УДК 004.4

АЛГОРИТМ ДОДАТКОВОГО КРИПТОГРАФІЧНОГО ЗАХИСТУ ГОЛОСОВИХ ДАНИХ

Гончарова С. В., Могилевич Д. І.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: goncharovasabina@gmail.com

Additional cryptographic algorithm protection of voice data

This article describes the algorithm additional cryptographic protection of voice data in mobile network. The results of testing pseudo-random pattern generator are presented.

У наш час дуже велика кількість інформації передається через мобільні мережі, більшість з неї є голосовою. Об'єми інформації, що передаються, збільшуються весь час, деяка частина з цієї інформації є конфіденційною. Додатковий криптографічний захист голосових даних в мобільній мережі дозволить захистити інформацію, що передається, від зловмисника.

В роботі [1] розглянуто роботу різних програмних засобів додаткового криптографічного захисту голосових даних в мобільних мережах. Всі програмні засоби у своїй структурі за основу беруть протоколи VoIP, а саме, ZRTP та SRTP. Ці протоколи дозволяють проводити автентифікацію між абонентами та використовувати різні, підтримувані протоколами, криптографічні алгоритми в різних режимах для забезпечення захисту голосових даних. Протоколи ZRTP та SRTP, є вразливими, але деякі компанії, такі як Silent Circle, додають перевірки для усунення цих вразливостей, але це не повністю вирішує проблему і атаки стають лише менш ймовірними [2, 3].

Виходячи з вищесказаного, для захисту голосової інформації, було вирішено створити власне програмне забезпечення, як альтернативу існуючим. Без використання ZRTP протоколу, а використовуючи звичайні мережеві протоколи, з більш швидким алгоритмом шифрування голосових даних та нецентралізованою системою зберігання даних про користувачів.

Алгоритм працює в режимі клієнт – сервер, але кожен абонент виступає одночасно і клієнтом, і сервером. З'єднання створено за допомогою технології сокетів.

Програмне забезпечення є багатопоточним. Перший потік створюється при запуску програми, це сервер, який дозволяє іншим користувачам робити виклик на даний пристрій. Другий потік створюється під час виклику чи прийому виклику, це клієнт який з'єднується з сервером іншого абонента. Ще в двох потоках працює запис голосу у буфер та відтворення голосу, а також, окремим потоком працює процес шифрування. Шифрування здійснюється методом гамування.

Коли абонент з'єднується з іншим для розмови, то по каналу передаються секретні ключі для шифру гамування за допомогою асиметричної криптосистеми RSA.

Якщо процедура пройшла успішно, то починається розмова. Розмова йде за допомогою багатопоточного використання класів AudioTrack та MediaRecorder.

Використовуючи MediaRecorder, голосові дані з мікрофону записуються у буфер, де над цими даними проводиться шифрування методом гамування, після цієї операції дані передаються через мережу. Коли інший абонент отримує дані, він їх розшифровує та передає буфер до AudioTrack, який відтворює ці данні у звук з динаміка для розмов.

Схема роботи алгоритму показана на рис.1.

