Лабораторна робота №1

Шифрувальна система на основі шифру Цезаря.

Мета:

Створити просту криптографічну систему на основі шифру Цезаря та дослідити її роботу.

Обладнання:

- персональний комп'ютер з встановленою операційною системою Windows
- будь-яка мова програмування.

Завдання:

1. Створити просту криптографічну систему на основі шифру заміни.
2. Перевірити її роботу.

Література:

1. М.Масленников. Практическая криптография. БХВ-Петербург,2003. – 464с.
2. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные коды на языке С. 1996.
3. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети. М."ДМК", 2004. – 616 с.

Теоретичні відомості.

Під *криптографією* будемо розуміти область знань, що відноситься до методів і засобів перетворення повідомлень у незрозумілу для сторонніх осіб форму, а також перевірки істинності цих повідомлень.

Під *криптоаналітикою* будемо розуміти засоби і методи, спрямовані на подолання криптографічного захисту.

Сукупність криптографії та криптоаналітики називається *криптологією*.

Розшифровуванням будемо називати відновлення вихідного повідомлення при відомому ключі шифрування.

Дешифруванням будемо називати процес відновлення вихідного повідомлення при невідомому ключі шифрування.

Таким чином, ті, кому призначено шифроване повідомлення його *розшифровують*, а ті, хто перехоплює його, намагаються *дешифрувати*.

Клод Шеннон у своїй роботі „Теорія связи в секретных системах" узагальнив накопичений до нього досвід розробки шифрів. Вияснилося, що навіть у дуже складних шифрувальних системах можна виділити в якості складових частин шифри заміни, шифри перестановки та їх комбінації. Деякі відомості про ці прості шифри можна знайти у художній літературі, зокрема „Золотий жук" Едгара По і „Пляшущие человечки" Артура Конан Дойла.

Розглянемо два приклади простих шифрів.

Шифр „Сцитала". Цей шифр відомо з часів війни Спарти проти Афін у V ст. до н.е. Для його реалізації використовувалась т.зв. „сцитала" – циліндричний жезл певного діаметру. На сциталу намотували вузьку папірусну стрічку і на ній писали повідомлення вздовж осі сцитали. Коли стрічку знімали, на ній залишалися незрозумілі літери. Для розшифровки повідомлення адресат намотував стрічку на такий самий жезл і читав повідомлення. В цьому шифрі перетворення оригінального тексту у шифрований зводиться до перестановки літер оригінального тексту. Тому клас таких шифрів отримав назву *шифру перестановки*.

Шифр Цезаря. Цей шифр реалізує таке перетворення відкритого тексту: кожна літера замінюється третьою після неї літерою алфавіту, який вважається написаним по колу, тобто після „я” йде „а”. Відмітимо, що Цезарь замінював її третьою літерою, але можна міняти і будь-якою іншою. Головне, щоби адресат цього повідомлення знав величину і напрямок цього зсуву. Клас шифрів, до якого відноситься шифр Цезаря, називається *шифрами заміни*.

З цього, напевне зрозуміло, що створення хорошого шифру є задачею непростою. Тому бажано збільшити час життя шифру, але тут зростає імовірність того, що криптоаналітики противника зможуть розкрити шифр і читати зашифровані повідомлення. Якщо у шифрі є змінний „ключ”, то його заміна призводить до того, що розроблені противником методи вже не дадуть ефекту.

Під *ключем* будемо розуміти змінний елемент шифру, який застосовується для шифрування конкретного повідомлення. Наприклад, у шифрі сцитала ключом є діаметр жезлу, а у шифрі Цезаря – величина і напрямок зсуву літер шифротексту відносно літер відкритого.

