ХАРЬКІВСКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

СТРУКТУРНІ КОМПОНЕНТИ МЕРЕЖІ GSM/GPRS ЯК ОБ'ЄКТИ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

ЛЕКЦІЯ 8

Доцент кафедри кібербезпеки та ІТ
к.т.н. Лимаренко Вячеслав Володимирович
к.т. 066-0708586 (Viber, Telegram)

ТЕХНОЛОГІЯ GSM

Технологія GSM (Global System for Mobile Communications) – глобальний цифровий стандарт для мобільного стільникового зв'язку з розділенням частотного каналу за принципом TDMA (Time Division Multiple Access) - множинний доступ з тимчасовим поділом) та середнім ступенем безпеки. Технологія GSM відноситься до мереж 2-го покоління (2G – цифровий стільниковий зв'язок), хоча з 2010 р. умовно знаходилась у фазі 2.75G завдяки численним розширенням. Технологія GSM функціонує в чотирьох частотних діапазонах: 850 МГц, 900 МГц, 1800 МГц, 1900 МГц. Загальна архітектура технології GSM представлена на рис. 1.

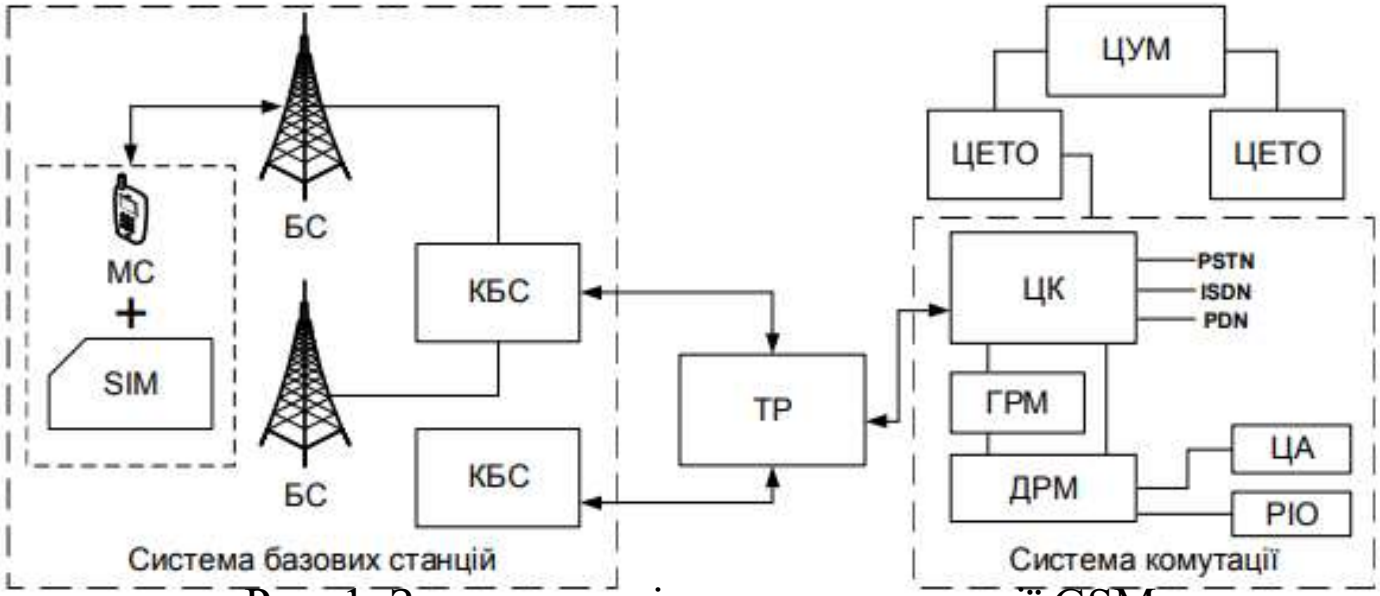
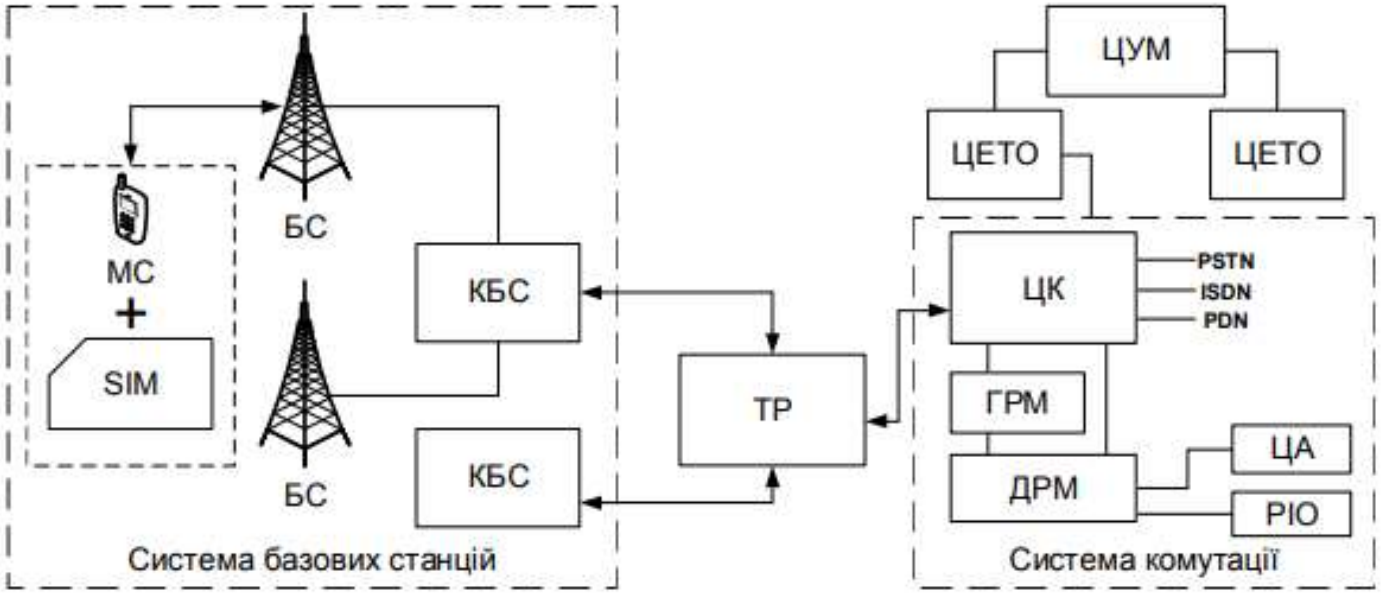


