СУЧАСНА МОЛОДЬ В СВІТІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Матеріали
ІІ Всеукраїнської науково-практичної інтернет-конференції молодих вчених та здобувачів вищої освіти

присвяченої Дню науки

14 травня 2021 р.

Херсон

Міністерство освіти і науки України
Херсонський державний аграрно-економічний університет
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Вінницький національний медичний університет
ім. М. І. Пирогова
Кременчуцький національний технічний університет
ім. Михайла Остроградського
Вінницький національний технічний університет
Херсонський національний технічний університет
Сумський державний університет
Херсонська державна морська академія

Матеріали
ІІ Всеукраїнської науково-практичної інтернет-конференції молодих вчених та здобувачів вищої освіти «*СУЧАСНА МОЛОДЬ В СВІТІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ*»

присвячена Дню науки

14 травня 2021р.
Херсон

УДК 004.7+004.05]:005.5](06)
С 91

«Сучасна молодь в світі інформаційних технологій»: матеріали II Всеукр. наук.-практ. інтернет-конф. молодих вчених та здобувачів вищої освіти, присвяченої Дню науки (14 травня 2021р., м. Херсон) / за ред. Н.В. Кириченко, Г.О. Димової та ін. – Херсон: Книжкове видавництво ФОП Вишемирський В.С., 2021. – 212 с.

С91

ISBN 978-617-7941-23-0 (електронне видання)

Конференція «Сучасна молодь в світі інформаційних технологій» присвячується Дню науки. Метою конференції є висвітлення розробок, результатів досліджень та досягнень молодих вчених України та здобувачів вищої освіти при розробці, використанні та впровадженні інформаційних технологій в різних галузях науки.

Тези наукової конференції містять результати наступних досліджень: менеджмент інформаційних технологій; прогнозування соціально-економічних процесів за умов невизначеності та ризику; управління проектами на підприємствах агропромислового комплексу; сучасні тенденції розвитку інформаційних технологій; впровадження інновацій та сучасних технологій; інформаційні технології в науці, освіті, економіці, логістиці, туристичній сфері, транспорті; математичні методи, моделі, інформаційні системи і технології в економіці; моделювання та оптимізація інформаційних систем; інвестиційне проектування в різних сферах суспільного життя; інформаційно-аналітичні та інформаційно-керуючі системи; системи відображення інформації і комп'ютерні технології; використання нових інформаційних технологій в медичній галузі; новітні технології в енергетичних системах та в галузі енергозбереження.

Роботи друкуються в авторській редакції, в збірці максимально зменшено втручання в обсяг та структуру відібраних до друку матеріалів. Редакційна колегія не несе відповідальність за достовірність інформації, що надано в рукописах, та залишає за собою право не розподіляти поглядів деяких авторів на ті чи інші питання.

АДРЕСА ОРГКОМІТЕТУ

73006, Україна, м. Херсон, вул. Стрітенська, 23
Херсонський державний аграрно-економічний університет, економічний факультет
кафедра менеджменту та інформаційних технологій
e-mail: conference.mywit@gmail.com, matematika_ek2017@ukr.net

УДК 004.7+004.05]:005.5](06)

ISBN 978-617-7941-23-0 (електронне видання)

СЕКЦІЯ «МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ, ІНФОРМАЦІЙНІ СИСТЕМИ І ТЕХНОЛОГІЇ В ЕКОНОМІЦІ»

СЕКЦІЯ «МОДЕЛЮВАННЯ ТА ОПТИМІЗАЦІЯ ІНФОРМАЦІЙНИХ СИСТЕМ»

СЕКЦІЯ «ІНФОРМАЦІЙНО-АНАЛІТИЧНІ ТА ІНФОРМАЦІЙНО-КЕРУЮЧІ СИСТЕМИ»

СЕКЦІЯ «СИСТЕМИ ВІДОБРАЖЕННЯ ІНФОРМАЦІЇ І КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ»

УДК 004.056.55

Г.О. Димова, І.А. Швидченко
Херсонський державний аграрно-економічний університет
anndymova@gmail.com

РЕАЛІЗАЦІЯ КОМП'ЮТЕРНОЇ ПРОГРАМИ ДЛЯ ДОСЛІДЖЕННЯ МЕТОДІВ ШИФРУВАННЯ ДАНИХ В РЕАЛЬНОМУ ЧАСІ

Технічні канали витоку інформації є джерелом інформації для технічної розвідки, що здійснює добування інформації за допомогою технічних засобів. Тому проблема захисту інформації від технічної розвідки має особливу актуальність. Для дослідження роботи потокових методів шифрування даних реального часу створена комп'ютерна програма на основі мови програмування Delphi. Програма по закриттю мовних сигналів розроблена шляхом реалізації в смуговому скремблері швидкого перетворювання Фур'є.

