Практична робота №6

ЗАХИСТУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ШИФРУ ПЕРЕСТАНОВКИ ТА ЗАМІНИ

Мета – здобуття практичних навичок захисту інформації за допомогою шифру перестановки та заміни

ТЕОРЕТИЧНІ ВІДОМОСТІ

1. Шифрування текстової інформації із використанням криптографічного шифру заміни

Заміна (підстановка) – це метод шифрування, при якому кожен знак вихідного тексту взаємно однозначно заміняється шифропозначенням – одним, або декількома знаками деякого набору символів (алфавіту) [2]. Шифр однобуквеної простої заміни – один з найдавніших шифрів. Шифропозначення для нього застосовувались різні – від букв алфавіту до фігурок «танцюючих чоловічків». У найпростішому вигляді даний шифр полягає в тому, що буква переходить у букву, а вхідний і вихідний алфавіти збігаються як множини, тобто з точністю до перестановки. Для зашифрування чергової букви відкритого тексту визначається її номер у вхідному алфавіті і на відповідне місце формовного шифртексту поміщається буква з тим же номером, але вже з вихідного алфавіту.

Створення ключа

Вихідним алфавітом є малі літери українського алфавіту та дефіс:

а б в г ґ д е є ж з и і ї й к л м н о п р с т у ф х ц ч ш щ ь ю я -

Для побудови ключа скористаємось процедурою рандомізації, тобто перемішаємо вихідний алфавіт у випадковому порядку. Отримуємо такий ключ:

б л з а п у х с я н к е ґ і и ю ц ч є й г р ї в м ф щ ж о ш - т д ь

Шифрування

Маємо наступний текст, який необхідно зашифрувати (відкрите повідомлення):

є-люди-які-беруть-у-руки-ціпок-коли-в-них-кульгають-докази

Створюємо таблицю зашифрування: зіставляємо вихідний символ алфавіту відповідному символу ключа.

а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	-
б	л	з	а	п	у	х	с	я	н	к	е	ґ	і	и	ю	ц	ч	є	й	г	р	ї	в	м	ф	щ	ж	о	ш	-	т	д	ь

Використовуючи отриману таблицю зашифровуємо відкрите повідомлення. Перший символ тексту «є» відповідно до таблиці кодується символом «с». Аналогічно, другий символ «-» – «ь» і т. д. В результаті отримуємо наступне зашифроване повідомлення:

сьютукьдиеьлхгвї-ьвыгвикьщейєиьиєюкьзьчкфьивю-абтї-ьуєибнк

Дешифрування

Аналогічно таблиці зашифрування створюємо обернену таблицю роз-

шифрування:

а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	-
г	а	у	р	ї	я	і	о	ч	в	к	й	т	п	и	б	ф	з	ш	ґ	с	є	ю	д	х	е	м	н	щ	ц	-	л	ж	ь

За допомогою цієї таблиці розшифровуємо попередньо отримане повідомлення: знаходимо відповідності зашифрованих символів до відкритих. Так перший символ «с» розшифровується як «є». Другий «ь» — «-». Після розшифрування усіх символів отримуємо:

є-люди-які-беруть-у-руки-ціпок-коли-в-них-кульгають-докази

Розшифроване повідомлення еквівалентне вихідному відкритому повідомленню. Це свідчить про правильність виконання процесів шифрування та дешифрування.

2. Провести шифрування текстової інформації із використанням криптографічного шифру перестановки

Теоретичні відомості

Шифри типу перестановки застосовувались ще у античні часи. Відмінність цього типу шифру від шифрів заміни полягає в тому, що під час зашифрування буква a_i відкритого тексту переходить не у фіксований знак алфавіту, а в іншу букву того ж відкритого тексту, скажемо a_j, у результаті чого букви розташовуються на нових місцях, тобто переставляються. Ключем для даного шифру також служить таблиця заміни, тільки не букв алфавіту, а їхніх індексів (номерів місць) у тексті, який підлягає зашифруванню. У загальному випадку розмір таблиці заміни дорівнює довжині відкритого тексту. Такі таблиці зручно формувати (і записувати) у вигляді так званих підстановок.

