Міністерство освіти і науки України
Державний вищій навчальний заклад
“Криворізький національний університет”

МЕТОДИЧНІ ВКАЗІВКИ

для виконання лабораторних робіт
з дисципліни
„ Захист інформації у комп’ютерних системах ”

Для студентів денної та заочної форм навчання

Спеціальність 123 «Комп’ютерна інженерія»
Факультет інформаційних технологій
Кафедра комп’ютерні системи і мережі

Кривий Ріг
2018

Методичні вказівки до виконання лабораторних робіт для студентів денної та заочної форм навчання з дисципліни „ Захист інформації у комп'ютерних системах ".

Укладач: доц.,к.т.н. Вдовиченко І.Н.
Комп'ютерний набір : доц., к.т.н. Вдовиченко І.Н.

Схвалено на засіданні кафедри комп'ютерні системи і мережі
(Протокол № 7 від 20.02. 2018 р.)

завкафедрою _____ д.т.н. А.І. Купін
підпис

Методичні вказівки розглянуто та схвалено вченою радою факультету інформаційних технологій
(Протокол № 7 від 21.02. 2018 р.)

Голова вченої ради ФІТ _____ В.А. Чубаров
підпис

Начальник навчально-методичного відділу _____ Г.Х.Отверченко
підпис

Методичні вказівки рекомендовано для виконання лабораторних робіт з курсу дисципліни „ Захист інформації у комп'ютерних системах ".

Вказівки містять 6 лабораторних робіт, теоретичний матеріал за темами, приклади розв'язання завдань та питання для самоконтролю. Лабораторні роботи включають методи криптографії.

Наклад примірників: за вимогою

ЗМІСТ

ВСТУП

Метою лабораторних робіт з дисципліни „Захист інформації у комп'ютерних системах" є формування у студентів навичок пов'язаних з захистом інформації. Навчити працювати з методами криптографії, проводити аналіз уразливостей, робити висновки про поведінку системи, вміти визначити уразливі місця та знищити їх, розробляти різні моделі захисту системи, використовувати різні стратегії захисту, оцінювати альтернативні варіанти.

Основне **завдання** лабораторних робіт з дисципліни „ Захист інформації у комп'ютерних системах" полягає в підготовці висококваліфікованих спеціалістів, здатних застосовувати захист інформації, обєктів, устаткування, процесів.

ВКАЗІВКИ ДО ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ

Для успішного виконання лабораторних робіт необхідно:

1. Ознайомитися з темою та метою лабораторної роботи.
2. Уважно вивчити теоретичний матеріал запропонований в лабораторній роботі.
3. Уважно вивчити хід роботи.
4. Виконати вказаний перелік дій даної роботи.
5. Перевірити робото спроможність шифрування.
6. Записати результати досліду.
7. Виконати необхідні розрахункові роботи за вказаним планом.
8. Проаналізувати отримані результати.
9. Оформити звіт.

Лабораторна робота №1

Тема роботи: *Дослідження шифрів заміни, перестановки та гамування*

Мета роботи: *Дослідити алгоритм та методики практичної реалізації шифрів заміни, перестановки та гамування.*

Теоретичні відомості

Шифр перестановки

Шифр, перетворення якого змінюють тільки порядок проходження символів вихідного тексту, називається ***шифром перестановки*** (***ШП***).

Розглянемо перетворення з ШП, яке призначене для зашифрування повідомлення довжиною n символів. Його можна представити за допомогою таблиці

1	2	…	n
i_1	i_2	…	i_n

де i_1 – номер місця шифротексту, на яке попадає перша літера вихідного повідомлення при обраному перетворенні, i_2 – номер місця для другої літери й т.д.

Знаючи підстановку, що задає перетворення, можна здійснити як зашифровування, так і розшифровування тексту.

Шифр заміни

Шифрування ***методом заміни*** засновано на алгебраїчній операції, яка називається підстановкою — взаємно однозначне відображення деякої кінцевої безлічі M на себе.

Даний алгоритм зашифровування можна описати наступними формулами, де кожна літера відкритого тексту M замінюється літерою шифрованого тексту C.

У загальному вигляді при будь-якому зрушенні

$$C=E(M)=(M+k) \bmod (N),$$

де k=1,...,32 для російського алфавіту.

Алгоритм розшифровування має вигляд

$$M=D(C)=(C-k) \bmod (N).$$

Прикладом поліалфавітного шифру заміни є система Виженера. Шифрування відбувається по таблиці, що представляє собою квадратну матрицю розмірністю n x n, де n – кількість літер використовуваного алфавіту.

Перший рядок містить усі літери алфавіту. Кожний наступний рядок виходить із попереднього циклічним зрушенням останнього на одну літеру ліворуч.

Під кожною літерою вихідного повідомлення послідовно записуються літери ключа (якщо ключ виявився коротшим за повідомлення, то його використовують кілька разів). Кожна літера шифротексту перебуває на перетинанні стовпця таблиці, обумовленого літерою відкритого тексту, і рядку, обумовленого літерою ключа.

Розшифровування отриманої криптограми здійснюється в такий спосіб.