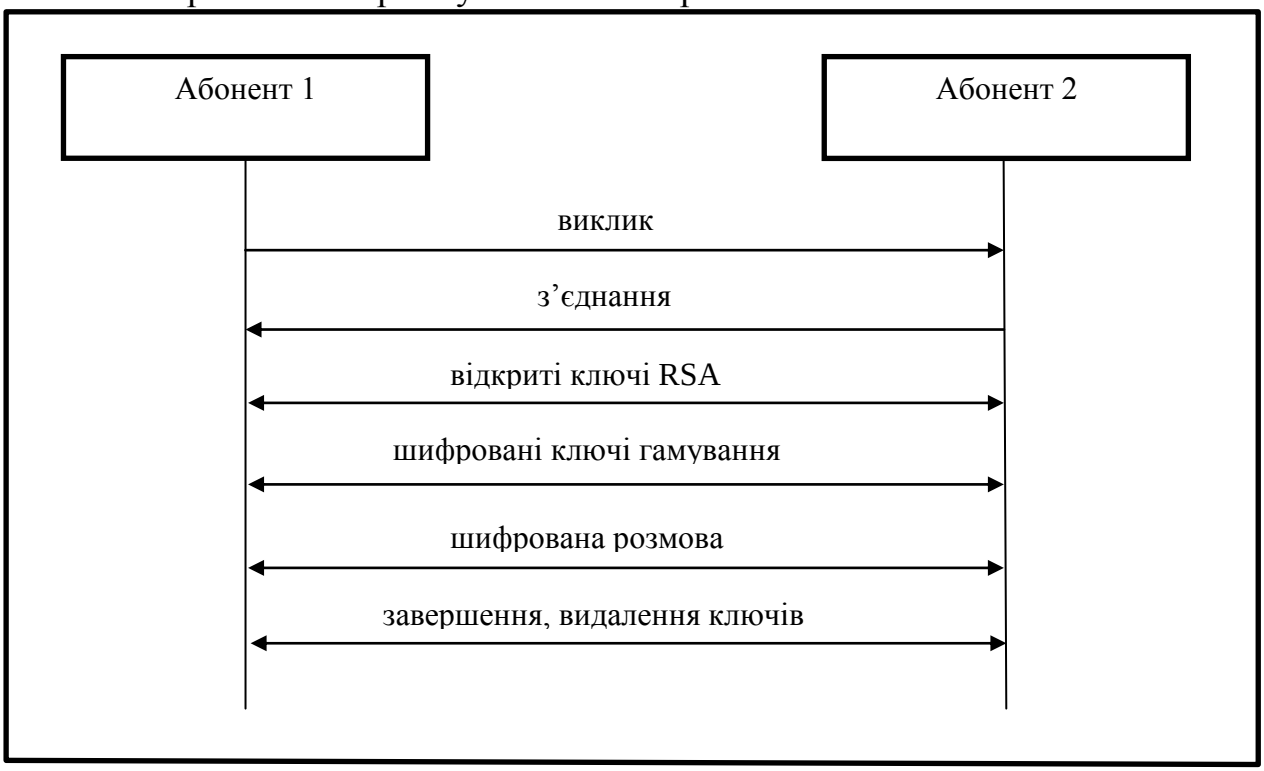

Рис. 1. Схема роботи алгоритму

Для генерації ключів було розроблено власний генератор псевдовипадкових послідовностей. Схема роботи генератора псевдовипадкових послідовностей показана на рис.2.

В якості джерела ентропії даного генератора псевдовипадкових послідовностей використовуються крайні праві дробової частини значень положень гіроскопу та акселерометру, зафіксовані в момент генерації. Гіроскоп та акселерометр фіксують положення в просторі та кут нахилу. Вони є достатньо випадковими так, як рухи кожної людини різні та гіроскопи і акселерометри в сучасних смартфонах настільки точні, що фіксують зміни, навіть, при вібрації руки людини. Кількість біт ентропії – 128, вони беруться по 32 крайніх біти з значення акселерометра та значень осей X, Y та Z гіроскопа.

Після отримання ентропії, ця послідовність подається на вхід булевій функції, яка має вигляд:

$$f(x_1, x_2, x_3, x_4) = x_2 \oplus x_4 \oplus x_2x_3 \oplus x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \quad (1)$$

Це робиться для того, щоб зробити неможливим знаходження джерела ентропії сторонньою особою і, як наслідок, зробити можливим підробку

ключів. Після використання булевої функції, вхідна послідовність скорочується до 32 біт. Щоб збільшити розмір входу використовується стандартний метод генерації псевдовипадкових чисел, а саме лінійно конгруентний.

Рис. 2. Схема роботи генератора псевдовипадкових послідовностей

Генератор побудовано за схемою Геффе, але оскільки генератор Геффе не є стійким проти кореляційної атаки, використовуються не звичайні регістри зсуву з лінійним зворотнім зв’язком, а з доданою нелінійністю.

Над генератором псевдовипадкових послідовностей було проведено тестування. По-перше набір тестів DIEHARD на випадковість, по-друге тест на швидкодію генерації [4]. Генератор показав дуже добрі статистичні результати.

В роботі було проаналізовано недоліки різних програмних засобів додаткового криптографічного захисту голосових даних в мобільних мережах. Для усунення цих вразливостей було запропоновано алгоритм додаткового криптографічного захисту голосових даних. Для забезпечення роботи алгоритму було створено генератор псевдовипадкових послідовностей. Генератор протестовано на швидкодію та випадковість. Доведено, що генератор є захищеним від атак.

Література

1. Огляд на засоби криптографічного захисту [Електронний ресурс]. – Режим доступу : http://encrypted-phone-review.com/
2. Вразливості ZRTP [Електронний ресурс]. – Режим доступу : http://blog.azimuthsecurity.com/2013/06/attacking-crypto-phones-weaknesses-in.html
3. Офіційна сторінка SilentCircle [Електронний ресурс]. – Режим доступу : https://silentcircle.com
4. DIEHARD документація [Електронний ресурс]. – Режим доступу : http://stat.fsu.edu/pub/diehard/