Для зашифрування шифром вертикальної перестановки будується прямокутна таблиця, кількість рядків якої визначається довжиною тексту, а кількість колонок дорівнює довжині ключа. Потім кожна буква ключового слова замінюється на число таким чином, щоб буква, яка має менший порядковий номер в алфавіті, замінялася на менше число. Отримані числа проставляються підряд на початку відповідних стовпців таблиці і надалі вважаються номерами цих стовпців. Відкритий текст вписується у таблицю, переходячи звичайним чином з рядка на рядок. Потім виписуються букви зі стовпців таблиці: спочатку весь стовпець, на початку якого стоїть одиниця, потім – стовпець, позначений двійкою і т. д. У підсумку, одержуємо шифротекст.

Створення ключа

Ключем для шифру перестановки буде слугувати гасло – слово «апогей». На основі гасла створюємо таблицю, яка буде використовуватись для шифрування (шкала рознесення). Кількість стовпців у таблиці дорівнює кількості літер у гаслі. Пронумеруємо кожен стовпчик таблиці таким чином, щоб менший порядковий номер літери гасла у алфавіті отримав менше число.

а	п	о	г	е	й

1	6	5	2	3	4

Шифрування

Дано наступний відкритий текст: «Не я належу минулому, а минуле належить мені».

Опускаємо неалфавітні символи тексту і вписуємо його до таблиці послідовно порядково:

а	п	о	г	е	й
1	6	5	2	3	4
н	е	я	н	а	л
е	ж	у	м	и	н
у	л	о	м	у	а
м	и	н	у	л	е
н	а	л	е	ж	и
т	ь	м	е	н	і

Виписуємо літери із стовпців таблиці: у порядку нумерації стовпців, зверху вниз. Отримуємо такий шифротекст (для зручності розбитий на групи по п’ять символів):

неумн тнмму ееаиу лжнлн аеиія уонлм ежлиа ь

Дешифрування

Для розшифрування шифротексту треба виконати обернену послідовність дій: у порядку номерів стовпчиків вписати до таблиці зверху вниз шифротекст і потім виписати послідовно порядково вихідний текст повідомлення.

3. Оцінювання стійкості паролів користувачів до зламу

Оцінимо стійкість U пароля до взлому.

1. Нехай L - довжина пароля.

Якщо довжина пароля $L \leq 4$, то U=0

інакше, якщо $5 \leq L \leq 7$, то U=6

інакше, якщо $8 \leq L \leq 15$, то U=12

інакше, якщо $16 \leq L$, то U=18

2. Якщо в паролі є букви, але тільки в одному (нижньому або верхньому регістрі), то U=U+5

інакше, якщо в паролі є букви і в нижньому і у верхньому регістрах, то U=U+7

3. Хай N - число цифр в паролі.

Якщо число цифр в паролі $1 \leq N \leq 2$, то U=U+5

інакше, якщо $3 \leq N$, то U=U+7

4. Хай S - число спецсимволів (#$%@) у паролі.

Якщо $1 \leq S < 2$, то U=U+5

інакше, якщо $2 \leq S$, то U=U+10.

5. Якщо в паролі є букви в обох регістрах, спецсимволи і цифри, то U=U+6 інакше, якщо тільки чогось одного з цього немає, U=U+4.

6. Оцінювання результатів.

Якщо U < 16 - пароль дуже слабкий

інакше, якщо 15 < U < 25 – слабкий

інакше, якщо 24< U < 35 – середній

інакше, якщо 34< U < 45 – сильний

інакше, якщо 44 < U – дуже сильний

ЗАВДАННЯ НА ВИКОНАННЯ

1. Ознайомитися з теоретичними відомостями.

2. Провести шифрування текстової інформації із використанням криптографічного шифру заміни, використовуючи гасло-шифр та зсув на кількість літер у гаслі-шифру. У таблиці 1.1 представлено індивідуальні завдання на виконання. Варіант завдання вибирається відповідно до списку академічної групи.