Під літерами шифротексту послідовно записуються літери ключа; у рядку таблиці, що відповідає черговій літері ключа, роблять пошук відповідної літери шифротексту — літера, що перебуває над нею в першому рядку таблиці, є відповідною літерою вихідного тексту, тобто перша літера по рядку тексту визначається за схемою (K_1 по стовпцю С1–М1).

<u>Шифрування методом гамування</u>

Для зашифровування вхідної послідовності за цим методом відправник виконує побітове додавання по модулю 2 ключа k

(відомий й одержувачу й відправнику) і m-розрядної двійкової послідовності, що відповідає повідомленню, яке пересилається:

$$c_i=m_i+k_i,\ i=1,m,$$

де m_i, k_i, c_i — черговий і-й біт відповідно вихідного повідомлення m, ключа k і зашифрованого повідомлення с. Процес розшифровування зводиться до повторної генерації ключової послідовності й накладенню її на зашифровані дані. Рівняння розшифрування має вигляд:

$$m_i=c_i–k_i,\ i=1,m$$

Розрізняють гамування з ***кінцевою*** й ***нескінченною гамами***. У якості кінцевої гами може використовуватися фраза, в якості нескінченної — послідовність, яка генерується генератором псевдовипадкових чисел.

У тому випадку, коли безліччю використовуваних для шифрування знаків повідомлення є текст, відмінний від двійкового коду, то його символи й символи гами замінюються цифровими еквівалентами, які потім підсумовуються по модулю N. Процес зашифровування в цьому випадку визначається співвідношенням

$$c_i=(m_i+r_i) \bmod N,\ i=1,\ m,$$

де m_i, r_i, c_i – черговий і-й знак вихідного повідомлення, гами й шифротексту відповідно; N – кількість символів в алфавіті повідомлення; m –кількість знаків відкритого тексту.

Хід роботи

1. Зашифрувати відкритий текст (текст повинен складатись не менш ніж з двох слів), використовуючи всі три методи шифрування (заміни, перестановки та гамування). Відкритий текст повинен бути у всіх випадках однаковий.

2. Обмінятись з наступною бригадою отриманим шифротекстом та ключами і провести розшифрування з метою отримання відкритого тексту.
3. Після розшифрування необхідно зробити звірку результатів.

Звіт повинен містити

1. Тему, мету і порядок роботи.
2. Приклади зашифрування та розшифрування для усіх розглянутих методів шифрування.
3. Висновки: переваги та недоліки наведених алгоритмів шифрування.

Питання для самоконтролю

1. Описати алгоритм методу заміни
2. Описати алгоритм методу перестановки
3. Описати алгоритм методу гамування
4. У чому різниця між кінцевою й нескінченною гамами.

Додатки

Кодування російського алфавіту

Літера	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Код	01	02	03	04	05	06	07	08	09	10	11	12
Літера	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Код	13	14	15	16	17	18	19	20	21	22	23	24
Літера	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	(пропуск)			
Код	25	26	27	28	29	30	31	32	33			

Таблиця Виженера

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_
А	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_
Б	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А
В	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б
Г	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В
Д	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г
Е	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д
Ж	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е
З	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж
И	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З
Й	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И
К	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ь	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ъ	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь
Ы	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ
Э	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы
Ю	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э
Я	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю
_	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я

Лабораторна робота №2

Тема роботи: *Дослідження криптоалгоритму шифрування RSA*

Мета роботи: *Дослідити структуру алгоритму та методики практичної реалізації криптосистеми шифрування RSA.*

Теоретичні відомості

Як відомо, алгоритми симетричного шифрування використовують ключі невеликої довжини й тому можуть швидко шифрувати великі обсяги даних.

При використанні ***алгоритму симетричного шифрування*** відправник і одержувач застосовують для шифрування й дешифрування даних один і той самий секретний ключ. Таким чином, алгоритми симетричного шифрування ґрунтуються на припущенні про те, що зашифроване повідомлення не зможе прочитати ніхто, крім того, хто має ключ для його дешифрування. При цьому, якщо ключ не скомпрометований, то при дешифруванні автоматично виконується аутентифікація відправника, тому що тільки він має ключ, за допомогою якого можна зашифрувати повідомлення. Таким чином, для симетричних криптосистем актуальна проблема безпечного розподілу симетричних секретних ключів. У зв'язку із цим без ефективної організації захищеного розподілу ключів використання звичайної системи симетричного шифрування в обчислювальних мережах практично неможливе.

Рішенням даної проблеми є використання ***асиметричних алгоритмів шифрування***, які називають криптосистемами з відкритим ключем.

В них для зашифровування даних використовується один ключ, який називають «***відкритим***», а для дешифровування —

інший, який називають «***закритим***» або «***секретним***». Варто мати на увазі, що ключ дешифрування не може бути визначений на основі ключа шифрування.

В асиметричних криптосистемах відритий ключ і криптограма можуть бути відправлені по незахищених каналах зв'язку. Концепція таких систем заснована на застосуванні односпрямованих функцій.

Прикладом односпрямованої функції може бути цілочисленне множення. Пряме завдання — обчислення добутку двох більших цілих чисел p і q, n = p*q. Це відносно нескладне завдання для ЕОМ.

