План лабораторного заняття № 7
Тема № 3 “Безпека в інформаційних мережах”

Навчальний час: 4 год.
Міжпредметні зв’язки: навчальна дисципліна “Захист інформації в інформаційних системах” взаємопов’язана з такими дисциплінами як “Економіко-математичне моделювання”, “Інформатика” та ін.

Мета і завдання лабораторного заняття: ознайомлення з симетричними методами шифрування повідомлень.

Питання для перевірки базових знань за темою лабораторного заняття:

1. Чим симетричне шифрування відрізняється асиметричного шифрування?
2. Що таке гібридне шифрування? Які проблеми вирішує гібридне шифрування?
3. У яких випадках використовується метод Вернама?
4. На якій операції базується метод Вернама?
5. Які властивості висуваються до ключа при шифруванні за методом Вернама?
6. Яке існує застереження при використанні методу Вернама?
7. Яка криптографічна стійкість методу Вернама?
8. У якому випадку повідомлення, зашифроване за допомогою методу Вернама, можна буде розшифрувати?

Завдання: автоматизувати алгоритм Вернама, що використовується при симетричному методі шифрування.

Хід виконання лабораторної роботи:

Для утворення шифротексту за методом Вернама, повідомлення об'єднується операцією XOR з ключем (названим одноразовим блокнотом або шифроблокнотом). При цьому ключ повинен мати три критично важливі властивості:

- Бути справді випадковим;
- Збігатися за розміром з заданим відкритим текстом;
- Застосовуватися тільки один раз.

Так як цей шифр був придуманий для комп'ютерних систем, то слід зауважити що базується він на двійковій арифметиці. Цей метод шифрування використовує логічну операцію XOR (взаємовиключні АБО).

Шифрування являє собою складання по модулю *n* (потужність алфавіту) символу відкритого тексту і символу ключа з одноразового блокноту. Кожен символ ключа використовується тільки один раз і для єдиного повідомлення, інакше навіть якщо використовувати блокнот розміром в кілька гігабайт, при отриманні криптоаналітиком декількох текстів з ключами, що перекриваються, він зможе відновити вихідний текст. Він зрушить кожну пару шифротексту відносно один одного і підрахує число збігів в кожній позиції. Якщо шифротексти зміщені правильно, то співвідношення збігів різко зросте. З цієї точки зору криптоаналіз не складе труднощів. Якщо ж ключ не повторюється і випадковий, то криптоаналітик, перехоплює він тексти чи ні, завжди має однакові знання. Випадкова ключова послідовність, складена з невипадковим відкритим текстом, дає абсолютно випадковий криптотекст, і ніякі обчислювальні потужності не зможуть це змінити.

Шифр Вернама (одноразовий блокнот) – єдиний відомій абсолютно секретний шифр. Він заснований на тому, що повідомлення кодується побітовім XOR з одноразовим ключем, довжина якого не менше довжина повідомлення, що передається:

$E_k(x_1) = x1 \oplus k$

$D_k (x_1 \oplus k \oplus k) = x_1$

Кожній літері алфавіту, на якій написано повідомлення, потрібно присвоїти відповідний їй порядковий номер у двійковій системі числення, у такій спосіб задаючи свою таблицю кодування. Після цього, написавши повідомлення і придумавши ключ, перетворіть кожен символ в їх числове значення, відповідне вашої таблиці кодування, і після цього здійснюйте операцію XOR над кожною відповідною парою.

Слід зауважити, що метод Вернама належить до симетричних методів шифрування, що дозволяє, застосувавши операцію XOR до кожної пари символів шифрограми і ключа, отримати одержувачем початкове повідомлення.

Недоліком є те, що не можна використовувати один і той же ключ декілька разів – при кодуванні однаково повідомлень з однаковим ключем, отримані повідомлення також будуть однаково, що дозволить аналізувати передані повідомлення.

Додаткові завдання для студентів: опрацювання теоретичного матеріалу теми, написати план-конспект заняття за вибраною темою із використанням демонстраційного матеріалу.
Форми контролю знань – презентація виконаних завдань, перевірка коду програми, обговорення виконаних завдань.

Рекомендована література до теми лабораторного заняття:
Основна та допоміжна література:

1. Харин Ю.С. Математические основы криптологии: учеб.пособ. / Ю.С.Харин, В.И.Берник, Г.В.Матвеев. – Мн.: БГУ, 1999. – 319 с.
2. Зима В. Безопасность глобальных сетевых технологий / В.Зима, А.Молдован, Н.Молдован. – СПб.: БХВ-Петербург, 2003. – 368 с.
3. Щербаков А. Прикладная криптография / А. Щербаков, А.Домашев. – М., 2003. – 404 с.
4. Алферов А.П. Основы криптографии: учеб. пособ. / А.П.Алферов, А.Ю.Зубов, А.С.Кузьмин,
5. А.В.Черемушкин. – М.: Гелиос АРВ, 2002 – 480 с.
6. Басалова Г.В. Основы криптографии / Г.В. Басалова. – М.: Национальный Открытый Университет "ИНТУИТ", 2016. – 283 с. URL: https://www.twirpx.com/file/1907188/

Інтернет-ресурси:
https://books.ifmo.ru/file/pdf/56.pdf
http://booksshare.net/index.php?id1=4&category=cryptography&author=alferov-ap&book=2002

Обладнання заняття, ТЗН тощо: комп’ютери.

Укладач:_____ Задорожна А. В., доцент кафедри цифрової економіки та бізнес-аналітики
(підпис) (ПІБ, посада, науковий ступінь, вчене звання)