Скремблер (scrambler) – це пристрій, призначений для шифрування вихідного і дешифрування вхідного сигналу [1]. Для організації захищеного сеансу зв'язку необхідна наявність двох скремблерів, у кожного абонента який бере участь в переговорах – свій. Принцип дії скремблера полягає в наступному: голосову інформацію скремблер на стороні відправника шифрує за специфічним алгоритмом, після чого відправляється в канал зв'язку. Скремблер приймаючої сторони повинен бути налаштований на використання того ж криптографічного алгоритму, він дешифрує отриману інформацію і передає абоненту у вигляді голосового сигналу.

Перехопити такий сигнал можливо, але його дешифрування вимагає високовартісного обладнання, підготовленого фахівця-криптоаналітика і часу для проведення криптографічного аналізу. Причому результат не гарантований. І навіть у разі успішного розкриття повідомлення, процес дешифрування може зайняти кілька місяців, за цей час отримана інформація сильно втратить актуальність [2].

Сенс скремблювання полягає в отриманні послідовності, в якій статистика появи нулів і одиниць наближається до випадкової, що дозволяє задовольняти вимогам надійного виділення тактової частоти і постійної, зосередженої в заданій області частот спектральної щільності потужності сигналу, що передається.

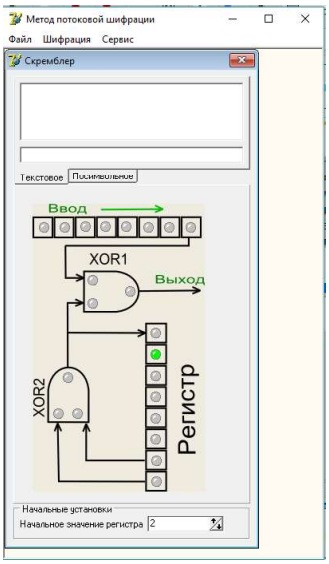
Скремблювання (від англійського слова to scramble – перемішувати) проводиться на передавальній стороні за допомогою пристрою – скремблера, що реалізує логічну операцію підсумовування по модулю вихідного і перетворюваного псевдовипадкового двійкових сигналів. На приймальній стороні здійснюється зворотна операція – дескремблювання пристроєм, що називається дескремблером. Дескремблер виділяє з прийнятої вихідну послідовність. Основною частиною скремблера є генератор псевдовипадкової послідовності у вигляді лінійного n-каскадного регістра зі зворотними зв'язками, яка формує послідовність максимальної довжини $(2^n - 1)$. Скремблер може забезпечити дуже високий ступінь захисту, але за умови використання ефективного криптографічного алгоритму [2, 3].

Принцип роботи скремблера – це зміщення шляхом XOR (АБО, що виключає) потоків бітів з генератором псевдовипадкових значень (бітів) XOR (АБО, що виключає) [4]. Отримуємо на виході випадкове значення, яке відмінно декодується другим генератором, що дає таку ж псевдовипадкову послідовність.

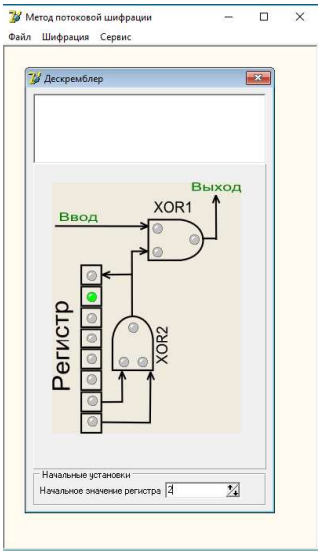
Практичною метою роботи програмного додатку, є демонстрація методу потокової шифрації, і наочна демонстрація шифрування даних в реальному часі методами: скремблювання, дескремблювання і комбінованим алгоритмом «Гібрид». Кожен метод можна розглянути у вигляді окремої процедури.