Зворотне завдання — факторизація або розкладання на множники великого цілого числа практично нерозв'язна при досить великих значеннях n.

Наприклад, якщо p≈q, а їхній добуток n≈2664, то для розкладання цього числа на множники буде потрібно 223 операції, що практично неможливо виконати за прийнятний час на сучасних ЕОМ.

Іншим прикладом односпрямованої функції є модульна експонента з фіксованою основою та модулем.

Наприклад, якщо $y=a^x$, то природно можна записати, що x=log (y).

Завдання дискретного логарифмування формулюється в такий спосіб. Для відомих цілих a, n, y варто знайти таке число x, при якому ax (mod n)=y.

Наприклад, якщо a=2664 і n=2664 знаходження показника ступеня x для відомого y вимагатиме близько 1026 операцій, що також неможливо виконати на сучасних ЕОМ. У зв'язку з тим, що в наш час не вдалося довести, що не існує ефективного

алгоритму обчислення дискретного логарифму за прийнятний час, то модульна експонента також умовно віднесена до односпрямованих функцій.

Іншим важливим класом функцій, які використовуються при побудові криптосистем з відкритим ключем є, так звані, ***односпрямовані функції із секретом***. Функція відноситься до даного класу за умови, що вона є односпрямованою й, крім того, можливо ефективне обчислення зворотної функції, якщо відомо секрет.

В даній лабораторній роботі досліджується криптосистема RSA, що використовує модульну експоненту з фіксованим модулем і показником ступеня (тобто односпрямовану функцію із секретом).

Хід роботи

Хід виконання роботи відповідає криптосистемі шифрування даних по схемі RSA, що розташована нижче.

<u>Схема алгоритму шифрування даних RSA</u>

1. Визначення відкритого ***«e»*** і секретного ***«d»*** ключів

1.1. Вибір двох взаємно простих великих чисел ***p*** і ***q***

1.2. Визначення їхнього добутку: $n=p*q$

1.3. Визначення функції Ейлера: $\varphi(n)=(p-1)(q-1)$

1.4.. Вибір відкритого ключа ***e*** з урахуванням умов:

$$1<e\leq\varphi(n),\ НОД\ (e,\varphi(n))=1$$

1.5. Визначення секретного ключа ***d***, що задовольняє умові

$$e*d\equiv 1\ (mod\ \varphi(n)),\ \text{де}\ d<n$$

2. Алгоритм шифрування повідомлення ***M*** **(**дії відправника)

2.1. Розбиваємо вихідний текст повідомлення на блоки $M_1, M_2,\ldots, M_n$

$$(M_i = 0, 1, 2,..., n)$$

2.2. Шифруємо текст повідомлення у вигляді послідовності блоків:

$$C_i = M_i^e \pmod n$$

2.3. Відправляємо одержувачеві криптограму: $C_1, C_2,..., C_n$

2.4. Одержувач розшифровує криптограму за допомогою секретного ключа d по формулі:

$$M_i = C_i^d \pmod n$$

3. Процедуру шифрування даних розглянемо на наступному прикладі (для простоти й зручності розрахунків у даному прикладі використані числа малої розрядності):

3.1. Вибираємо два простих числа p і q, $p=3$, $q=11$;

3.2. Визначаємо їхній добуток (модуль) $n=p*q=33$;

3.3. Обчислюємо значення функції Ейлера $\varphi(n)=(p-1)(q-1)$

$$\varphi(n)=2*10=20$$

3.4. Вибираємо випадковим чином відкритий ключ із урахуванням виконання умов

$$1<e\le\varphi(n) \text{ і } НОД(e,\varphi(n))=1,\ e=7;$$

3.5. Обчислюємо значення секретного ключа d, що задовільняє умові

$$e*d \equiv 1 \pmod{\varphi(n)},\ 7*d \equiv 1 \pmod{20};\ d=3;$$

3.6. Відправляємо одержувачеві пари чисел ($n=33$, $e=7$);

Представляємо шифруєме повідомлення M як послідовність цілих чисел **312.**

3.7. Розбиваємо вихідне повідомлення на блоки $M_1=3$, $M_2=1$, $M_3=2$;

3.8. Шифруємо текст повідомлення, який представлено у вигляді послідовності блоків:

$$C_i = M_i^e \pmod n$$

$$C_1=3^7 \pmod{33} = 2187 \pmod{33} = 9,$$
$$C_2=1^7 \pmod{33} = 1 \pmod{33} = 1,$$

$$C_3=2^7 (mod\ 33) = 128\ (mod\ 33) = 29.$$

3.9. Відправляємо криптограму $C_1=9, C_2=1, C_3=29$.

3.10. Одержувач розшифровує криптограму за допомогою секретного ключа d по формулі:

$$Mi=C_i^d\ (mod\ n)$$

$$M_1=9^3 (mod\ 33) = 729\ (mod\ 33) = 3$$

$$M_2=1^3 (mod\ 33) = 1\ (mod\ 33) = 1$$

$$M_3=29^3 (mod\ 33) = 24389\ (mod\ 33) = 2.$$

Отримана послідовність чисел **312** являє собою вихідне повідомлення M.