Рис. 1. Загальна архітектура технології GSM

ТЕХНОЛОГІЯ GSM



Мобільна станція (МС);
Мікропроцесорна карта SIM (Subscriber Identify Modul);
Контролери базових станцій (КБС);
Базові станції (БС);
Центр комутації (ЦК);
Транскодер (ТР);
Домашній реєстр місцезнаходження (ДРМ);
Гостьовий реєстр місцезнаходження (ГРМ);
Центр автентифікації (ЦА);
Реєстр ідентифікації обладнання (РІО);
Центр експлуатації технічного обслуговування (ЦЕТО);
Центр управління мережею (ЦУМ).

ТЕХНОЛОГІЯ GSM

Мобільна станція (МС) із мікропроцесорною картою SIM (Subscriber Identify Modul), в яку занесені унікальні дані для обміну інформацією між абонентами.

Контролери базових станцій (КБС) – здійснюють керування базовими станціями (БС) і в подальшому формують з'єднання з центром комутації (ЦК), за допомогою якого можна створити канал передавання даних між двома абонентами.

Транскодер (ТР), як проміжна ланка між БС та системою комутації, забезпечує перетворення вихідних сигналів каналу передавання мовного сигналу і даних (64 Кбіт/с) до виду, що відповідає рекомендаціям GSM по радіоінтерфейсу (13 Кбіт/с).

В домашньому реєстрі місцезнаходження (ДРМ) зберігається інформація про місцезнаходження будь-якої МС, яка дозволяє центру комутації реалізувати виклик до цієї станції.

Загалом ДРМ представляє базу даних (БД), в якій зберігається службова інформація про абонента.

ТЕХНОЛОГІЯ GSM

Гостьовий реєстр місцезнаходження (ГРМ) – це тимчасова БД абонентів, які знаходяться в зоні дії відповідного центру комутації. У кожного ЦК є лише один гостьовий реєстр місцезнаходження. В ГРМ зберігається та ж інформація що і в ДРМ, але лише до того часу допоки МС знаходиться в зоні дії цього ГРМ.

Центр автентифікації (ЦА) – це сервіс, за допомогою якого перевіряється право на доступ абонента до мережі, зокрема формуються ключі та алгоритми автентифікації. В ЦА зберігаються: унікальні номери абонента, індивідуальний ключ, алгоритм автентифікації.

Реєстр ідентифікації обладнання (РІО) – сервіс, в якому знаходиться централізована БД для підтвердження міжнародного ідентифікаційного номеру МС (IMEI).

Центр експлуатації технічного обслуговування (ЦЕТО) – забезпечує контроль і керування іншими компонентами мережі та контроль якості її роботи.

Центр управління мережею (ЦУМ) – дозволяє забезпечити раціональне ієрархічне управління мережею GSM та відповідає за експлуатацію і технічне обслуговування.

