УДК 007.681 **Пархуць Ю.Л. (НУ «Львівська політехніка»)**

КРИПТОГРАФІЧНІ МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЇ В МОБІЛЬНОМУ ЗВ'ЯЗКУ

В статті розглянуті принципи функціонування механізмів захисту інформації в мережах мобільного зв'язку, наведена оцінка їх ефективності, здійснено огляд сучасних додаткових засобів забезпечення конфіденційності розмов, визначені напрями подальших вдосконалень захисту, наведена модель рішення задачі інформаційної безпеки абонента.

Ключові слова: захист інформації, кодування, алгоритм шифрування, ідентифікація, авторизація, конфіденційність, смартфон, скремблер, криптографія.

Стрімкий розвиток в галузі бездротового зв'язку призвів до ситуації коли тотальна більшість сеансів обміну інформацією відбувається саме за допомогою засобів стільникового зв'язку. За допомогою мобільного телефону ми обговорюємо як звичайні побутові питання, так і певні конфіденційні дані, які можуть становити неабиякий інтерес зі сторони різного роду зловмисників (конкурентів, шпигунів і т.д.). Тому недивно, що увага до питання конфіденційності зв'язку невпинно зростає. Саме аспекти інформаційної безпеки будуть предметом розгляду даної статті. На сьогоднішній день існує декілька стандартів мобільного зв'язку, які по різному вирішують задачу захисту даних абонента.

В стандарті GSM політика інформаційної безпеки складається з механізмів ідентифікації та аутентифікації абонента, а також шифрування його мовного сигналу. Основним елементом за яким можна ідентифікувати користувача є SIM карточка, яка містить міжнародний ідентифікаційний номер IMSI (International Mobile Subscriber Identity), унікальний ключ аутентифікації Ki та алгоритм аутентифікації A3 [2, с.10-11]. При реєстрації абонента, центр авторизації домашньої мережі генерує 128-бітне випадкове число RAND (Random) і пересилає його на телефон користувача. В SIM карті за допомогою ключа Ki та алгоритму A3 відбувається обчислення 32-бітної відповіді SRES (Signed Result) за схемою, що наведена на рис.1.

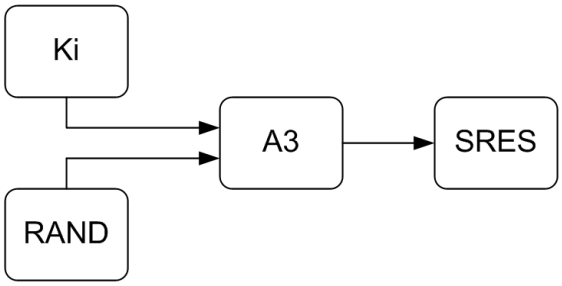

Рис.1. Процедура формування відповіді для авторизації в стандарті GSM

Аналогічні обчислення відбуваються і в центрі авторизації мережі за допомогою вибраного з реєстру абоненті ключа Ki користувача. Телефон надсилає свій результат обчислення SRES, який порівнюється із відповідним значенням, обчисленим в центрі авторизації. Якщо ці значення співпадають то процес авторизації вважається успішним і абоненту присвоюється тимчасовий номер TMSI (Temporary Mobile Subscriber Identity), який слугує виключно для підвищення безпеки взаємодії абонента. Далі відбувається передача серійного номеру телефону IMEI в мережу, де він перевіряється в базі даних реєстру ідентифікації обладнання. Якщо даний номер не знаходиться в чорному списку мережа дає дозвіл на роботу з відповідним апаратом [1, с.142-144].

Окрім розглянутих процесів ідентифікації та аутентифікації абонента є ще один важливий з точки зору інформаційної безпеки механізм – шифрування інформації в мережі стільникового зв'язку. Для реалізації даного механізму використовуються вже згадувані

