ный характер. Таким образом, мы видим, что система управления с нечетким регулятором имеет значительно более высокую устойчивость к изменяющимся внешним условиям, обеспечивает лучшую надежность и долговечность системы отопления и создает более комфортные условия внутри здания.

1. Дорф Р., Бишоп Р. Современные системы управления / Пер. с англ. – М. : Лаборатория Базовых Знаний, 2002. – 832 с. 2. Гостев В.И. Нечеткие регуляторы в системах автоматического управления. – К. : Издательство "Радіоаматор", 2008. – 972 с. 3. Гостев В.И. Проектирование нечеткого регулятора при идентичных возведенных в степень треугольных функциях принадлежности // Інформаційна безпека. – 2009. – № 1 (1). – С. 51–58.

Надійшла до редколегії 16.02.10

УДК 004.6

В.Б. Дудикевич, д-р. техн. наук, проф.,
В.О. Ракобовчук, здобувач,
В.М. Стеренчук, здобувач

ДОСЛІДЖЕННЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ НА ПРИКЛАДІ ВИБРАНИХ ІСТОРИЧНИХ ШИФРІВ В ПАКЕТІ CRYPTOOL

Робота присвячена дослідженню можливості використання пакету CrypTool з метою навчання спеціалістів для подальшої роботи в галузі захисту комп'ютерної інформації. Докладно описані імітаційні можливості пакету для застосування методів криптографічного аналізу історичних алгоритмів шифрування.

Ключові слова: захист комп'ютерної інформації, криптографічний аналіз.

Work is devoted to research of possibility of the using the package CrypTool with the purpose of specialists studies for subsequent work in industry of computer information defence. Imitation possibilities of package are thoroughly described for application of cryptographic analysis methods of historical enciphering algorithms.

Keywords: computer information defence, cryptographic analysis.

Вступ. В зв'язку з розповсюдженням інформаційних технологій і збільшенню кількості локальних і регіональних комп'ютерних мереж пошук і дослідження математичних методів криптографічних перетворень є одною з важливіших складових рішення проблеми захисту інформації. На основі історичних знань розробляються нові криптографічні системи і алгоритми. Тому знання первинно створених шифрів є запорукою успіху при розробці нових більш складних криптографічних алгоритмів.

Робота присвячена дослідженню можливості використання пакету CrypTool з метою навчання спеціалістів для подальшої роботи в галузі захисту комп'ютерної інформації.

В даній роботі покроково описані методики аналізу історичних шифрів заміни та перестановок.

Традиційним завданням криптографії було забезпечення конфіденційності текстової інформації, тобто приховування її семантичного змісту шляхом шифрування. Схему традиційного (симетричного) шифрування (рис. 1) можна описати використовуючи п'ять основних понять: відкритий або явний текст; алгоритм шифрування – процес спеціальних криптографічних перетворень, який виконується над символами відкритого тексту; таємний ключ – параметр, який також подається на вхід алгоритму шифрування і є необхідний для безперешкодного здійснення шифрування текстів; шифрований текст або шифрограма; алгоритм дешифрування.

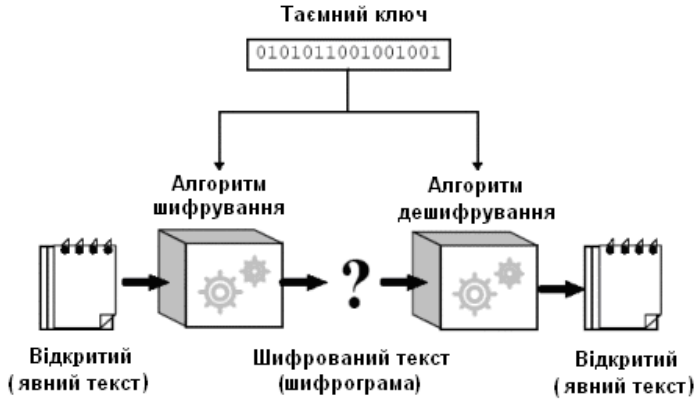

Рис. 1. Узагальнена схема традиційного шифрування

Є два основні методи, криптографічних перетворень: підстановки **(**заміна символів відкритого тексту на інші символи того самого або іншого алфавіту) і перестановок **(**перемішуванні символів відкритого тексту, отже шифрограма містить лише ті символи і в тій самій кількості, що і вихідний явний текст).

Однією із важливих характеристик шифру є число його можливих ключів, оскільки взлом шифру може здійснюватися перебором можливих ключів.

Шифр підстановки кожен символ відкритого тексту замінює на деякий інший. В класичній криптографії розрізняють чотири типи шифру підстановки:

1. Одноалфавітний шифр підстановки (шифр простої заміни) – шифр, при якому кожен символ відкритого тексту замінюється на деякий, фіксований при даному ключі символ того ж алфавіту. Приклади: шифри Цезара, Rot-13.