ТЕХНОЛОГІЯ GSM

В GSM використовується дві смуги частот: uplink (трансмісія вгору) 890 – 915 МГц, яка призначена для передавання даних від МС до БС; downlink (трансмісія вниз) 935 – 960 МГц відповідно для передавання інформації від БС до МС. Кожна із смуг дозволяє організувати по 124 симплексних канали із частотним рознесенням між каналами до 200 кГц. Враховуючи архітектуру, функціонування та особливості технології GSM розглянемо характеристику системи “об’єкт – загроза – захист” згідно інформаційної моделі (рис. 2)

ТЕХНОЛОГІЯ GSM

Технологія GSM та її характеристика

GSM	Характеристики системи "об'єкт-загроза-захист"
Об’єкт: середовище передавання даних, обладнання	Ефір: ▪ Мобільна станція ▪ Базові (передавально-приймальні) станції ▪ Провідне середовище, або ефір: ▪ Контролер базових станцій ▪ Транскодер ▪ Центр комутації ▪ "Домашній" регістр місцезнаходження ▪ "Гостьовий" регістр місцезнаходження ▪ Центр автентифікації ▪ Регістр ідентифікації обладнання ▪ Центр експлуатації і технічного обслуговування ▪ Центр управління мережею
Загрози інформаційній безпеці	▪ Знищення або викривлення логічної структури даних ▪ Несанкціоноване отримання інформації та її модифікація ▪ Зашумлення каналу зв’язку

ТЕХНОЛОГІЯ GSM

Технологія GSM та її характеристика

Загрози інформаційній безпеці		▪ Знищення або викривлення логічної структури даних ▪ Несанкціоноване отримання інформації та її модифікація ▪ Зашумлення каналу зв'язку
Захист інформації: технології	Методи	▪ Шифрування даних в радіоканалі ▪ Автентифікація повідомлень ▪ Автентифікація користувача ▪ Перепризначення TMSI ▪ Ідентифікація обладнання
	Засоби	▪ Скремблери ▪ Криптофони ▪ Інвертори спектру ▪ Генератори шуму ▪ Змінювачі голосу ▪ SIM-карти ▪ Шифратори ▪ Алгоритми шифрування (A5/1, A5/2, A5/3) ▪ Ідентифікаційний номер рухомого терміналу (IMEI)

ТЕХНОЛОГІЯ GSM
Процедура автентифікації

У стандарті GSM процедура автентифікації пов’язана з використанням модуля ідентифікації абонента (Subscriber Identity Module – SIM), званого також SIM-картою (SIM-card) або смарт-картою (smart-card). Модуль SIM – це знімний модуль, що встановлюється у відповідне гніздо абонентського апарату. Модуль SIM містить персональний ідентифікаційний номер абонента (Personal Identification Number – PIN), міжнародний ідентифікатор абонента мобільного зв’язку (International Mobile Subscriber Identity – IMSI), індивідуальний ключ автентифікації абонента Ki, індивідуальний алгоритм автентифікації абонента A3, алгоритм обчислення ключа шифрування A8.

ТЕХНОЛОГІЯ GSM
Процедура автентифікації

Для автентифікації використовується зашифрований відгук (signed response) S, що є результатом застосування алгоритму A3 до ключа Ki і квазівипадкового числа R, яке рухома станція отримує від центра автентифікації через центр комутації. Алгоритм A8 використовується для знаходження ключа шифрування повідомлень. Унікальний ідентифікатор IMSI для поточної роботи замінюється тимчасовим ідентифікатором TMSI (Temporary Mobile Subscriber Identity – тимчасовий ідентифікатор абонента мобільного зв'язку), який присвоюється радіотелефону при його першій реєстрації у конкретному регіоні, що визначається ідентифікатором LAI (Location Area Identity – ідентифікатор області місцеположення), і анулюється при виході апарату за межі цього регіону. Ідентифікатор PIN – це код, відомий тільки абонентові, який має служити захистом від несанкціонованого використання SIM-карти, наприклад при її втраті. Після трьох невдалих спроб набору PIN-кода SIM-карта блокується, а блокування може бути знято або набором додаткового коду – персонального коду розблокування (Personal unblocking key – PUK), або за командою з центру комутації.