вище випадкове число RAND і ключ авторизації абонента Ki, які за алгоритмом A8, що також знаходиться в SIM карточці, визначають 64-бітний ключ шифрування Кс. Даний ключ використовується для шифрування і розшифрування при передачі даних між мобільною станцією та базовою станцією. Додатковий рівень секретності забезпечується періодичною зміною ключа. Ключ Кс разом із номером TDMA фрейму за алгоритмом A5 визначають 114-бітну послідовність, яка в подальшому накладається за допомогою операції XOR на два 57-бітних блоки пакету даних (рис.2). Алгоритм A5 виконує шифрування потоку даних трьох синхронізованих лінійних регістрів із зворотнім зв'язком степенів 19, 22 і 23. В цих регістрах сигнал зворотного зв'язку формується лінійною логічною схемою, відбувається перетворення згортки зовнішньої вхідної послідовності з послідовністю комбінаційних коефіцієнтів. Якщо зобразити зовнішній вхідний сигнал у вигляді многочлена, в якому степені незалежної змінної означають часову затримку, а комбінаційні коефіцієнти аналогічним чином зобразити в вигляді другого многочлена, то регістр із лінійним зворотнім зв'язком можна розглядати як пристрій ділення першого многочлена на другий. При відсутності зовнішньої вхідної послідовності регістр може сам по собі використовуватися для формування m - послідовностей (періодична послідовність максимальної довжини, яка використовується в якості псевдовипадкової послідовності). Послідовність максимальної довжини чи m - послідовність рівна 2n-1, де n – степінь реєстру зсуву. Для формування m – послідовності зовнішня вхідна послідовність LFSR повинна відповідати примітивному многочлену степеня n по модулю 2. Робота таких трьох регістрів і лежить в основі алгоритму шифрування потоків даних A5. Управління синхронізацією являє собою порогову функцію від середніх бітів для кожного із трьох регістрів зсуву. Сума степенів всіх трьох регістрів рівна 64, 64–бітний ключ використовується для ініціалізації вмісту регістрів зсуву, а 22-бітний номер TDMA фрейму подається на регістри зсуву. Два 114-бітних потоки ключів генеруються для кожного TDMA фрейму, для того щоб в подальшому накласти їх операцією XOR на вхідні і вихідні трафік канали. Стверджується, що алгоритм A5 має ефективну довжину ключа – 40 біт.