Звіт повинен містити

1. Тему, мету і порядок роботи.
2. Блок-схему та програму алгоритму шифрування RSA.
3. Висновки: переваги й недоліки алгоритму шифрування RSA.

Питання для самоконтролю

1. Описати алгоритм методу шифрування RSA
2. Які змінні вибираємо випадково
3. У чому відмінність симетричних і асиметричних алгоритмів шифрування
4. Що таке секретний ключ
5. Як виконати дешифрування методом RSA

Лабораторна робота №3

Тема роботи: *Дослідження електронного цифрового підпису (ЕЦП) RSA*

Мета роботи: *Дослідити структуру алгоритму та методики практичної реалізації (ЕЦП) RSA.*

Теоретичні відомості

Технологія застосування системи ЕЦП припускає наявність мережі абонентів, що обмінюються підписаними електронними документами. При обміні електронними документами по мережі значно знижуються витрати, пов'язані з їхньою обробкою, зберіганням і пошуком.

Одночасно при цьому виникає проблема, як аутентифікації автора електронного документа, так і самого документа, тобто встановлення дійсності автора й відсутності змін в отриманому електронному повідомленні.

В алгоритмах ЕЦП як і в асиметричних системах шифрування використаються односпрямовані функції. ЕЦП використовується для аутентифікації текстів, переданих по телекомунікаційних каналах.

ЕЦП представляє собою невеликий обсяг додаткової цифрової інформації, переданої разом з підписаним текстом.

Концепція формування ЕЦП заснована на оборотності асиметричних шифрів, а також на взаємозв'язку вмісту повідомлення, самого підпису й пари ключів. Зміна хоча б одного із цих елементів унеможливить підтвердження дійсності підпису, що реалізується за допомогою асиметричних алгоритмів шифрування й хеш-функцій. Система ЕЦП включає дві процедури:

- формування цифрового підпису;
- перевірку цифрового підпису.

В процедурі формування підпису використовується секретний ключ відправника повідомлення, у процедурі перевірки підпису — відкритий ключ відправника.

Безпека системи RSA визначається обчислювальними труднощами розкладання на множники великих цілих чисел. Недоліком алгоритму цифрового підпису RSA є уразливість його до мультиплікативної атаки. Інакше кажучи, алгоритм ЕЦП RSA дозволяє хакеру без знання секретного ключа сформувати підписи під тими документами, в яких результат хешування можна обчислити як добуток результату хешування вже підписаних документів.

Хід роботи

Завдання на виконання лабораторної роботи видається викладачем після проходження студентами співбесіди по основах аутентифікації даних та концепції формування електронного цифрового підпису.

Порядок виконання роботи відповідає, наведеному нище алгоритму формування ЕЦП за схемою RSA.

Алгоритм електроннго цифрового підпису (ЕЦП) RSA

1. Визначення відкритого «e» і секретного «d» ключів

1.1. Вибір двох взаємно простих великих чисел ***p*** і ***q***

1.2. Визначення їхнього добутку: $n=p*q$

1.3. Визначення функції Ейлера: $\varphi(n)=(p-1)(q-1)$

1.4. Вибір відкритого ключа ***e*** з урахуванням умов:

$$1<e\leq\varphi(n),\ НОД\ (e,\varphi(n))=1$$

1.5. Визначення секретного ключа ***d***, що задовольняє умові

$$e*d \equiv 1 \pmod{\varphi(n)}, \text{ де } d<n$$

2. Формування ЕЦП

2.1. Обчислення хеш-значення повідомлення ***M:***

$$m=h(M)$$

2.2. Для одержання ЕЦП шифруємо хеш-значення ***m*** за допомогою секретного ключа ***d*** і відправляємо одержувачеві цифровий підпис $S=m^d \pmod n$ і відкритий текст повідомлення ***M***

3. Аутентифікація повідомлення — перевірка дійсності підпису

3.1. Розшифровка цифрового підпису ***S*** за допомогою відкритого ключа ***e*** і обчислення його хеш-значення $m^1=S^e \pmod n$

3.2. Обчислення хеш-значення прийнятого відкритого тексту ***M***

$$m=h(M)$$

3.3. Порівняння хеш-значеннь ***m*** і m^1, якщо $m=m^1$, то цифровий підпис ***S*** — достовірний.

Процедуру формування ЕЦП повідомлення M розглянемо на наступному простому прикладі:

4. Обчислення хеш-значення повідомлення M: m=h(M).

Повідомлення M, що хешується, представимо як послідовність цілих чисел 312. Відповідно до наведеного вище алгоритму формування ЕЦП RSA вибираємо два взаємно простих числа ***p=3***, ***q=11***, обчислюємо значення ***n=p*q=3*11=33***, вибираємо значення секретного ключа ***d=7*** і обчислюємо значення відкритого ключа ***e=3***. Вектор ініціалізації H_0 обираємо рівним ***6*** (вибирається випадковим чином).