ТЕХНОЛОГІЯ GSM
Процедура автентифікації

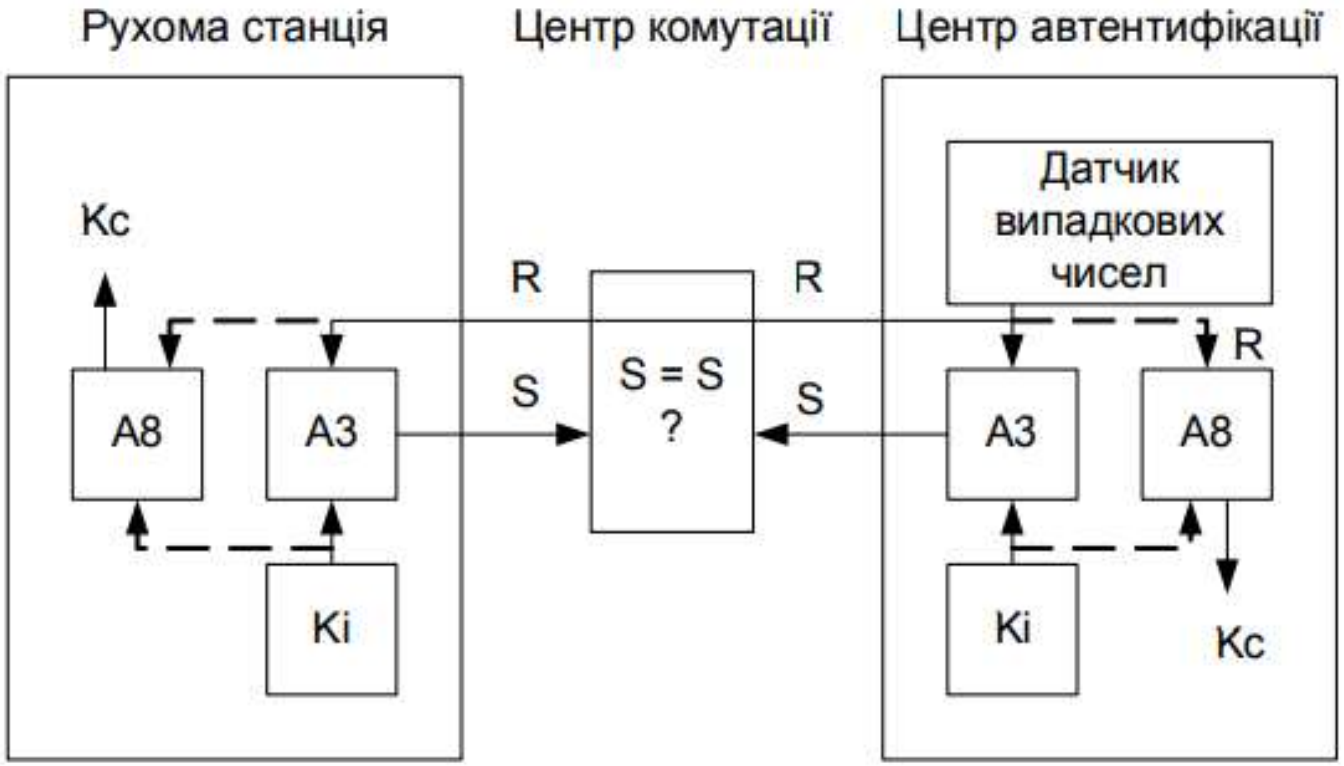


Рис. 2. Структурна схема проведення процедури автентифікації у стандарті GSM

Пунктиром позначені елементи, що не відносяться безпосередньо до процедури автентифікації, але використовуються для знаходження ключа шифрування Кс. Таким чином, апарат функціонуватиме, якщо він не ідентифікований у “чорних" списках і автентифікований.

ТЕХНОЛОГІЯ GSM
Процедура автентифікації

Суть аутентифікації в GSM - уникнути клонування мобільного телефону користувача. Секретним ключем є 128-бітний ключ Ki, яким володіє як абонент, так і Центр Аутентифікації (AuC - Authentication Centre). Ki зберігається в SIM-карті, також як і алгоритм A3. Також в аутентифікації беруть участь Домашній реєстр місцеположення (HLR - Home Location Registry) і Центр комутації (MSC - Mobile Switching Centre)

Коли MS запитує доступ до мережі GSM (наприклад при включенні), MSC повинен перевірити справжність MS. Для цього MSC відправляє в HLR унікальний міжнародний ідентифікатор абонента (IMSI - International Mobile Subscriber Identity) і запит на отримання набору спеціальних триплетів. Коли HLR отримує IMSI запит на триплети, він спочатку перевіряє свою базу даних, щоб упевнитися, що MS з таким IMSI дійсно належить мережі. Якщо перевірка пройшла успішно, то HLR відправляє IMSI і запит встановлення автентичності в AUC.

ТЕХНОЛОГІЯ GSM
Процедура автентифікації

AuC використовує IMSI, щоб знайти Ki відповідає цьому IMSI. Також AuC генерує випадкове 128-бітове число RAND. Після цього AuC обчислює 32-бітний відгук SRES (SRES - Signed Response) за допомогою алгоритму A3: SRES = A3 (RAND, Ki). Крім того, AUC обчислює 64-бітний сеансовий ключ Kc за допомогою алгоритму A8: Kc = A8 (RAND, Ki). Kc надалі використовується в алгоритмі A5 для шифрування і розшифрування даних.
RAND, SRES, і Kc якраз утворюють триплети, які MSC запросив у HLR. AuC генерує п'ять таких триплетів і посилає їх в HLR, потім HLR пересилає цей набір в MSC. Генерується саме набір триплетів, щоб зменшити передачу сигналів в GSM core network, яка відбувалася б кожен раз, коли MS запитувала б доступ до мережі, а MSC мав би перевірити справжність MS. Слід зазначити, що набір триплетів унікальний для одного IMSI і не може бути використаний для будь-якого іншого IMSI.
MSC зберігає Kc і SRES і надсилає запит RAND мобільної станції MS абонента. Отримавши запит RAND, MS обчислює відповідь на запит SRES за допомогою алгоритму A3 і секретного ключа Ki: SRES = A3 (RAND, Ki), і посилає його в MSC. Якщо прийнятий SRES збігається з SRES, що зберігаються в MSC, то аутентифікація вважається пройденою успішно.