Таблиця 3.1. Індивідуальні завдання із використанням криптографічного шифру заміни

№ варіанту	Гасло-шифр	Текст, який необхідно зашифрувати
1.	Захист	Вимоги безпеки до технологічного обладнання та процесів
2.	Підручник	Інтерфейс прикладного програмування системи
3.	Синема	Для створення шифрованого тексту на вихідний накладається гама.
4.	Зупинка	Атака, що має на меті змусити сервер не відповідати на запити
5.	Порушник	Безліч людей розмовляють в масштабі реального часу шляхом набору повідомлень на клавіатурі
6.	Гроза	Сьогодні є чимало каналів просочування інформації з організації
7.	Модель	У першій частині розглядаються загальні проблеми безпеки інформаційних систем
8.	Форма	У другій частині увага приділяється методам та засобам можливого вирішення цих проблем
9.	Техніка	Роль інформації в сучасному світі та необхідність її захисту
10.	Слова	Разом з поняттям інформація, важливе значення має поняття дані
11.	Ключ	Від інформації дані відділяються конкретною формою подань.
12.	Пароль	Інформація на стадії даних характеризується певною формою подання й додатковою характеристикою
13.	Футляр	Нематеріальність інформації полягає у тому, що не можна виміряти параметри відомими фізичними методами
14.	Вірус	Таким чином, інформація зберігається і передається на

№ варіанту	Гасло-шифр	Текст, який необхідно зашифрувати
		матеріальних носіях
15.	Клей	Все що є матеріальним об’єктом, інформацією бути не може
16.	Користувач	Інформація не може існувати сама по собі, у відриві від матеріального носія
17.	Логін	Матерія ж не може не нести інформації, оскільки завжди перебуває в певному стані
18.	Флешка	Матеріальними носіями інформації можуть бути мозок людини, звукові та електромагнітні хвилі
19.	Тенол	Інформація, якщо вона міститься на матеріальному носієві, доступна людині.
20.	Техніка	Цінність інформації визначається мірою її корисності для власника
21.	Захист	Якщо доступ до інформації обмежується, то така інформація є конфіденційною
22.	Крипто	Для позначення цінності конфіденційної комерційної інформації використовується категорія конфіденційно
23.	Граф	Інформацію правочинно розглядати як товар, що має певну цінність
24.	Модель	Кількість інформації тим більша, чим нижча ймовірність події
25.	Теорія	Підхід ентропії широко використовується при визначенні кількості інформації, переданої по каналах зв’язку
26.	Процес	Тезарусний підхід заснований на розумінні інформації як знань
27.	Директор	У результаті копіювання без зміни інформаційних параметрів носія кількість інформації не змінюється, а ціна зменшується
28.	Завуч	Проблеми захисту інформації непокоїли людство з давніх-давен.
29.	Равлик	Необхідність захисту інформації виникла через потребу таємного передавання інформації (повідомлень)
30.	Таємниця	Створення сучасних комп’ютерних систем і мереж радикально змінили характер і діапазон проблем захисту інформації.
31.	Краб	Античні спартанці шифрували свої військові повідомлення
32.	Шифр	Завдяки персональним комп’ютерам працювати з інформацією дуже просто
33.	Портал	Зловмисникам стало набагато простіше викрадати конфіденційну інформацію
34.	Ложка	Краще вчитися на чужих помилках. Нехай навіть безглуздих
35.	Монстер	Чим безглуздіша помилка, тим передбачливішими треба бути, щоб її передбачити.

3. Провести шифрування текстової інформації із використанням криптографічного шифру перестановки. У таблиці 1.2 представлено

індивідуальні завдання на виконання. Варіант завдання вибирається відповідно списку академічної групи.

