абонента та контролю дозволеного обладнання через AuC і EIR.
- Після встановлення з’єднання дані передаються у зашифрованому вигляді для зменшення ризику підслуховування.
- Для захисту конфіденційності користувача застосовується тимчасова ідентифікація та приховування його місцезнаходження.

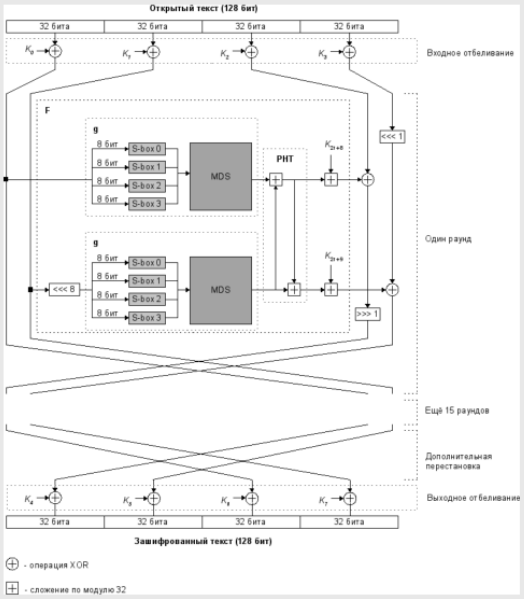
ТИПОВІ АЛГОРИТМИ ШИФРУВАННЯ ДАНИХ

- Для забезпечення конфіденційності можуть використовуватись DES, 3DES, IDEA, AES, Twofish, Blowfish та інші симетричні алгоритми.
- Під час вибору алгоритму важливими критеріями є довжина ключа, довжина блоку, кількість раундів та складність математичних перетворень.
- Для мультимедійних даних у реальному часі необхідно поєднати криптографічну стійкість із невеликими часовими затримками.

АЛГОРИТМ ШИФРУВАННЯ AES

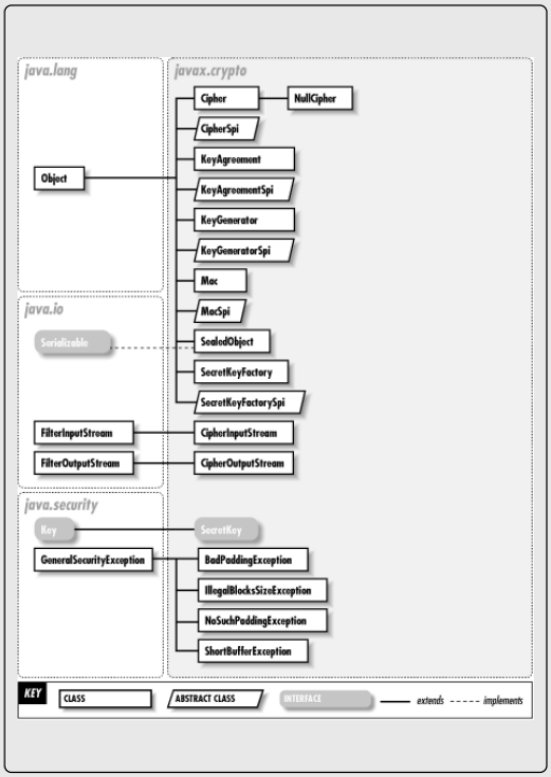
- AES офіційно прийнято як федеральний стандарт шифрування даних у США у 2001 році; його попередником був алгоритм Rijndael.
- Використовуються варіанти AES-128, AES-192 і AES-256; довжина блоку даних становить 128 біт.
- Основні етапи перетворення: AddRoundKey, ByteSub, ShiftRows, MixColumns та фінальний раунд без MixColumns.
- Перевагами AES є висока стійкість, поширеність та можливість ефективної програмної реалізації.

АЛГОРИТМ ШИФРУВАННЯ TWOFISH



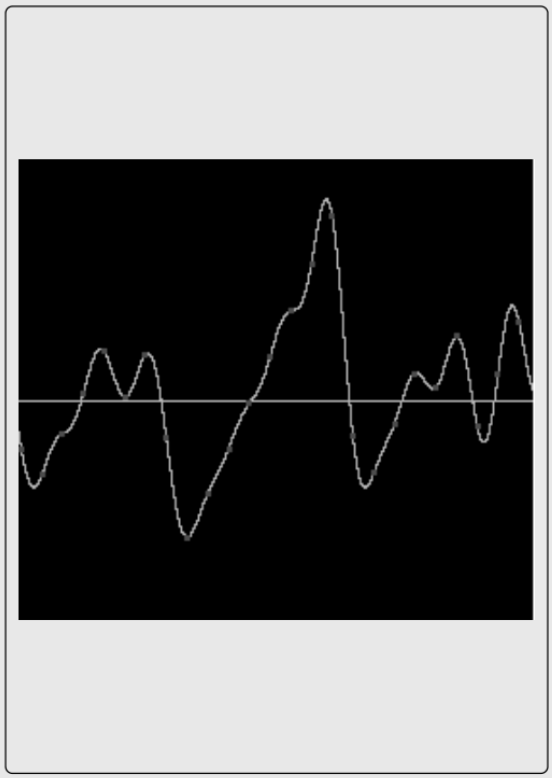
- Twofish — симетричний блочний алгоритм шифрування з розміром блоку 128 біт і довжиною ключа до 256 біт.
- Алгоритм має 16 раундів та використовує попередньо обчислені S-box, залежні від ключа, а також складну схему розгортання підключів.
- Twofish належав до фіналістів конкурсу AES і є придатним для побудови захищених телекомунікаційних рішень.

РОЗРОБКА ДОДАТКУ ДЛЯ ШИФРУВАННЯ ЗА АЛГОРИТМОМ AES



- Для реалізації додатку обрано мову програмування Java та середовище розробки Eclipse Neon.
- Програму умовно поділено на сім класів, зокрема AesEncription, Audiorecorder, CriptoException, DecriptionForm, EncriptionForm та SoundCapture.
- Для побудови інтерфейсу використано бібліотеку Swing, а для криптографічних операцій — можливості Java Cryptography Extension.

ОСНОВНІ РЕЗУЛЬТАТИ РОБОТИ



- Проаналізовано особливості поширення GSM сигналів і визначено фактори, що впливають на захищеність каналів стільникового зв’язку.
- Розглянуто алгоритми Rijndael (AES) і Twofish та обґрунтовано доцільність використання AES для захисту сигналів GSM.
- Розроблено програмний додаток для шифрування сигналу алгоритмом AES із використанням сучасних бібліотек Java для обробки звуку.

ДЯКУЮ ЗА УВАГУ!

Доповідь підготував здобувач вищої освіти Артем КОБЕЦЬ

Тема: «Захист інформації у мережах мобільних операторів стандарту GSM»

Київ – 2025