Після п'яти сесій аутентифікації MSC запитує у HLR новий набір триплетів (RAND, SRES, Kc)

ТЕХНОЛОГІЯ GSM

Процедура автентифікації

В даний час прийнято наступний формат вхідних і вихідних даних RAND, Ki, SRES алгоритму A3: довжина Ki - 128 біт довжина RAND - 128 біт довжина SRES - 32 біта.

Час виконання алгоритму A3 має бути менше 500 мілісекунд.

В даний час відомі наступні стандартні реалізації алгоритму A3:

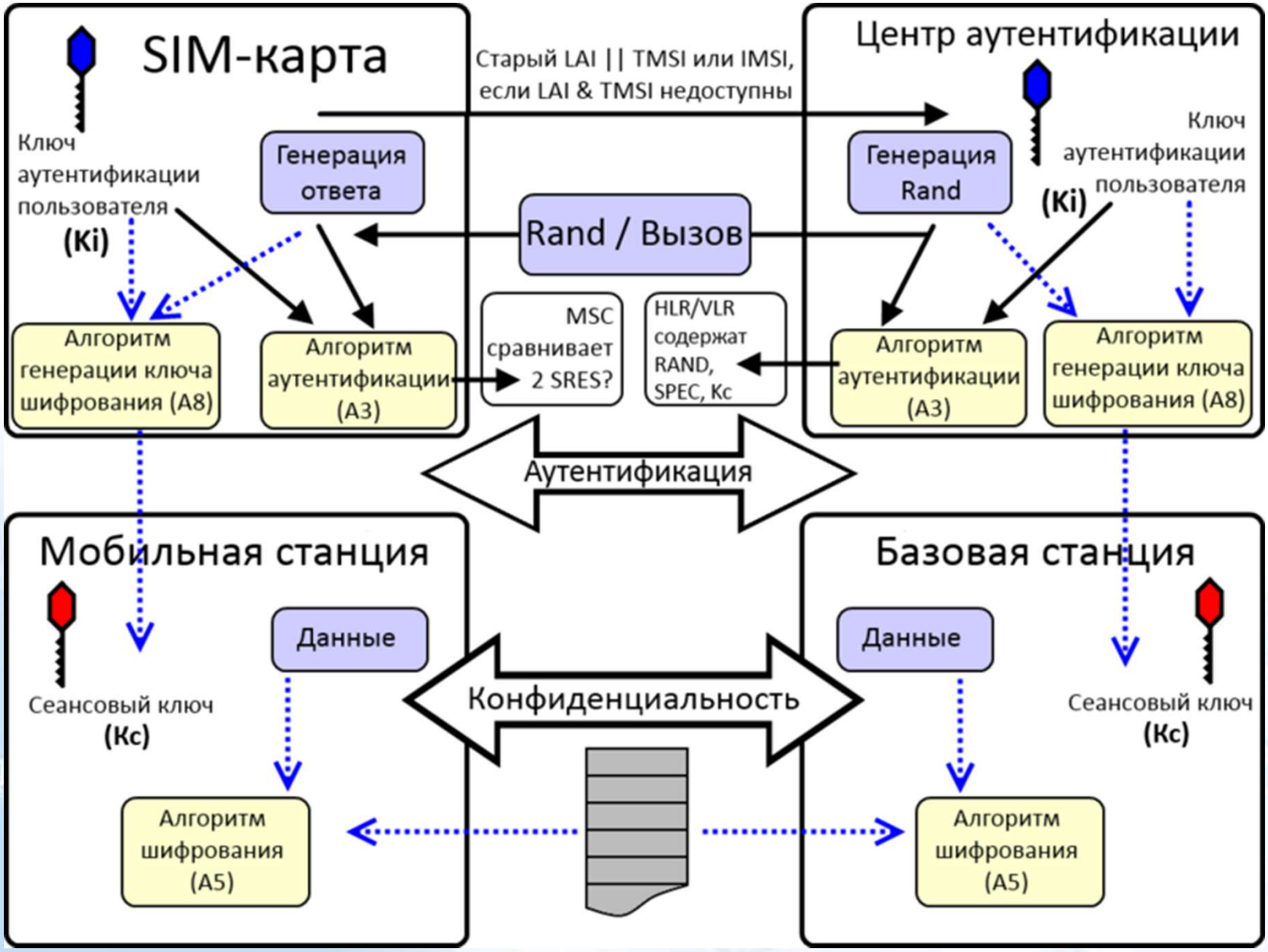
· COMP128 (структура цього алгоритму називається «формою метелика». Складається з 8 раундів в кожному раунді по 5 ітерацій)

· COMP128-2 (тримається в секреті)

· COMP128-3 (тримається в секреті)

· MILENAGE (вважається невразливим до будь-яких відомим атакам)

ТЕХНОЛОГІЯ GSM
Процедура автентифікації



ТЕХНОЛОГІЯ GSM
Алгоритм A3/A8

Формат вхідних і вихідних даних для алгоритму A8 строго визначений консорціумом 3GPP. Але A8 не є стандартизованим, а визначається оператором. Алгоритми A3 і A8 реалізовані як єдине обчислення, вихідні дані якого (96 біт) трактуються так: 32 біта для визначення SRES і 64 біта для визначення Kc. Довжина значної частини ключа Kc, видана алгоритмом A8 може бути менше 64 біт. Тоді значущі біти доповнюються нулями до кількості 64, зазначеного в специфікації алгоритму. В даний час відомі наступні стандартні реалізації алгоритму A3 / A8:

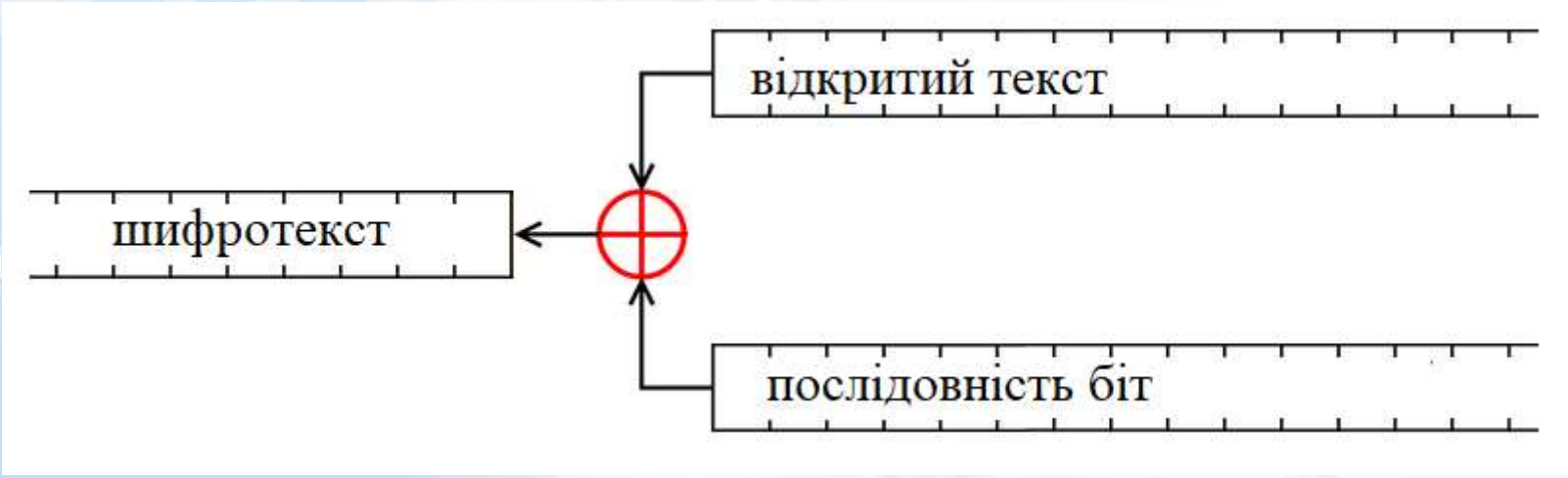
COMP128
COMP128-2
COMP128-3
MILENAGE

Хоча існують альтернативи COMP128, але цей протокол як і раніше підтримується в переважній більшості мереж GSM. За даними SDA (Smarcard Developer Assosiation), більшість операторів зв'язку не виробляє перевірку на одночасне включення «однакових» абонентів, настільки вони впевнені в неможливості клонування Sim-карт.

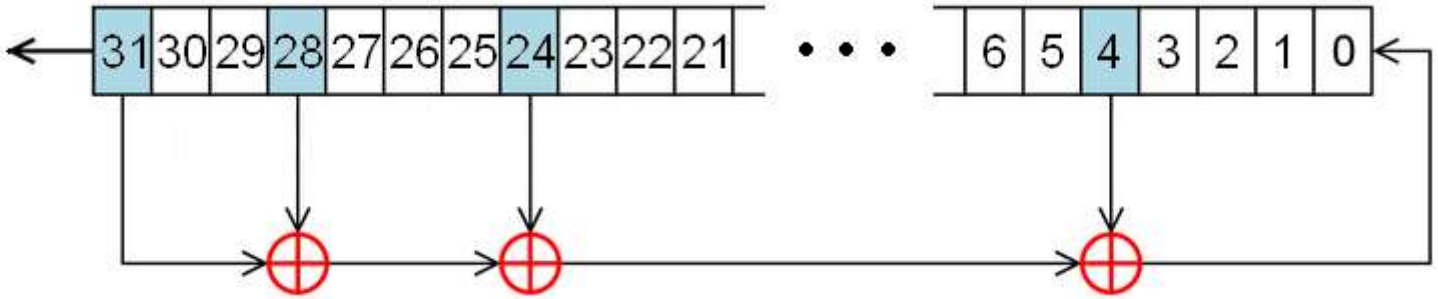
ТЕХНОЛОГІЯ GSM
Алгоритм A5

A5 - це потоковий алгоритм шифрування, використовуваний для забезпечення конфіденційності даних між телефоном і базовою станцією в європейській системі мобільного цифрового зв'язку GSM (Groupe Spécial Mobile).

