Лабораторна робота № 1-4

БАЗОВІ ШИФРИ. ЧАСТОТНИЙ КРИПТОАНАЛІЗ

Мета роботи: ознайомитися з базовими шифрами. Розглянути методику частотного криптоаналізу.

Використовуване програмне забезпечення: середа розробки GNU Octave.

1.1 Теоретичні відомості

В криптографії здавна використовувались два види шифрів: заміна та перестановка. Історичним прикладом шифру заміни є шифр Цезаря. Його сутність така: в строку виписується алфавіт, після чого під ним виписується той же алфавіт з циклічним зсувом на 3 букви вліво.

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЄЮЯ
ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЄЮЯАБВ

При зашифруванні буква відкритого тексту замінюється на букву, що знаходиться під нею в нижній строчці. Наприклад: РИМ – УЛП. Ключем в шифрі Цезаря є величина здвигу нижньої строки.

1.1.1 Шифр простої заміни

Подальший розвиток шифру Цезаря є очевидним: нижня строчка може бути записана з випадковим порядком букв. Такий шифр носить назву шифру простої заміни. Ключем такого шифру є порядок розташування букв в нижній строчці, так звана «таблиця заміни». Якщо в шифрі Цезаря існує тільки 33 варіанта ключів, то в шифрі простої заміни їх вже 33! (33 факторіал).

1.1.2 Квадрат Полібія

Одна з відомих модифікацій шифру простої заміни – квадрат Полібія. Візьмемо алфавіт з 32 букв. Виберемо ключ – будь-яке слово, в якому немає однакових букв. Запишемо його в перші клітинки квадрата розміром, наприклад, 4×8. В останні клітинки запишемо алфавіт за віднятком тих букв, що зустрічаються в ключі. Для зашифрування букви повідомлення замінюються на букви, що стоять *під* ними в квадраті Полібія. Наприклад:

Ключ – «**САВКОМ**».

Повідомлення – «**НЕЛЬЗЯ ПОМОЧЬ ТОМУ, КТО НЕ ЖЕЛАЕТ СЛУШАТЬ СОВЕТОВ**».

На рис. 1.1 представлено Квадрат Полібія для ключа «**САВКОМ**».

С	**А**	**В**	**К**
О	**М**	Б	Г
Д	Є	Ж	З
И	И	Л	Н
П	Р	Т	У
Ф	Х	Ц	Ч
Ш	Щ	І	І
Ь	Е	Ю	Я

Рисунок 1.1 – Квадрат Полібія

Зашифроване повідомлення:

«**УЙТМНКФАВАЪМЦАВЧГЦАУЙЛЙТЕЙЦБТЧЬЕЦМБАДЙЦАД**».

Для розшифрування букви шифротексту замінюються на ті букви, що стоять *над* ними в квадраті Полібія.

1.1.3 Шифр перестановки

Оберемо ціле додатне число, наприклад, 5. Створимо випадкову підстановку:

$$\begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,2\,5\,1\,4 \end{pmatrix}$$

Зашифруємо фразу:

«БАЖАЄШ БАГАТО ЗНАТИ, ТРЕБА МЕНШЕ СПАТИ».

Для цього доповнимо фразу до довжини кратної 5 випадковими символами та розіб’ємо на групи по 5 букв.

БАЖАЄ ШБАГА ТОЗНА ТИТРЕ БАМЕН ШЕСПА ТИВСЕ

Букви кожної групи переставимо згідно обраної підстановки.

Отриманий текст запишемо без пропусків.

«ААБЄЖГБШААНОТАЗРИТЕТЕАБНМПЕШАССИТЕВ»

При розшифруванні текст розбивається на групи по 5 букв і букви переставляються в зворотному порядку. Ключом шифру є степінь підстановки (тут 5) і порядок розташування чисел в нижньому рядку підстановки.