2. Гомоморфний (однозвучний) шифр підстановки схожий на одноалфавітний за винятком того, що символ відкритого тексту може бути замінений одним з декількох можливих символів.

3. Поліграммний шифр підстановки замінює не один символ, а цілу групу. Приклади: шифр Плейфера, шифр Хілла.

4. Багатоалфавітний шифр підстановки складається з декількох шифрів простої заміни. Приклади: шифр Віженера, шифр Бофора, Варнама (одноразового блокноту).

В шифрі Цезаря як ключ використовується одна буква із алфавіту. Залежно від позиції цієї букви в алфавіті, букви шифрованого тексту зсуваються в замкнених циклах. Якщо алфавіт складається лише із великих букв (класичний випадок), пересування на одну позицію відбудеться, якщо вписати літеру "B", на дві – залітери "C" і т.д. При дешифруванні зашифрований текст пересувається в протилежному напрямі. Отже, модель шифрування та дешифрування можна подати такими формулами

$$C_i = (P_i + K) \bmod A, \quad (1)$$

$$P_i = (C_i - K) \bmod A, \quad (2)$$

де P_i і C_i - номер *i*-ої букви відповідно відкритого тексту і шифрограми; K – ключ; A – розмір алфавіту, наприклад для англійського алфавіту 26.

Особливим випадком шифру Цезаря є шифр Rot-13, який інколи застосовують на чатах та в дискусійних групах. Шифр Rot-13 пересуває кожну букву на 13 позицій, що відповідає шифру Цезаря з ключем "M". Повторне застосування шифру Rot-13 до шифрограми відтворює явний текст.

У класичному варіанті для шифрування і дешифрування за Віженером використовувалася таблиця алфавітів, так звана tabula recta. Щодо англійського алфавіту таблиця Віженера складається з рядків по 26 символів, причому кожен наступний рядок зсувається на одну позицію

Для шифруваня кожної букви відкритого тексту шифр Віженера використовує різні алфавіти з цієї таблиці залежно від символу ключового слова. У шифрі Віженера ключ задається набором з K символів, які по черзі визначають рядок (алфавіт) для заміни поточної букви відкритого тексту. Можна сказати, що шифр Віженера складається з послідовності декількох шифрів Цезаря із різними значеннями зсуву.

Дешифрування здійснюється у зворотному напрямку: із рядка таблиці Віженера, що відповідає першому символу ключового слова ***K*** знаходять першу літеру зашифрованого тексту **V** і за стовпцем, якому належить ця літера зчитують букву відкритого тексту **L** і т.д.

Модель процесу шифрування і дешифрування за Віженером можна описати формулами

$$c_i = (p_i + k_i) \bmod A, \quad (3)$$

$$p_i = (c_i - k_i) \bmod A, \quad (4)$$

де k_i – *i*-й символ ключа.

Повторне застосування двох і більше шифрів Віженера називатється складеним шифром Віженера і описується рівнянням:

$$C_i = (P_i + K_i + L_i + \ldots + S_i) \bmod A, \quad (5)$$

де ключі K_i, L_i ..., S_i можуть мати різні періоди, а період їх суми $(K_i + L_i + \ldots + S_i)$ буде найменшим спільним кратним окремих періодів.

Якщо використовується шифр Віженера з "необмеженим" ключем, що не повторюється впродовж відкритого тексту, то одержуємо шифр одноразового блокноту (Вернама). Якщо ключем служить текст, що має зміст, то це шифр із біжучим ключем.

Експериментальна частина. Для вивчення алгоритмів шифрування і дешифрування спочатку створюється робочий файл у пакеті CrypTool з розширенням *.txt. Відкривається в діалоговому вікні **Шифрування** опція **Історичний,** це дозволяє обрати яким саме історичним шифром потрібно шифрувати (рис. 2).

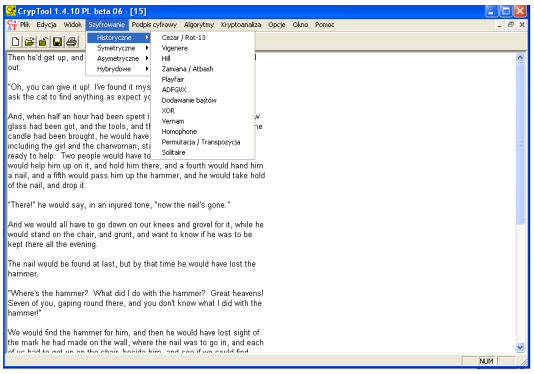

Рис. 2. Вибір історичного шифрувального алгоритму

Для шифру Цезаря/Rot-13 (рис. 3). В діалоговому вікні можна задати всі опції, які необхідно для шифрування методом Цезаря і Rot-13.