Хеш-код повідомлення ***M=312*** формується в такий спосіб:

$$H_1=(M_1+H_0)^2 \pmod n=(3+6)^2 \pmod{33}=81 \pmod{33} = 15$$

$$H_2=(M_2+H_1)^2(mod\ n)=(1+15)^2\ (mod\ 33)=256\ (mod\ 33)\ =\ 25$$

$$H_3=(M_3+H_2)^2(mod\ n)=(2+25)^2\ (mod\ 33)=729\ (mod\ 33)\ =\ 3,\ m=3$$

4.1. Для одержання ЕЦП шифруємо хеш-значення ***m*** за допомогою секретного ключа ***d*** і відправляємо одержувачеві цифровий підпис

$S=m^d(mod\ n)$ і відкритий текст повідомлення ***M***

$$S=3^7(mod\ 33)\ =\ 2187\ (mod\ 33)\ =\ 9$$

4.2. Перевірка дійсності ЕЦП

Розшифровка ***S*** (тобто обчислення її хеш-значення m^1) виконується за допомогою відкритого ключа ***e***.

$$m^1=S\ (mod\ n)\ =\ 9^3\ (mod\ 33)\ =\ 729\ (mod\ 33)\ =\ 3$$

4.3. Якщо порівняння хеш-значеннь m^1 і ***m*** показує їхню рівність, тобто $m=m^1$, то підпис достовірний.

Звіт повинен містити

1. Тему, мету і порядок роботи.
2. Блок-схему алгоритму й програму формування ЕЦП RSA.
3. Висновки: переваги й недоліки ЕЦП RSA.

Питання для самоконтролю

1. Описати алгоритм електронного цифрового підпису RSA
2. Які змінні вибираємо випадково
3. Назвіть властивості хеш функції
4. Назвіть переваги й недоліки ЕЦП RSA

Лабораторна робота №4

Тема роботи: *Дослідження криптоалгоритму шифрування Ель Гамаля*

Мета роботи: *Дослідити структуру алгоритму та методики практичної реалізації криптосистеми шифрування Ель Гамаля.*

Теоретичні відомості

Схема шифрування Ель Гамаля може бути використана як для формування цифрових підписів, так і для шифрування даних.

Безпека схеми Ель Гамаля обумовлена складністю обчислення дискретних логарифмів у кінцевому полі.

Для розшифрування даних одержувач зашифрованої інформації використовує секретний ключ, що не може бути визначений з відкритого ключа.

При використанні алгоритму шифрування Ель Гамаля довжина шифротексту вдвічі більше довжини вихідного відкритого тексту M.

В реальних схемах шифрування необхідно використовувати як модуль n велике просте число, що має у двійковому поданні довжину 512…1024біт.

Слід відзначити, що формування кожного підпису по даному методу вимагає нового значення k, причому це значення повинне вибиратися випадковим чином. Якщо порушник розкриє значення k, повторно використане відправником, то може розкрити й секретний ключ x відправника.

Хід роботи

Завдання на виконання лабораторної роботи видається викладачем після проходження студентами співбесіди по основах криптографічного захисту інформації.

Порядок виконання роботи відповідає наведеній нижче криптосистемі шифрування даних за схемою Ель Гамаля.

<u>Схема алгоритму шифрування даних Ель Гамаля</u>

1. Визначення відкритого "y" і секретного "x" ключів

1.1. Вибір двох взаємно простих великих чисел p і q, $q<p$

1.2. Вибір значення секретного ключа x, $x<p$

1.3. Визначення значення відкритого ключа y з виразу:

$$y=q^x \pmod p$$

2. Алгоритм шифрування повідомлення M

2.1. Вибір випадкового числа k, що задовольняє вимозі:

$$0 \le k < p-1 \text{ і НОД } (k,p-1) = 1$$

2.2. Визначення значення a з виразу: $a=q^{k \pmod p}$

2.3. Визначення значення b з виразу: $b=y^k M \pmod p$

2.4. Криптограма C, що складається з a і b, відправляється одержувачеві

2.5. Одержувач розшифровує криптограму за допомогою виразу:

$$M = b+(a\text{^}x \pmod p)$$

3. Процедуру шифрування даних розглянемо на наступному прикладі (для зручності розрахунків у даному прикладі використані числа малої розрядності):

3.1. Вибираємо два взаємно простих числа $p=11$ і $q=2$;

3.2. Вибираємо значення секретного ключа x, $(x<p)$, $x=8$;

3.3. Обчислюємо значення відкритого ключа y з виразу

$$y=q^x \pmod p=2^8 \pmod{11}=256 \pmod{11}=3$$

3.4. Вибираємо значення відкритого повідомлення ***M=5;***

3.5. Вибираємо випадкове число ***k=9; НОД (9,10)=1***;

3.6. Визначаємо значення ***a*** з виразу:

$$a=q^{k\ (mod\ p)=29}(mod\ 11)=512\ (mod\ 11)=6;$$

3.7. Визначаємо значення ***b*** з виразу:

$$b=y^{k}\ M\ (mod\ p)\ =\ 3^{9}*5\ (mod\ 11)=98415\ (mod\ 11)=9.$$

Таким чином, одержуємо зашифроване повідомлення як ***(a,b)=(6,9)*** і відправляємо одержувачеві.