Таблиця 3.2. Індивідуальні завдання до виконання завдання із використанням криптографічного шифру перестановки

№ варіанту	Ключове слово	Текст, який потрібно зашифрувати
1.	Файл	Існують різні методи боротьби з фішингом
2.	Засіб	Ніколи не відповідайте на листи, що запитують вашу конфіденційну інформацію
3.	Фітинг	У разі одержання інформації з джерела, яке викликає у вас недовіру перевірте його сайт
4.	Фішинг	Регулярно перевіряйте стан своїх електронних рахунків
5.	Рівень	Перевіряйте рівень захисту відвідуваного вами сайту
6.	Метод	Будьте обережними, працюючи з електронними листами й конфіденційними даними
7.	Захист	Забезпечте якісний захист свого комп’ютера
8.	Копія	Завжди повідомляйте по виявлену підозрілу активність
9.	Диск	Алгоритми симетричного шифрування використовують ключі не дуже великої довжини.
10.	Інтер	Алгоритми симетричного шифрування можуть швидко шифрувати великі обсяги даних.
11.	Буква	Ключ шифрування в асиметричних системах називається відкритим ключем
12.	Шифр	Ключ розшифрування потрібно тримати в секреті
13.	Рупор	На противагу тайнопису криптографією з ключем називають сьогодні алгоритми шифрування
14.	Колесо	У криптографічних системах ключ формує людина або він створюється автоматично
15.	Інформація	Усі крипто алгоритми з ключем поділяються на симетричні і асиметричні
16.	Мережа	У симетричних криптоалгоритмах використовуються ідентичні ключі
17.	Літера	Ключ несе у собі всю інформацію про засекречування повідомлення
18.	Коефіцієнт	Електростатичне і магнітостатичне екранування ґрунтується на замиканні екраном
19.	Україна	На високій частоті застосовується виключно електромагнітне екранування
20.	Небо	Двері і вікна приміщення серверної кімнати повинні бути екрановані
21.	Соловей	Усі системи захисту телефонних ліній поділяються на пасивні і активні
22.	Калина	Для контролю стану ліній зв’язку використовуються різні індикатори
23.	Сонце	Апаратура пригнічення радіовипромінюючих пристроїв

№ варіанту	Ключове слово	Текст, який потрібно зашифрувати
		прослуховування являє собою генератор шумових перешкод
24.	Козак	Робоче місце користувача автоматизованої системи має бути обладнане відповідно до рекомендацій
25.	Гетьман	Помилкові операції або дії можуть викликати відмови апаратних і програмних засобів.
26.	Мороз	Деякі помилкові дії можуть привести до порушень цілісності інформації
27.	Загрево	Для блокування помилкових дій використовуються технічні й апаратно-програмні засоби
28.	Цінність	Дублювання інформації є ефективним способом забезпечення цілісності інформації
29.	Конфіденційність	Найбільш простим методом дублювання інформації є використання виділених ділянок на робочому диску
30.	Руйнування	Найбільшого поширення комп'ютерні віруси зазнали з розвитком персональних комп'ютерів
31.	Наклеп	Особливістю пакетного вірусу є розміщення його голови в пакетному файлі
32.	Техніка	Копіювання вірусу в середину файлу може статися в результаті помилки вірусу
33.	Практика	До шкідливого програмного забезпечення відносять також віруси і хробаки
34.	Зошит	Найуразливішими з точки зору безпеки є критичні комп'ютерні системи
35.	Папір	Технічні засоби і системи можуть лише випромінювати в довкілля сигнали

4. Для двох зареєстрованих користувачів інформаційної системи обрахувати стійкість їх паролів. Зробити висновок для чого у великих інформаційних системах зберігають паролі користувачів у вигляді хеш функцій.

5. Провести програмну реалізацію варіанту завдання 2 або 3. Продемонструвати викладачу робочу програму та представити лістинг у звіті у вигляді додатку .

ЗАВДАННЯ НА САМОСТІЙНУ ПІДГОТОВКУ

Реалізувати програмний варіант завдання. Продемонструвати викладачу робочу програму та отримати додатково 3 бали в рейтинг-лист.

КОНТРОЛЬНІ ПИТАННЯ

1. Які недоліки мають розглянуті алгоритми?
2. Яким чином можна покращити стійкість криптографічних алгоритмів?
3. Які типи криптографічних алгоритмів Ви знаєте?
4. Дайте визначення поняттю «електронний цифровий підпис».
5. Дайте визначення поняттю «стеганографія».