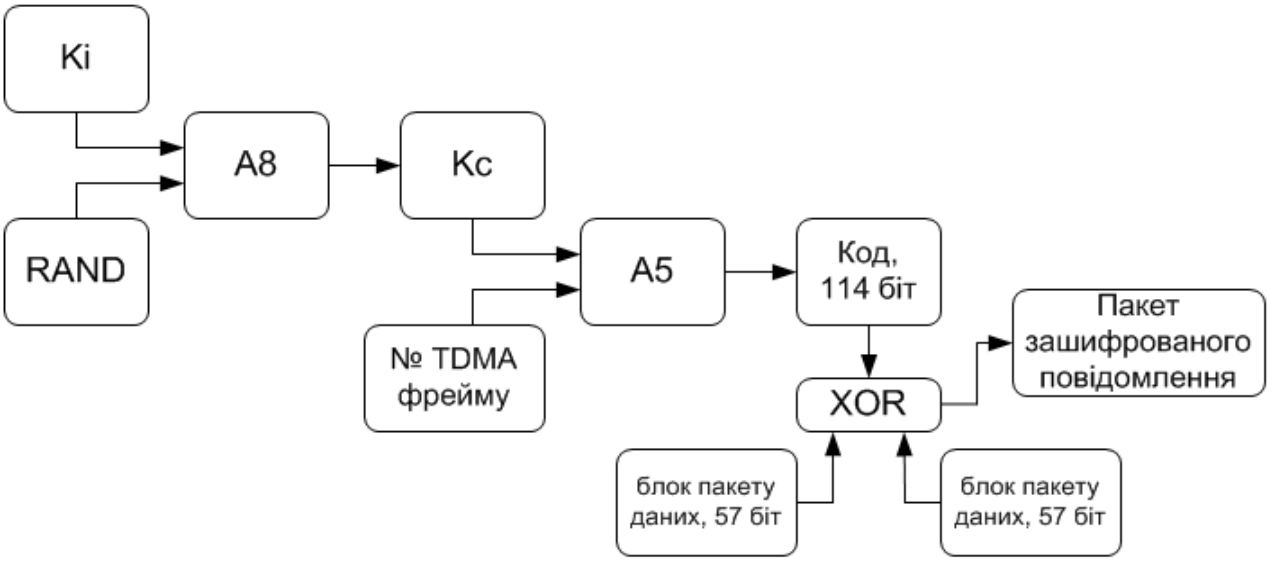

Рис.2. Процедура шифрування даних абонента в стандарті GSM

Певний час функціонували два варіанти алгоритму A5, а саме A5/1 та A5/2. В 2002р. асоціація GSM затвердила новий алгоритм шифрування – A5/3, який був розроблений спільними зусиллями комітету безпеки асоціації GSM, організацією 3GPP і комітетом з алгоритмів безпеки Європейського інституту телекомунікаційних стандартів ETSI. Причому новий алгоритм можна використовувати як в звичайних 2G мережах так і в модернізованих

2,5G (GPRS) та 3G (HDCSD і EDGE). Алгоритм A5/3 реалізований на апаратному рівні і враховує особливості обробки сигналів в мобільних телефонах, причому шифрується не лише голосовий трафік, але і дані, що передаються по безпровідному каналу.

Все більшої популярності останнім часом набирає стандарт із кодовим розділенням каналів CDMA. Безпека абонентської інформації в даному стандарті базується на чотирьох фундаментальних елементах: 1) функція CAVE (Cellular Authentification and Voice Encryption) - функція перемішування, що використовується в протоколах аутентифікації запит - відповідь і для генерації ключів; 2) операція XOR - повторювана маска, що накладається на голосові дані для гарантування безпеки їх передачі; 3) шифр ORYX - потоковий шифр, призначений для використання в послугах бездротового доступу до даних; 4) шифр CMEA (Control Message Encryption Algorithm) - простий блоковий шифр, що використовується для шифрування службових повідомлень. Криптографічні протоколи стандарту CDMA грунтуються на 64-бітному аутентифікаційному ключі A-key і серійному номері мобільного телефону ESN (Electronic Serial Number). Для аутентифікації абонента при реєстрації мобільного телфону в мережі а також наступної генерації допоміжних ключів, що приймають участь в забезпеченні конфіденційності передачі голосових даних і кодованих повідомлень використовується випадкове двійкове число RANDSSD (Random Shared Secret Data), що генерується аутентифікаційним центром AC (Authentification Center) реєстру власних абонентів HLR (Home Location Register). Ключ A-key запрограмований в мобільному телефоні а також зберігається в центрі аутентифікації мереж. Стандартизований алгоритм шифрування CAVE використовується для генерації 128 бітного підключа SSD. Таким чином ключ A-key, серійний номер ESN і згенероване мережею випадкове число RANDSSD подаються на вхід алгоритму CAVE, який в свою чергу генерує допоміжний ключ SSD. Цей ключ складається з двох частин: SSD_A, що використовується для створення аутентифікаційного цифрового підпису, і SSD_B, що використовується при генерації ключів для шифрування голосових даних і службових повідомлень. Ключ SSD може бути переданий іншій мережі при роумінгу абонента для забезпечення локальної аутентифікації. Новий SSD може бути згенерований при поверненні абонента в домашню мережу або зміні гостьовій мережі в роумінгу. Мережа генерує і розсилає відкрито в ефір випадкове число RAND, а мобільні пристрої, що реєструються в мережі, використовують його як вхідні дані для алгоритму CAVE, який генерує 18-бітний цифровий підпис AS (Authentification Signature), і посилає його на базову станцію. Цей цифровий підпис звіряється в центрі комутації MSC (Mobile services Switching Center) з підписом згенерованим самим центром комутації для перевірки легітимності абонента [5, с.122-127]. При цьому випадкове число RAND може бути як однаковим для всіх користувачів, так і заново генеруватися кожного разу, використання конкретного методу визначається оператором. Перший варіант забезпечує дуже швидку аутентифікацію.