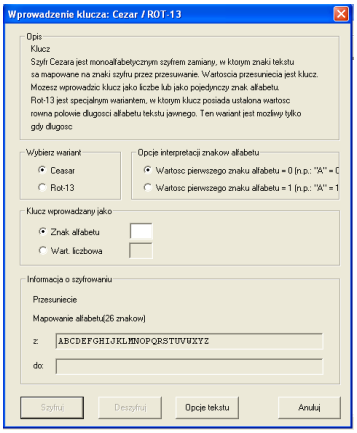

Рис. 3. Ввід ключа шифру Цезара

Вводиться буква алфавіту і після вибору опції **Шифруй з**'явиться вікно із зашифрованим текстом. Відкритий текст може бути отриманий через дешифрацію документа. Потрібно при активному вікні з шифрограмою, знову вибрати в меню Шифрування \ Історичне \ Ceasar / Rot-13 варіант Цезар і ввести ключ, за допомогою якого даний документ був зашифрований. Щоб відтворити з шифрограми дійсний текст треба клікнути на клавішу **Дешифруй**.

Ключ для алгоритму кодування Віженера вводиться в діалог Ввід ключа (рис. 4).

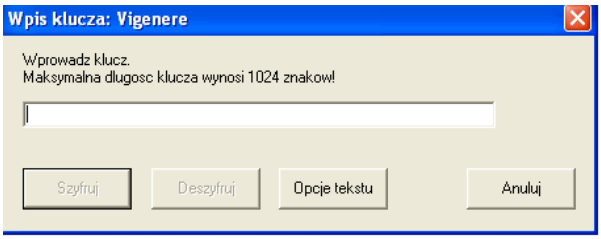

Рис. 4. Вікно вводу ключа для шифру Віженера

За допомогою програми CrypTool можна легко визначати ентропію відкритого тексту через меню Криптоаналіз (Kryptoanaliza) \ Засоби аналізу (Narzedzia analizy) \ Entropia (рис. 5) і частості виступу окремих знаків в тексті з допомогою меню Kryptoanaliza \ Narzedzia analizy \ Histogram (рис. 6).

Ентропія документа показує вміст в ньому інформації і вимірюється в бітах на знак.Для документів, що складаються тільки з великих букв ентропія знаходиться в межах від 0 біт/знак (в документах які мають тільки один знак) до $\log_2(26)$ біт/знак = 4.700440 біт/знак (в документах в яких всі 26 букв з'являються з однаковою імовірністю). Для документів, які можуть мати всі знаки від 0 до 256, ентропія знаходиться в межах від 0 біт/знак (в документах, які складаються тільки з одного знаку) до $\log_2(256)$ біт/знак = 8 біт/знак (в документах в яких всі 256 знаків з'являються однаково часто).

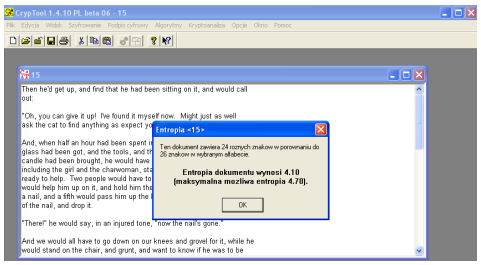

Рис. 5. Аналіз ентропії відкритого тексту

Гістограма документа показує частість появи знаків в документі в графічній формі в інтерактивному вікні. По осі абцис гістограми відкладаються всі знаки із вибірки знаків, числа від 0 до 255 за таблицею ASCII. Частота появи (у відсотках) кожного знаку показана на осі ординат. На рис. 6,7 показані бінарні гістограми початкового і зашифрованих текстів з використанням алгоритму Цезара.

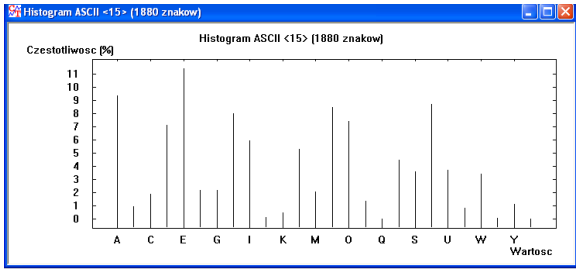

Рис. 6. Аналіз частоти знаків в явному тексті

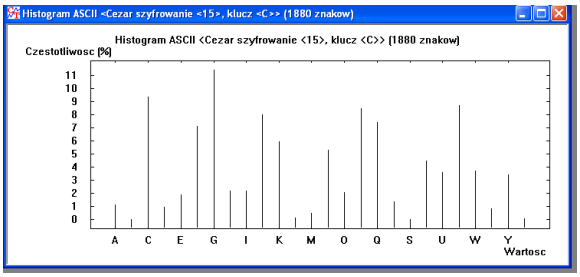

Рис. 7. Аналіз частоти знаків в шифрованому тексті

Аналіз гістограм зашифрованого документу показує, що багатократність виступу знаків при ключі С були пересунуті на три позиції. Означає це, що вибраний алгоритм шифрування не є безпечним.