3.8. Одержувач розшифровує даний шифротекст, використовуючи секретний ключ ***x*** і вирішуючи наступне зрівняння:

M=(ba^(p-1-x)) mod p

Обчислене значення повідомлення ***M=5*** являє собою задане вихідне повідомлення.

Звіт повинен містити

1. Тему, мету і порядок роботи.
2. Блок-схему та програму алгоритму шифрування Ель Гамаля.
3. Висновки: переваги та недоліки алгоритму шифрування Ель Гамаля.

Питання для самоконтролю

1. Описати алгоритм шифрування методом Ель Гамаля
2. Які змінні вибираємо випадково
3. Що собою представляє шифротекст
4. Що собою представляє секретний ключ
5. Назвіть переваги й недоліки методу Ель Гамаля відносно методу RSA

Лабораторна робота №5

Тема роботи: *Дослідження електронного цифрового підпису (ЕЦП) Ель Гамаля*

Мета роботи: *Дослідити структури алгоритму та методики практичної реалізації (ЕЦП) Ель Гамаля.*

Теоретичні відомості

Загальновизнані прийоми встановлення дійсності фізичного підпису під документом абсолютно не придатні при обробці документів в електронній формі. Рішенням даного питання є алгоритм, так званої, системи електронного підписування документів. Для гарантії дійсності авторства й цілісності інформаційного повідомлення необхідно зашифрувати його вміст. При використанні цифрового підпису інформація не шифрується й залишається доступною будь-якому користувачеві, що має до неї доступ.

При обміні електронними документами по мережі значно знижуються витрати, пов'язані з їхньою обробкою, зберіганням та пошуком.

Одночасно при цьому виникає проблема, як аутентифікації автора електронного документа, так і самого документа, тобто встановлення дійсності автора та відсутності змін в отриманому електронному повідомленні.

ЕЦП використовується для аутентифікації текстів, переданих по телекомунікаційних каналах. Функціонально він аналогічний звичайному рукописному підпису та має основні його властивості:

- засвідчує, що підписаний текст виходить від особи, що поставила підпис;

- не дає цій самій особі можливості відмовитися від зобов'язань, пов'язаних з підписаним текстом;
- гарантує цілісність підписаного тексту.

ЕЦП представляє собою невеликий обсяг додаткової цифрової інформації, переданої разом з підписаним текстом.

Концепція формування ЕЦП за схемою Ель Гамаля також заснована на оборотності асиметричних шифрів і на взаємозв'язку вмісту повідомлення, самого підпису й пари ключів.

Ідея алгоритму цифрового підпису Ель Гамаля базується на тому, що для обґрунтування практичної неможливості фальсифікації цифрового підпису в ній використана більш складне обчислювальне завдання дискретного логарифмування, ніж розкладання на множники великого цілого числа. Основною перевагою такої схеми цифрового підпису є можливість створення ЕЦП для великої кількості повідомлень із використанням одного секретного ключа.

Безпека схеми Ель Гамаля обумовлена складністю обчислення дискретних логарифмів у кінцевому полі.

Хід роботи

Завдання на виконання лабораторної роботи видається викладачем після проходження студентами співбесіди по основах аутентифікації даних і концепції формування електронного цифрового підпису за схемою Ель Гамаля.

<u>Схема формування ЕЦП Ель Гамаля</u>

1. Визначення відкритого “y” і секретного “x” ключів

1.1. Вибір двох взаємно простих великих чисел p і q, $q<p$

1.2. Вибір значення секретного ключа x, $x<p$

1.3. Визначення значення відкритого ключа ***y*** з виразу:

$$y=q^x \pmod p$$

2.Формування ЕЦП

2.1. Обчислення хеш-значення повідомлення ***M: m=h(M); 1<m<p-1***

2.2. Вибір випадкового числа ***k,***

$$0 < k < p-1 \text{ і НОД } (k,p-1)=1$$

2.3. Визначення значення ***a*** з виразу: $a=q^k \pmod p$

2.4. Визначення значення ***b*** з виразу:

$$m=(xa+kb) \pmod{(p-1)}$$

2.5. Цифровий підпис ***S=(a,b)*** і відкритий текст повідомлення ***M*** відправляються одержувачеві.

3. Аутентифікація повідомлення — перевірка дійсності підпису

3.1. Обчислення хеш-значення прийнятого відкритого тексту повідомлення ***M*** $m^1=h(M)$ визначення ***b*** з виразу:

$$m=(xa+kb) \pmod{(p-1)}$$

3.2. Підпис вважається достовірним, якщо $a<p$, $m=m^1$ і виконується умова

$$y^a \, a^b \pmod p = q^{m1} \pmod p$$

4. У якості процедури формування ЕЦП розглянемо наступнийприклад (для зручності розрахунків у даному прикладі використані числа малої розрядності):