1.1.4 Шифр Тритемія

В XV столітті абат Тритемій (Германія) запропонував шифр на основі “таблиці Тритемія”. Для російського алфавіту вона має наступний вигляд:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЄЮЯ
БВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯА
ВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБ
ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВ
ДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГ
ЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГД
ЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕ
ЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁ
ЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖ
ИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗ
ЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИ
КЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙ
ЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙК
МНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛ
НОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМ
ОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМН
ПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНО
РСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОП
СТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПР
ТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРС
УФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТ
ФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУ
ХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФ
ЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХ
ЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦ
ШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧ
ЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШ
ЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩ
ЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫ
ЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪ
ЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬ
ЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭ
ЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮ

Рисунок 1.2 – Таблиця Тритемія для російського алфавіту

Тут перша строчка є одночасно і строчкою букв відкритого тексту. Перша буква тексту шифрується по першій строчці, друга – по другій і т.д. Після останньої строчки знову повертаємось до першої. Наприклад, слово "**КРИПТОГРАФИЯ**" зміниться на "**КСКТЦУИЧЗЭТЙ**". Однак, в такому варіанті, в шифрі Тритемія був відсутній ключ. В подальшому удосконалення шифру пішли по двом шляхам:

- введення випадкового порядку розташування букв алфавіту;
- застосування більш складного порядку вибору строк таблиці при шифруванні (по ключу).

1.1.5 Частотний крипто аналіз

Частотний криптоаналіз базується на застосуванні статистики для аналізу текстової інформації. Текст складається із слів, слова із літер. Кількість літер в кожній мові обмежена. Важливими характеристиками тексту є повторюваність літер, пар літер (біграм) і , взагалі, m-грам, поєднання літер друг с другом, чередування голосних і приголосних і т.д. Всі ці характеристики є достатньо стійкими і можуть бути використані для аналізу шифртекстів. В табл. 1.1 та 1.2 приведені однобуквені ймовірності англійської та російської мов.

Таблиця 1.1 - Однобуквені ймовірності англійської мови

Літера	Імовірність	Літера	Імовірність
A	0.0856	N	0.0707
B	0.0139	0	0.0797

C	0.0279	P	0.0199
D	0.0378	Q	0.0012
E	0.1304	R	0.0677
F	0.0289	S	0.0607
G	0.0199	T	0.1045
H	0.0528	U	0.0249
I	0.0627	V	0.0092
J	0.0013	W	0.0149
K	0.0042	X	0.0017
L	0.0339	Y	0.0199
M	0.0249	Z	0.0008

Таблиця 1.2 - Однобуквені ймовірності російської мови

Літера	**Імовірність**	**Літера**	**Імовірність**	**Літера**	**Імовірність**
А	0,062	К	0,028	Ф	0,002
Б	0,014	Л	0,035	Х	0,009
В	0,038	М	0,026	Ц	0,004
Г	0,013	Н	0,053	Ч	0,012
Д	0,025	О	0,090	Ш	0,006
Е	0,072	П	0,023	Щ	0,003
Ж	0,007	Р	0,040	Ы	0,016
З	0,016	С	0,045	Ь,Ъ	0,014
И	0,062	Т	0,053	Э	0,003
И	0,010	У	0,021	Ю	0,006
				Я	0,018

Процес криптоанализу можна представити наступним чином. Криптоаналітик підраховує частоти букв в шифротексті. Далі він бере в шифртексті символ, що зустрічається найбільш часто, и припускає, що це пробіл. Потім бере наступний символ, що зустрічається найбільш часто, и припускає, що це Е (для англійскої мови), и т.д. Шляхом проб і помилок такий метод може привести до рішення задачі. Крім того, при підставленні букв замість символів аналізованого шифртексту криптоаналітик враховує частоти появи сполучень із двох букв (діаграм), трьох букв (триграмм) і т.д.

1.2 Завдання на лабораторну роботу

1.2.1 Розробити програми шифрування та розшифрування наступними шифрами:

- шифр простої заміни;
- квадрат Полібія;
- шифр перестановки;
- шифр Тритемія з вибором строк по ключу;

(У якості ключа або сова, що аналізується, використовувати власне ім’я.)

1.2.2 Виконати частотний криптоаналіз отриманих зашифрованих текстів.

1.3 Зміст звіту

1.3.1Титульний лист, тема і мета роботи.
1.3.2Відповіді на контрольні питання.
1.3.3Тексти програм.
1.3.4Обране повідомлення для шифрування.
1.3.5Обраний ключ.
1.3.6Зашифроване повідомлення.
1.3.7Розшифроване повідомлення.
1.3.8Результати проведення частотного криптоаналізу.

1.4 Контрольні питання

1.4.1Опишіть шифр Полібія.
1.4.2Опишіть шифр простої заміни.
1.4.3Опишіть шифр Тритемія.
1.4.4Опишіть шифр перестановки.
1.4.5Чи є шифр Полібія шифром простої заміни?
1.4.6Як залежить стійкість шифру від довжини ключа?
1.4.7Опишіть метод частотного криптоанализу.
1.4.8 В яких випадках можна застосовувати метод частотного криптоанализу?