Програмне забезпечення шифрування мовних повідомлень у GSM каналі

Достaвалов В. В.
Наукові керівники: Швець В. А. Цигвінцев Р.Д.
НН ІПДС НАУ
м. Київ, Україна
AceFire-fist@mail.ru

***Анотація* — Програмне забезпечення шифрування мовних повідомлень у GSM каналі шляхом скремблювання мовного сигналу за допомогою програмного забезпечення, та алгоритму побудованого на основі кодів Фібоначчі.**

Ключові слова — Криптографія, скремблер, шифрування, Фібоначчі код, акустична інформація, шифр.

I. Вступ

Розвиток криптографії [1] в наш час, в основному, пов'язано з широким використанням комп'ютерних мереж і зокрема глобальної мережі Інтернет [2], через яку передають дуже великі обсяги інформації військового, державного, комерційного та приватного змісту, не допускає можливості доступу до неї сторонніх осіб, а з іншого, поява нових потужних обчислювальних ресурсів уможливила дискредитації ряду криптографічних систем. Незважаючи на широке впровадження автоматизованих і комп'ютеризованих систем обробки інформації, людська мова залишається одним з найважливіших шляхів інформаційної взаємодії. Ось чому так важливо розробити програмне забезпечення, яке допоможе зберегти мовну інформацію в цілісності, збільшити ступень захищеності та зменшити можливість отримання її сторонніми людьми.

II. Застосування маскуючих систем

Основними властивостями і характеристиками маскуючих систем (далі скремблерів), завдяки яким вони набули широкого використання та популярності у сучасному світі є:

- досить висока якість відновленої мови;
- невисока складність реалізації;
- наявність залишкової інформації в закритому сигналі, яка може бути використана нападаючою стороною.

Цифрові скремблери [3] не передають будь-яку часту початкового мовного сигналу, як роблять це аналогові системи маскування [4]. Мовні компоненти кодуються в цифровий потік даних, який змішується з псевдовипадковою послідовністю, що виробляється ключовим генератором по одному з криптографічних алгоритмів, і отримане таким чином закрите мовне повідомлення передається за допомогою модему в канал зв'язку, на приймальному кінці якого виробляються зворотні перетворення з метою отримання відкритого мовного сигналу. Такі системи називають кодерами. Це процедури, що представляють мовний сигнал моделлю; параметри моделі, що змінюються в часі, шифрують як потік даних і передають за допомогою модемів.

Перевага представленої інноваційної ідеї полягає в тому, що розроблена програма може бути встановлена на будь якому пристрої, тобто перевага такої інновації у відмінності від попередніх реалізацій – це мобільність і доступність. Головною відмінністю є те, що розроблену програму можна встановити будь де, і будь коли, при цьому майже не витративши на це ресурси, при цьому, забезпечивши собі надійних захист передачі мовної інформації.

Характеристики програми, дозволяють майже у реальному часі закодувати мовне повідомлення й передати його без помилок на інший пристрій з його подальшим розковуванням, й перетворенням у первинний вид мовного сигналу.

Система може бути інтегрована в усі операційні системи які відомі на даний момент, не важливо мобільні це пристрої чи стаціонарні комп’ютери. Ця характерна особливість була досягнута за рахунок універсальності коду та використаної мови програмування.

Список використаних джерел

[1] Венбо Мао. Сучасна криптографія. Теорія та практика. - СПб .: Вільямс, 2005. 239 с.
[2] Конахович Г. Ф., Климчук В. П., Павук С. М. Захист інформації в телекомунікаційних системах. - До.: "МК-Пресс", 2005. - 288 с.
[3] Цифрові і аналогові системи передачі: Підручник для вузів / Іванов В.І., Гордієнко В.М., Попов Г.Н. та ін.; Під ред.Іванова В.І. .-М .: Радио и связь, 2007.-232с .: іл. .-Бібліогр.: С.229-230.- ISBN 5-256-01226-6.
[4] Дружинін В.В., контори Д.С. Системотехніка. - М .: «Радіо і зв'язок», 1985. -200 с.