4.1. Вибираємо просте число ***p*** і два випадкових числа ***q*** і ***x*** ***(q і x < p),***

p=11, q=2 і секретний ключ ***x=8;***

4.2. Обчислюємо значення відкритого ключа ***y***

$$y=q^x \pmod p=28 \pmod{11}=3;$$

4.3. Визначаємо хеш-значення вихідного повідомлення ***M (312)***

m=h(M), у даному прикладі приймаємо ***m=3***

4.4. Вибираємо випадкове ціле число ***k,*** взаємно просте з ***p-1.***

Приймаємо ***k=9, НОД (9,10)=1.***

4.5. Для формування ЕЦП обчислюємо елементи підпису ***a*** і ***b***

$$a=q^{k} \pmod p=29 \pmod{11}=6.$$

Елемент ***b*** визначаємо за допомогою розширеного алгоритму Евкліда з наступного співвідношення:

$$m=(xa+kb) \pmod{(p-1)};$$
$$3=(8*6+9*b) \pmod{10}); \quad 9*b=-45 \pmod{10}$$
$$b=5.$$

У даному прикладі цифровим підписом є пара чисел ***a=6, b=5.***

Цифровий підпис ***S=(a,b)*** і відкритий текст повідомлення ***M*** відправляються одержувачеві. Для контролю цілісності повідомлення й вірогідності ЕЦП одержувач обчислює хеш-значення m^1 прийнятого відкритого тексту повідомлення ***M***. При цьому відправник і одержувач використовує одну й ту саму хеш-функцію ***h.***

Отримавши підписане повідомлення й відкритий ключ ***y=3***, одержувач для перевірки дійсності підпису перевіряє виконання умови:

$$y^{a}\, a^{b} \pmod p=q^{m1} \pmod p$$
$$3^{6} * 6^{5} \pmod{11}=2^{3} \pmod{11}$$
$$5668704 \pmod{11}=8 \pmod{11}$$
$$8 \pmod{11}=8 \pmod{11},$$

тому якщо умова виконується, то прийняте одержувачем повідомлення вважається справжнім.

Таким чином, процедура встановлення дійсності прийнятого повідомлення полягає в перевірці відповідності

аутентифікатора повідомлення.

Варто мати на увазі те, що кожний підпис за схемою Ель Гамаля вимагає нового значення ***k***. Випадкове значення ***k*** повинне зберігатися в секреті.

Звіт повинен містити

1. Тему, мету і порядок роботи.
2. Блок-схему та програму алгоритму ЕЦП Ель Гамаля.
3. Висновки: переваги та недоліки ЕЦП Ель Гамаля.

Питання для самоконтролю

1. Описати алгоритм ЕЦП Ель Гамаля
2. Які змінні вибираємо випадково
3. Що собою ЕЦП
4. Навіщо використовують ЕЦП
5. Назвіть переваги й недоліки ЕЦП Ель Гамаля відносно ЕЦП RSA

Лабораторна робота №6

Тема роботи: *Пошук уразливих місць комп'ютера за допомогою програми «XSpider»*

Мета роботи: *Виявити уразливі місця комп'ютера за допомогою програми «XSpider» та ліквідувати їх*

Теоретичні відомості

Спочатку у програмі Xspider необхідно задати ip-адресу комп'ютера, який буде підлягати скануванню на уразливі місця.

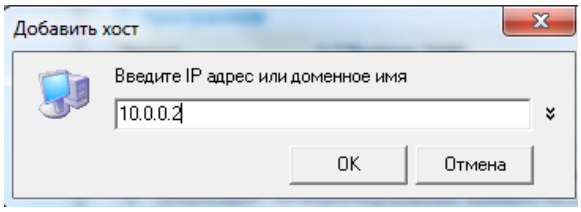

Рисунок 1.1 – Введення ip-адреси комп'ютера

Після введення ip-адреси пк він одразу додається до списку сканування у програмі Xspider.

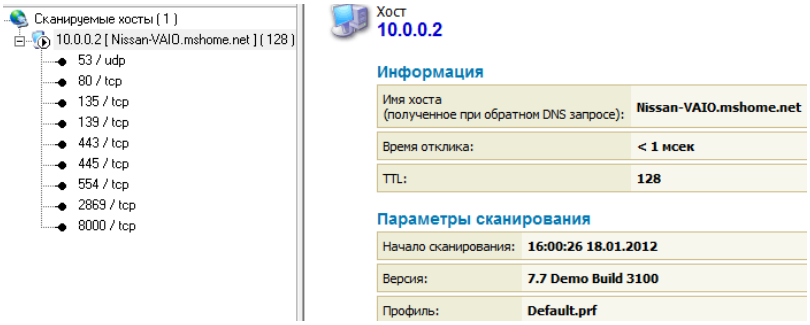

Рисунок 1.2 – Додання комп'ютера до списку сканування

Далі необхідно розпочати сканування комп'ютера на уразливі місця, якими може скористатися зловмисник. По закінченню сканування буде виведено список виявлених уразливостей комп'ютера.