Шифр заснований на побітового складання по модулю два (булева операція «виключне або») генерується псевдослучайной послідовності і шіфруемий інформації. У A5 псевдослучайная послідовність реалізується на основі трьох лінійних регістрів зсуву зі зворотним зв'язком. Регістри мають довжини 19, 22 і 23 біти відповідно. Зрушеннями управляє спеціальна схема, організуюча на кожному кроці зміщення як мінімум двох регістрів, що призводить до їх нерівномірного руху. Послідовність формується шляхом операції «виключне або» над вихідними битами регістрів.



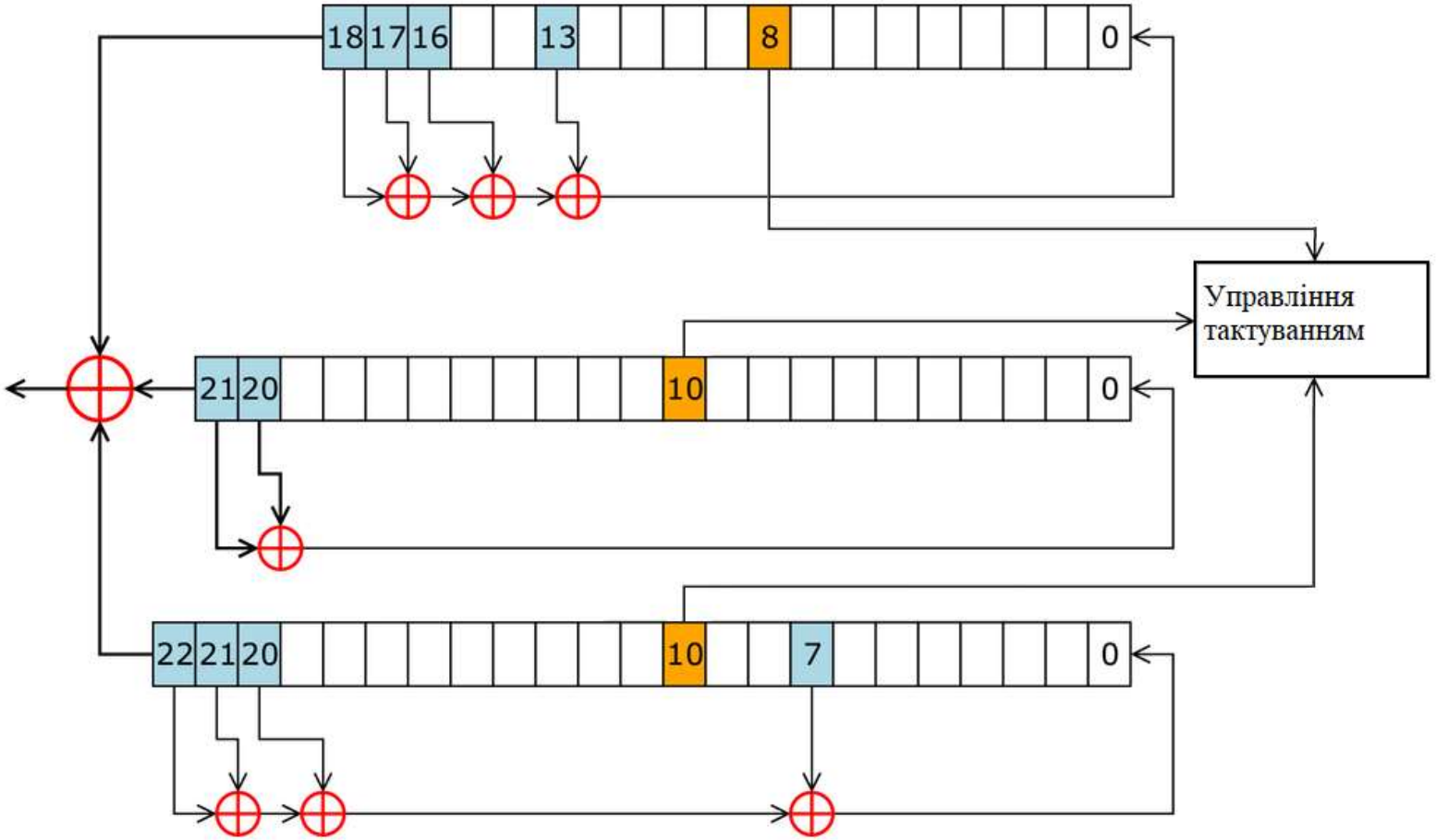
ТЕХНОЛОГІЯ GSM
Алгоритм A5



Регістр зсуву, прімітивний многочлен

$x^{32}+x^{29}+x^{25}+x^{5}+1$

ТЕХНОЛОГІЯ GSM
Алгоритм A5/1



- $X^{19} + X^{18} + X^{17} + X^{14} + 1$ для R1
- $X^{22} + X^{21} + 1$ для R2
- $X^{23} + X^{22} + X^{21} + X^{8} + 1$ для R3

ТЕХНОЛОГІЯ GSM
Алгоритм A5/1 функція тактування

Управління тактуванням здійснюється спеціальним механізмом:

в кожному регістрі є біти синхронізації: 8 (R1), 10 (R2), 10 (R3), обчислюється функція F = x & y | x & z | y & z, де & - логічне AND, | - булево OR, а x, y і z - біти синхронізації R1, R2 і R3 відповідно, зсуваються тільки ті регістри, у яких біт синхронізації дорівнює F, фактично, зсуваються регістри, сінхробіт яких належить більшості, Вихідний біт системи - результат операції XOR над вихідними битами регістрів.