Якщо вибрати в меню Kryptoanaliza \ Algorytmy historyczne \ tylko szyfr документ буде автоматично проаналізований і можливе отримання ключа, який використовувався для шифрування документу.

За допомогою меню Kryptoanaliza/Algorytmy historyczne/Tylko szyfr, текст буде автоматично проаналізований. Наприклад, якщо необхідно знайти ключ для документу зашифрованого за допомогою алгоритму Віженера, то спочатку необхідно відкрити вікно autokorelacja (автокореляція). Після чого є можливість визначення довжини ключа за регулярними піками автокореляційної функції (11 знаків) і отримати ключ, яким був зашифрований документ (рис. 8).

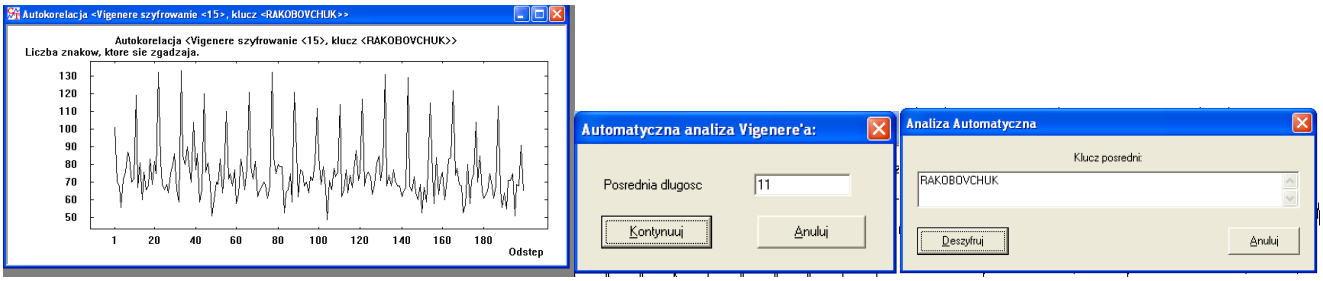

Рис. 8. Автокореляційний метод аналізу

Ключ для алгоритму кодування методом перестоновки вводиться в діалоговому вікні пермутація/транспозиція (рис. 9).

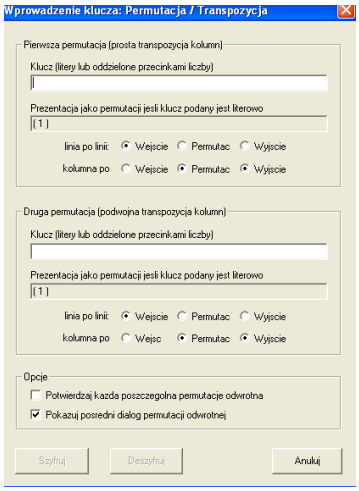

Рис. 9. Приклад шифрування методом транспозиції

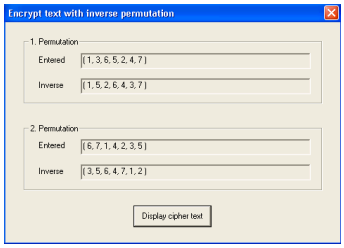

Рис. 10. Застосування пермутації і інверсії пермутації

В кожне, з двох полів до заповнення, можна вписати ключове слово або нумеричну перестановку. Заповнення першого поля обов'язкове. Заповнення другого поля є опціональним. Якщо було заповнено друге поле, створюється не одна, а дві пермутації. Для кожної пермутації додатково можна встановити виконання пермутації з колонок або з віршів. Максимальна довжина пермутації 26. Може бути вписано або 26 великих букв, чи секвенція чисел, тобто пермутація 1, 2 ..., 26.

Через активацію відповідного поля вибору в групі опції, можна встановити шифруванням або дешифруванням вхідної пермутації, або анулювати дії.

Можна отримати більше інформації про вибір пермутації і її інверсії якщо клікнути кнопку шифрування або дешифрування (рис. 10).

Висновки. Пакет імітаційного моделювання алгоритмів шифрування і дешифрування CrypTool можна використовувати для навчання спеціалістів для подальшої роботи в галузі захисту комп'ютерної інформації.

1. Столлингс Вильям. Основы защиты сетей. Приложения и стандарты: Пер. с англ. – М.: Издательский дом "Вильямс", 2002. – 432 с. 2. Петраков А.В. Основы практической защиты информации. – М.: Радио и связь. 1999.- 368с. 3. Брюс Шнайер. Практическая криптография. – М.: Издательский дом "Вильямс", 2005. – 424 с.

Надійшла до редколегії 8.02.10