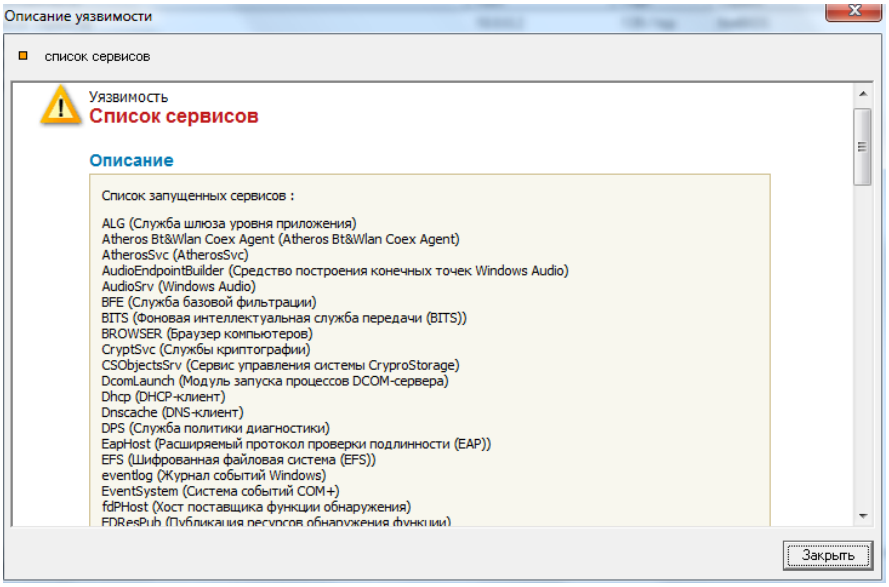

Рисунок 1.3 – Список виявлених уразливостей ком'ютера

У кінці списку буде наведено вирішення щодо знищення уразливих місць комп'ютера.

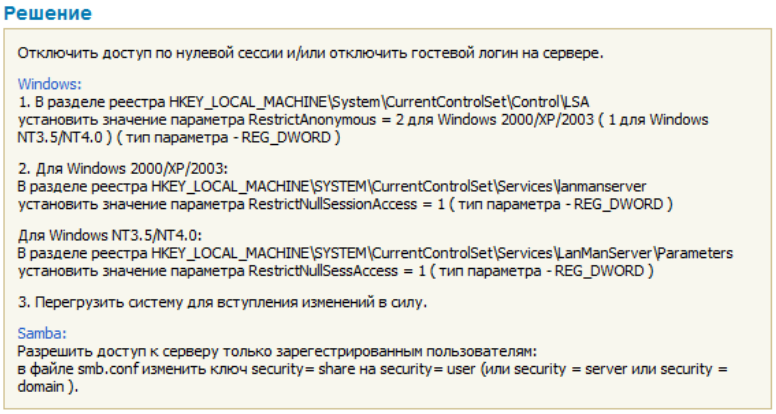

Рисунок 1.4 – Список вирішення щодо знищення уразливих місць комп'ютера

Після виконання запропонованих інструкцій щодо знищення уразливостей по завершенню проведення повторного сканування уразливостей не знайдено.

Рисунок 1.5 – Результати виконання повторного сканування комп'ютера

Звіт повинен містити

1. Тему, мету і порядок роботи.
2. Блок-схему та алгоритм.

3. Висновки: переваги та недоліки методу пошуку уразливих місць.

Питання для самоконтролю

1. Що таке уразливі місця
2. Які параметри треба задати для роботи програми
3. Які уразливості можливо знищіти і як

Список літератури

1. Алферов А.П. Основы криптографии: Учеб. пособие, 5-е и зд., испр. и доп. /Алферов А.П., Зубов А.Ю. и др. -М.: Гелиос АРВ, 2012.- 480 с.
2. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. /Иванов М.А. - М.: Кудиц-Образ, 2001.- 368 с.
3. Мельников В.В. Защита информации в компьютерных системах. / Мельников В.В. - М.: ФиС, 2007
4. Романец Ю.В. Защита информации в компьютерных системах и сетях /Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.. -М.: Радио и связь, 2001.-376 с.
5. Хамидуллин Р.Р. Методы и средства защиты компьютерной информации: Учеб. пособие. /Хамидуллин Р.Р., Бригаднов И.А., Морозов А.В. – СПб.: СЗТУ, 2005. – 178 с.
6. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. /Шнайер Б. – М.: Издательство ТРИУМФ, 2002. – 816 с.
7. Шеховцов В.А. Операційні системи. / Шеховцов В.А. – К.: Видавнича група BHV, 2005. – 576 с.: іл.
8. В.Г. Олифер. Сетевые операционные системы. /В.Г. Олифер, Н.А. Олифер. –СПб.: Питер, 2002. – 544 с.
9. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. /Завгородний В.И. -М.: Логос; 2001. -264 с.
10. Петраков А.В. Основы практической защиты информации. /Петраков А.В. –М.: Радио и связь, 2001. – 368 с.
11. Соколов А.В. Защита информации в распределённых корпоративных сетях и системах /Соколов А.В., Шаньгин В.Ф. -М.: ДМК Пресс, 2002. -656с.
12. Хоффман А. Современные методы защиты информации. /Хоффман А. -М.: Радио и связь.
13. В.Василюк, С.Климчук. Інформаційна безпека, К.,КНТ, 2008 р., - 190 с.
14. В. Галатенко. Стандарты информационной безопасности., М., НИИСИ РАН, 2006, - 262 с.
15. Грайворонський М.В. Безпека інформаційно-комунікаційних систем. / Грайворонський М.В., Новіков О.М. – К.: Видавнича група BHV, 2009. – 608 с
16. Петров А. А., Комп'ютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000.– 488 с.