Як мобільний телефон так і мережа ведуть 6-бітові лічильники дзвінків, що забезпечує можливість детектування двійників: для цього достатньо лише контролювати відповідність значень лічильників на телефоні і в центрі комутації MSC. Секретний ключ A-key може бути перепрограмованим при необхідності, але у разі його зміни інформація на мобільному телефоні і в регістрі мережі HLR повинна бути синхронізована. Зміна ключа може бути прошита на заводі, дилером в точці продажу, абонентом через інтерфейс телефону, а також за допомогою спеціального сервісу OTASP (Over The Air Aervice Provisionig). Даний сервіс використовує в процесі передачі 512 бітний алгоритм узгодження ключів Діффі-Хелмана, що гарантує достатньо високий рівень безпеки. OTASP забезпечує легкий спосіб зміни ключа A-key мобільного телефону на випадок появи в мережі двійника мобільного телефону, оскільки така зміна автоматично спричинить за собою відключення послуг двійника мобільного телефону і повторне включення послуг легітимного абонента. Таким чином секретність ключа A-key є практично найважливішою компонентою безпеки CDMA системи.

Безпека передачі голосових даних, інформації та службових повідомлень досягається наступним чином. Мобільний телефон використовує допоміжний код SSD_B і алгоритм CAVE для генерації маски PLCM (Private Long Code Mask), 64-бітного підключа CMEA (Cellular Message Encryption Algorithm) і 32-бітного DATA-key. Маска PLCM використовується як мобільним телефоном, так і мережею для зміни характеристик Long Code Mask. Цей модифікований Long Code використовується для шифрування голосових даних, що підвищує таємність їхньої передачі. PLCM не шифрує інформацію, вона просто замінює відомі величини, що використовуються в кодуванні CDMA сигналу секретними величинами, відомими тільки мобільному телефону і мережі. Таким чином підслуховування розмов без знання даної маски є надзвичайно складним завданням. Більш того, мобільний телефон і мережа використовують CMEA і модифікований E_CMEA алгоритми для шифрування і дешифрування службових повідомлень при передачі їх по ефіру. Окремий DATA-key і алгоритм шифрування ORYX використовується мобільним телефоном і мережею для шифрування і дешифрування потоку інформації по каналу зв'язку CDMA. Описаний процес зображений на рис.3.

Розглянуті нами стандарти мобільного зв’язку забезпечують захист даних клієнта за допомогою вбудованих криптографічних механізмів. Такого захисту достатньо щоб гарантувати безпеку від випадкових або аматорських прослухувань, але результати досліджень відомих криптографів Елада Баркана, Елі Біхама та Натана Келлера показали що існуючі алгоритми не є абсолютно стійкими і при наявності необхідної апаратури можуть бути розкриті в доволі короткі проміжки часу.