«Скремблер» дозволяє послати повідомлення, перед цим зашифрувавши його. Вікно "скремблер" дозволяє зашифрувати повідомлення методом шифрування скремблювання для цього вся інформація «розбита» на біти, потім вона шифрується регістром, який насправді є ще і псевдовипадковим генератором. Скремблер (джерело) і Дескремблер (одержувач) запускаємо з двох програмних проектів, тому що дві програми на одному програмному

продукті, з однаковими портами не працюватимуть як скремблер і дескремблер. З скремблера буде йти відправка даних, але на дескремблері не буде відображення отримання даних. Якщо записати повідомлення в рядку для відправки і зробити відправку, то повідомлення спочатку відбивається в загальному полі повідомлень. В «Лозі скремблеру-вхід» відбивається посилається текст (рис. 1а). На іншому проекті – дескремблері відбивається отримане повідомлення, а лог «дескремблер-вихід» відображає правильність отриманого повідомлення, в порівнянні з відправленим (рис.1б). Випадкове символьне значення для шифрації даних можна переглянути включивши прапорець, зробити команду введення, переглянувши передачу даних скремблер і отриманням цих даних на дескремблері, наочно. Також можна переглянути показ передачі даних більш повільніше, при цьому необхідно увімкнути прапорець «анімацію, показ із затримкою» (рис. 2).



а) скремблер



б) дескремблер

Рис. 1 – Вигляд вікна проекту

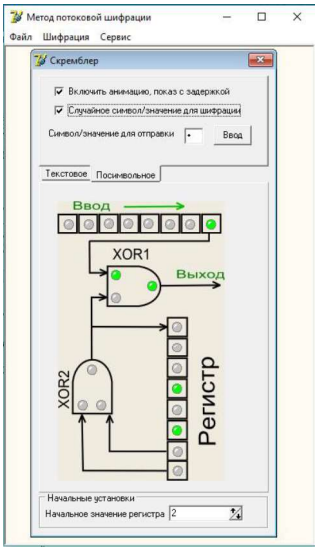


Рис. 2 – Показ з затримкою і випадкового значення

Комбінований алгоритм «Гібрид» дозволяє також використовувати технологію спілкування в режимі реального часу шифрування даних, яка називається онлайнової. Алгоритм "Гібрид" запускаємо двома програмними проектами і з різними портами. Один з портів буде служити джерелом, інший приймачем. Хост-адресу опишемо і позначимо як "localhost", адреса локальної мережі.

Протокол UDP (User Datagram Protocol, RFC-768) є одним з основних протоколів, розташованих безпосередньо над IP. Протокол UDP не вимагає з'єднання з віддаленим модулем UDP («беззв'язковий» протокол). До заголовку IP-пакета UDP додає поля: порт відправника і порт одержувача, які забезпечують мультиплексування інформації між різними прикладними процесами, а також поля: довжина UDP-дейтограми і контрольна сума, що дозволяють підтримувати цілісність даних. Таким чином, якщо на рівні IP для визначення місця доставки пакету використовується адреса, на рівні UDP – номер порту. Хоча протокол не гарантує доставки, але передбачається, що ймовірність втрати пакета досить мала.

ЛІТЕРАТУРА:

1. Блейхут Р. Быстрые алгоритмы цифровой обработки сигналов. Москва: Мир, 1989. 448 с.
2. Хорев А.А. Способы и средства защиты информации. – Учебное пособие. Москва: Радио и связь, 1998. 316 с.
3. Ярочкин В. И. Информационная безопасность. Учебник для студентов вузов. Москва: Академический Проект, 2003. 640 с.
4. Биячуев Т.А. Безопасность корпоративных сетей. Санкт-Петербург: СПбГУ ИТМО, 2004. 161 с.

Наукове електронне видання

ХДАЕУ Менеджмент та ІТ – 2021

Матеріали
ІІ Всеукраїнської
науково-практичної інтернет-конференції
молодих вчених
та здобувачів вищої освіти
«Сучасна молодь в світі інформаційних технологій»
присвячена Дню науки

Праці конференції

ISBN 978-617-7941-23-0 (електронне видання)

Підписано до видання 12.05.2021 р. Формат 60×84/8.
Гарнітура Times.
Ум. друк. арк. 17,11. Обл.-вид. арк. 18,40.
Замовлення № 1972.

Книжкове видавництво ФОП Вишемирський В.С.
Свідоцтво про внесення до державного реєстру суб'єктів видавничої справи:
серія ХС №48 від 14.04.2005
видано Управлінням у справах преси та інформації
73000, Україна, м.Херсон, вул. Соборна, 2,
тел. 050-514-67-88, 080-133-10-13,
e-mail: printvvs@gmail.com