ТЕХНОЛОГІЯ GSM

Джерело загроз № 1.

Постачальник послуг – оператор стільникового зв'язку.

Оператор стільникового зв'язку акумулює повну інформацію про абонентів. Причому надходить вона з двох джерел: з реєстраційної форми абонента (персональні дані) та передається в білінг при користуванні послугами. У мережі модулем ідентифікації абонента є SIM-карта, яка має кілька параметрів і в поєднанні зі спеціальними параметрами мобільного пристрою може розповісти про абонента все. Так, у базу даних білінгової системи завантажуються профілі дзвінків (напрямок, номер, тривалість), геопозиціонування (визначається за прив'язкою до базової станції та сотою), обсяг і профіль використання трафіку, SMS, MMS та ін. Зрозуміло, оператор вдається до безпрецедентних заходів захисту цієї інформації, проте трапляються витоки інформації.

Крім загрози компрометації білінгу, небезпека може виходити і від сервісів оператора зв'язку. Так, послуга батьківського контролю або будь-яка послуга трекінгу може використовуватися для відстеження переміщення абонента.

Джерело загроз № 2.

Виробники мобільних пристроїв і систем керування (операційна система).

Новітні пристрої мобільного зв'язку вкрай гнучкі в налаштуванні різних систем стеження, і пов'язано це саме з тим, що з'явилися повноцінні операційні системи, що призвело до можливості написання шпигунського програмного забезпечення і впровадження його в логіку операційної системи. Додаткову загрозу створює безперервне з'єднання з мережею Інтернет і передача міток геопозиціонування.

ТЕХНОЛОГІЯ GSM

Джерело загроз № 3.

Перехоплення інформації в радіоканалі (комплекси перехоплення: активні, напівактивні, пасивні та ін. Засоби перехоплення).

До способів перехоплення можна віднести впровадження хибної базової станції (пастка IMSI), яка знижує встановлений у мережі рівень шифрування та значно полегшує перехоплення даних. Вона працює з унікальним ідентифікатором, прописаним у SIM-карті – IMSI (International Mobile Subscriber Identity). Пастка IMSI – невеликий пристрій, що імітує вежі стільникового зв'язку. Стандарт зв'язку GSM передбачає обов'язкову автентифікацію апарату в мережі при відсутності подібного зобов'язання від самої мережі. Пастка відключає шифрування, збирає дані і передає вже відкритий сигнал базової станції (з'єднувати абонента вона не вміє).

ТЕХНОЛОГІЯ GSM

IMSI-ПЕРЕХОПЛЮВАЧ.

Це пристрій (розміром з валізу або навіть всього лише з мобільник), яке використовує конструктивну особливість мобільників, - віддавати перевагу тій стільникового вишці, чий сигнал найбільш сильний (щоб максимізувати якість сигналу і мінімізувати власне енергоспоживання). Крім того, в мережах GSM (2G) проходити процедуру аутентифікації повинен тільки мобільник. Від стільникової вишки цього не потрібно. Тому мобільник легко ввести в оману, - в тому числі, щоб відключити на ньому шифрування даних. З іншого боку, універсальна система мобільного зв'язку UMTS (3G) вимагає двосторонньої аутентифікації; однак її можна обійти, використовуючи режим сумісності GSM, присутній в більшості мереж. Мережі 2G і раніше широко поширені - мережеві оператори використовують GSM в якості резервної мережі в тих місцях, де UMTS недоступна.

ТЕХНОЛОГІЯ GSM

SAI-2. Система активного GSM перехвата с промежуточной базовой станцией

Активный GSM перехватчик

Основные характеристики

Артикул	1104
Производитель	Intercept
Категория	Сотовый перехват
Стандарт	2G (GSM)/900/1800/850/1900
На выходе	Голос и SMS, данные звонков
Питание	220/110/24/12-16V, 220W
Радиус действия (м)	500
ОС	Windows 7, 10
Дешифрование	A5.2, A5.1, (A5,3 через понижение); до 20 ключей в сек
Аккумулятор	через AC-DC конвертер
Дисплей	17" TFT, 1024x768
SMS(MMS)	на всех языках
Антенна	Одинарная вседиапазонная или направленная
Кол-во каналов	8 расширяются до 12
Интернет	Да
Разъемы	USB
Передача данных	GPRS / EDGE
Протоколы	IMEI, IMSI, TMSI
Управление	API, IP
Комплект поставки	Перехватчик, ноутбук, антенна, конвертер AC-DC, S\W
Размеры (ВхШхД)	290x280x80 мм
Вес	10 кг
Доставка	По всему миру

ТЕХНОЛОГІЯ GSM