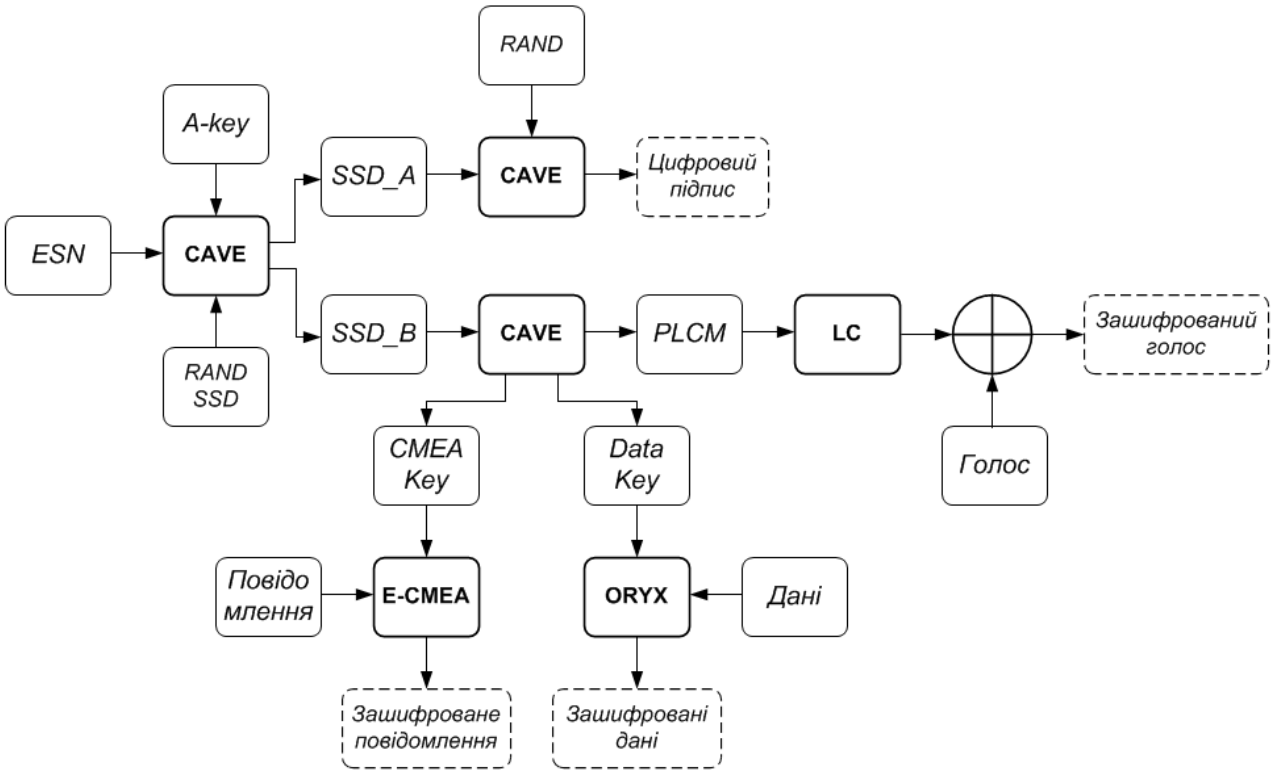

Рис.3. Процес шифрування інформації абонента в стандарті CDMA

З метою вирішення даної задачі були розроблені додаткові засоби захисту:. скремблери у вигляді мініатюрних приставок до телефону і окремі, незалежні пристрої - криптосмартфони з вбудованим процесором для шифрування інформації. Принцип дії скремблерів полягає в здійсненні переміщень відрізків мовного сигналу в часовій області за

певним алгоритмом на стороні передавача і зворотне відновлення сигналу на стороні приймача. Середній діапазон цін на дані пристрої коливається в межах від 300 до 400 у.о., що робить їх достатньо доступними але при цьому наявні наступні недоліки: низький рівень захисту, зумовлений простотою застосовуваних алгоритмів; спричиняють затримку в часі сигналу до 100мс.; призводять до значних втрат в розбірливості мовного повідомлення; незручні у використанні через наявність додаткового пристрою і можливість застосування лише через гарнітуру. Криптосмартфони виконують шифрування інформації за допомогою спеціального крипто чіпу, що реалізує певний криптографічний алгоритм, переважно з відкритим ключем довжиною порядку 256 біт. Забезпечують значно вищий рівень захисту інформації у порівнянні зі скремблерами, але відповідно мають відчутно вищу вартість 2000 – 2500 у.о., і обмежений вибір модельного ряду.

Серед наявних на сьогоднішній день додаткових засобів захисту немає оптимального варіанту з точки зору поєднання доступної вартості, зручності використання і достатнього рівня надійності. Тому задача по вдосконаленню захисту інформації абонента мобільної мережі є досі нерозв'язаною і потребує подальших досліджень. Центральним елементом системи захисту однозначно повинен стати один із стійких криптографічних алгоритмів із забезпеченням можливості абонента впливати на формування ключів шифрування. Дана система має мати програмну реалізацію і підтримуватися широким модельним рядом мобільних терміналів. Виконати поставлені вимоги можна при використанні телефонів, які володіють власною операційною системою і дозволяють проводити певні модифікації програмного забезпечення. Мова йде про смартфони, які оснащені процесорами з достатньо високою швидкодією і працюють на платформі однієї із мобільних операційних систем: Symbian OS, Windows Mobile, Android. Це дає змогу реалізувати програмні рішення для вирішення поставленої задачі. Отже можемо запропонувати наступний напрямок розвитку системи інформаційної безпеки абонента, який полягатиме в розробці програмної аплікації, що реалізує шифрування потоку даних за допомогою криптографічного перетворення. Аплікація створюється в середовищі програмування, яке підтримується конкретною мобільною операційною системою (наприклад C++ для Symbian OS чи .NET Compact Framework для Windows Mobile) [4, с.14-15]. Важливим питанням є вибір крипто алгоритму, який лежатиме в основі програмних модифікацій даних. Він має забезпечувати достатньо високий рівень стійкості захисту і при цьому не вимагати значних часових затрат, адже шифрування здійснюватиметься в режимі реального часу. Відповідно до наведених вимог оптимальним є симетричний алгоритм блочного шифрування AES. Розмір блоку в даному алгоритмі є фіксований і становить 128 біт, а довжина ключа може бути вибрана серед значень 128, 192, 256 біт. Програма повинна мати зручний користувацький інтерфейс з меню включення/виключення режиму шифрування і полем для введення даних, на основі яких генеруватимуться криптографічні ключі. Це забезпечить абоненту повний контроль над процесом забезпечення захисту його інформації. Аплікація працюватиме на програмному рівні після перетворення голосових даних абонента в цифровий потік (рис.4).