Описані міркування призвели до того, що безпека повідомлень, що шифруються, в першу чергу стала забезпечуватися ключем. Сам шифр, шифромашина або принцип шифрування прийнято вважати відомими суперникові і доступними для попереднього вивчення, але у шифрі з’явився невідомий елемент –ключ, від якого істотно залежать застосовувані перетворення інформації. Тепер користувачі, перш ніж обмінятися шифрованими повідомленнями, повинні обмінятися ключем, за допомогою якого можна прочитати зашифроване повідомлення. А для криптоаналітиків, які хочуть прочитати перехоплене повідомлення, основною задачею є знаходження ключа.

Принципи частотного криптоаналізу

Встановлено, що в будь-якій мові літери абетки зустрічаються нерівномірно. Якщо взяти достатньо великий текст (порядку мільйона символів) загального змісту та підрахувати частоту, з якою кожна літера абетки зустрічається в цьому тексті, ми побачимо, що найчастіше в українських текстах зустрічається літера „О” (0.082), а в російських та англійських – „Е” (0.071 та 0.12 відповідно). Звичайно, в залежності від тематики текстів, частотні характеристики його змінюються, але тенденція залишається незмінною.

На цьому факті ґрунтується метод частотного криптоаналізу. Якщо метод шифрування „перехопленої шифровки” не приховує частотних особливостей мови (а саме таким і є шифр Цезаря), то криптоаналітики виконують наступні дії:

1. Підраховують відносні частоти, з якими кожна літера абетки зустрічається в „перехопленому” повідомленні. Робиться це за формулою: *частота=кількість/довжина*; де *кількість* – скільки разів літера зустрічається в повідомленні; *довжина* – кількість літер в повідомленні.
2. Літеру з найбільшою відносною частотою ототожнюють з літерою, яка має найбільшу частоту в таблиці.
3. Визначають величину зсуву.
4. Пробують дешифрувати повідомлення з визначеною в п.3 величиною зсуву. Якщо отримано логічний зв‘язний текст, повідомлення вважається дешифрованим. Якщо зв‘язного тексту не отримано, процедуру продовжують.
5. Літеру з найбільшою відносною частотою ототожнюють з літерою, яка має другу найбільшу частоту в таблиці.
6. Пробують дешифрувати повідомлення, перебираючи частотну таблицю, поки не отримують зв‘язного тексту.

Цим методом Вам необхідно користуватися для криптоаналізу в цій лабораторній роботі.

Практична частина.

1. Підгрупа розбивається на пари за бажанням.
2. Один з членів пари пише програму шифрування та розшифрування тексту шифром Цезаря. Програма шифрування повинна задовольняти таким умовам: читати файл з набраним текстом; шифрувати текст з довільним зміщенням, значення якого вводиться з клавіатури; виводити зашифрований текст у файл. Програма розшифровування повинна задовольняти таким умовам: читати файл із зашифрованим текстом; розшифровувати його; видавати на екран розшифрований текст.
3. Другий з членів пари пише програму криптоаналізу методом частотного аналізу. Програма криптоаналізу повинна задовольняти наступним вимогам: а) читати „перехоплений" зашифрований файл; б) розраховувати відносну частоту, з якою зустрічається кожний символ у „перехопленому" файлі.
4. Перший з пари зашифровує повідомлення і передає його для криптоаналізу другому. Другий дешифрує отримане повідомлення методом частотного криптоаналізу і знаходить ключ шифрування (величину зміщення).

Звіт з лабораторної роботи повинен містити:
1. Протоколи дій обох членів пари.
2. Розшифровані тексти та значення ключа, знайдені за допомогою криптоаналізу.

Контрольні запитання.

1. Що називається криптографією? Для чого вона використовується?
2. Що називається криптоаналітикою? Для чого вона використовувається?
3. Що називається криптологією?
4. Яка різниця між розшифровкою і дешифровкою?
5. Що називається ключем шифрування? Для чого він використовується?
6. Які Ви знаєте типи шифрів? Наведіть приклади.
7. Охарактеризуйте „шифр сцитала".
8. Охарактеризуйте шифр Цезаря.
9. Які б ви запропонували методи розкриття шифру сцитала?