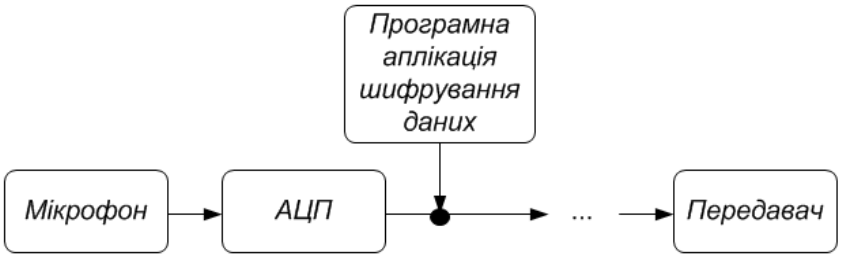

Рис.4. Місце криптографічної аплікації в процесі обробки голосових даних

На приймальній стороні відбуватиметься зворотне програмне перетворення сигналу і після розшифрування він подаватиметься на ЦАП і далі на динамік телефону слухача. Використання достатньо швидкого алгоритму AES дозволить звести затримки сигналу в часі до мінімуму, що не створюватиме незручностей при розмові. Щодо питання надійності такого захисту, то авторитет алгоритму AES, який є одним із найпоширеніших і найбільш стійких криптографічних протоколів, із використанням ключа довжиною 256 біт дозволить забезпечити достатній рівень безпеки інформації абонента.

Отже стандартні засоби захисту, які використовуються в відомих на сьогоднішній день протоколах мобільного зв'язку, забезпечують лише базовий рівень безпеки здатний протистояти аматорським спробам несанкціонованого перехоплення інформації. Для підвищення рівня безпеки додатково можуть використовуватися спеціальні пристрої - скремблери у вигляді приставок до телефону або окремі абонентські термінали - криптосмартфони з вбудованим процесором для шифрування інформації. Перші мають доступну ціну, але невисоку якість, а другі володіють значно кращими показниками, але в свою чергу відзначаються достатньо високою вартістю і вузьким модельним рядом. Тому в якості альтернативного напрямку розробки системи захисту абонентської інформації була запропонована модель клієнто-орієнтованої програмної аплікації, яка орієнтована на використання у мобільних телефонах із власною операційною системою. В основі роботи даної аплікації лежить криптографічне перетворення оцифрованого голосу абонента за допомогою симетричного блочного алгоритму AES з довжиною ключа 256 біт. Клієнтоорієнтованість такого рішення полягає в можливості абонента самому визначати коли використовувати захищений калан зв'язку і впливати на формування крипто-ключів, а отже повністю контролювати процес забезпечення конфіденційності розмови.

Література

1. Громаков Ю.А. Стандарты и системы подвижной радиосвязи.- М.:ЭкоТрендз Ко, 1998. – 240 с.

2. Громаков Ю.А., Северин А.В., Шевцов В.А. Технологии определения местоположения в GSM и UMTS.- М.:ЭкоТрендз Ко, 1998. – 140 с.

3. Андрианов В.И., Соколов А.В. Средства мобильной связи.- Санкт-Петербург:БХВ, 2001. – 256 с.

4. Климов А.П. Программирование КПК и Смартфонов на .NET Compact Framework.- СПб.: Питер, 2007.- 320 с.

5. Шахнович И.В. Современные технологии беспроводной связи.- М.:Техносфера, 2006. – 288 с.

Надійшла: 0.03.11

Рецензент: д.т.н., проф. Кузнєцов Г.В.