Лабораторна робота №2

Тема: Стійкість парольного захисту електронних документів та архівів

Мета: Формування умінь і навичок створення стійких паролів. Отримання знань методів і способів подолання парольного захисту та навичок використання відповідного програмного забезпечення. Закріплення знань файлової структури, умінь і навичок використання можливостей віртуальних принтерів, архіваторів, текстових і табличних редакторів для організації парольного захисту.

Теоретичні відомості

Практично всі користувачі використовують та створюють PDF-файли, офісні документи, архівують свої файли за допомогою популярних архіваторів ARJ, ZIP, RAR та захищають їх паролями, за допомогою яких вміст цих файлів шифрується. Для кращого запам'ятовування користувачі створюють нескладні паролі, які базуються на звичайних словах (кажуть — слова зі словника). Тому що алгоритм шифрування файлів певного типу є відомим, то підбір таких паролів не складає особливих труднощів і у більшості випадків має певне програмне забезпечення. Зрозуміло, що саме широко розповсюджене програмне забезпечення можна використовувати для визначення стійкості паролю до файлів. До таких програм слід віднести: Advanced Archive Password Recovery (ARCHPR), Advanced ARJ Password Recovery (AAPR), Advanced ZIP Password Recovery (AZPR), Advanced RAR Password Recovery (ARPR), Advanced PDF Password Recovery (APDFPR), Advanced Office Password Recovery (AOPR) чи подібними до них. Всі вони використовують наступні загальні алгоритми:

- послідовний перебір різних комбінацій символів (Brute-force чи „грубої сили");
- послідовний перебір по масці, якщо відома хоча б частина паролю;
- атака по словнику, коли перебір виконується серед найуживаніших паролів;
- гібридний метод (атака по словнику + метод послідовного перебору).

Крім цього, для архівів можливий злам захисту на основі частини "відомого тексту" (known-plaintext attacks). На сьогодні програми зламу захисту архівів здатні:

- забезпечувати швидкість перебору паролів понад два мільйони в секунду;
- підтримувати всі методи стискування;
- працювати з архівами, що саморозпаковуються;
- встановлювати параметри перебору паролів: діапазон кодової довжини, кодову сторінку, набір символів тощо;
- підтримувати не англійські літери при використанні методу "грубої сили";
- атакувати за допомогою "словника" з можливістю його зміни.

Простий засіб підвищення надійності шифрування може забезпечуватись через збільшення довжини паролю від 10 символів. Однак жоден пароль не може бути безпечним на 100 відсотків. Принципово його можна відгадати або розшифрувати. Надійний пароль важко розкрити стороннім особам. Такі паролі слід використовувати у всіх випадках, коли потрібен пароль: наприклад, для входу на комп'ютер, в обліковому записі Інтернету або для захисту документів.

Надійні паролі:

- відрізняються для різних ідентифікаторів;
- складаються не менше, ніж з семи знаків;
- містять одночасно великі й малі літери, цифри та спеціальні символи на позиціях від другої;
- мають вигляд випадкової сукупності знаків;
- не містять повторюваних знаків;
- не містять послідовних знаків, наприклад, *1234*, *abed* або *qwerty*;
- не дають змоги розпізнати будь-яку закономірність, тематику або цілі слова будь-якою мовою;
- не використовують цифри або символи замість подібних до них знаків (наприклад, $ замість S або 1 замість 1), оскільки це полегшує розкриття паролю;
- не містять частково або повністю вашого імені користувача для входу до комп'ютера, інтернету або до мережі;
- не вказують на ваші особисті дані, ключові дати чи дані близьких вам людей.

Для підвищення захисту паролі часто змінюються, при цьому, новий пароль повинен повністю відрізнявся від старого, і в ньому не використовують жодної частини старого паролю.

Практична частина

1. Зробіть текстовий документ (1-2 повних сторінок) і збережіть його з іменем, наприклад, *Proba.docx*.
2. За допомогою електронних таблиць (MS Excel або LibreOffice Calc) зробіть наступну таблицю для фіксування часу пошуку паролів різної довжини для документів різних типів:

Тривалість пошуку паролів різної довжини документів різних типів, с

Тип документа	Довжина паролю (символів)						
	1	2	3	4	5	6	N
PDF							
RAR							
ZIP							
DOCX							

3. Збережіть файл *Proba.docx* у форматі PDF під назвою *Proba1.pdf*, заборонивши копіювання та друк його фрагментів. Для цього:
   3.1. Розпочніть друк завантаженого документа на віртуальному принтері **PDF Creator**;
   3.2. У вікні основних параметрів PDF-файла перейдіть у вікно додаткових параметрів створення;
   3.3. Оберіть параметри PDF-документа, віднайдіть і встановіть на його відповідній закладці прапорець **Использовать защиту**, прапорець задання паролю та редагування, та прапорці, які забороняють копіювання та друк PDF-документа;
   3.4. Закрийте вікно додаткових параметрів із збереженням внесених змін;
   3.5. Продовжіть створення PDF-документу та введіть пароль із одного символу для його редагування.
4. Самостійно почергово збережіть файл *Proba.docx* у форматі PDF під назвами *Proba2.pdf*, *Proba3.pdf*, *Proba4.pdf*, *Proba5.pdf*, задаючи паролі відповідно з 2, 3, 4 та 5 символів чи знаків.
5. Збережіть файл *Proba.docx* у форматі PDF під назвою *Proba6.pdf* з шифруванням паролем його вмісту. Для цього:
   5.1. Відкрийте файл *Proba.docx*, наприклад, у текстовому процесорі MS Word 2010;
   5.2. Розпочніть створення PDF-файла, використовуючи пункт стрічки меню **Файл – Сохранить как**, після чого вкажіть у відповідному вікні назву нового файла та його тип;
   5.3. За допомогою кнопки **Параметры** у нижній частині цього вікна відкрийте вікно параметрів PDF-файла, встановіть у ньому прапорець **Зашифровать документ с помощью пароля** та збережіть внесені зміни;
   5.4. Продовжіть створення PDF-документа та введіть пароль для його редагування.
6. Самостійно збережіть файл *Proba.docx* у форматі PDF під назвами *ProbaS.pdf*, зашифрувавши його послідовними знаками, наприклад, *1234*, *abed* або *qwerty*.
7. Самостійно збережіть файл *Proba.docx* у форматі PDF під назвами *ProbaN.pdf*, зашифрувавши його “не словниковим” паролем.
8. Підберіть паролі до створених захищених PDF-документів за допомогою програми Advanced PDF Password Recovery (APDFPR). Для цього почергово:
   8.1. Самостійно завантажте програму APDFPR (рис. 1), врахувавши, що вона створена корпорацією Elcomsoft;
   8.2. За допомогою кнопки **Открыть** оберіть PDF-файл з яким проводиться експеримент;
   8.3. У списку **Тип атаки** оберіть вид зламу **По словарю**;
   8.4. Для початку підбору натисніть кнопку **Старт**;
   8.5. Якщо підібрати пароль по словнику не вдалося, то самостійно відновіть його послідовним перебором, обираючи необхідний набір символів та максимальну довжину (на закладці **Длина**). Тривалість зламу в секундах, яку визначає сама програма, занесіть у перший рядок із даними порівняльної таблиці. Коли прогнозована тривалість зламу перевищує 10 хвилин, то зупиніть процес підбору та внесіть у таблицю прогнозований час перебору.

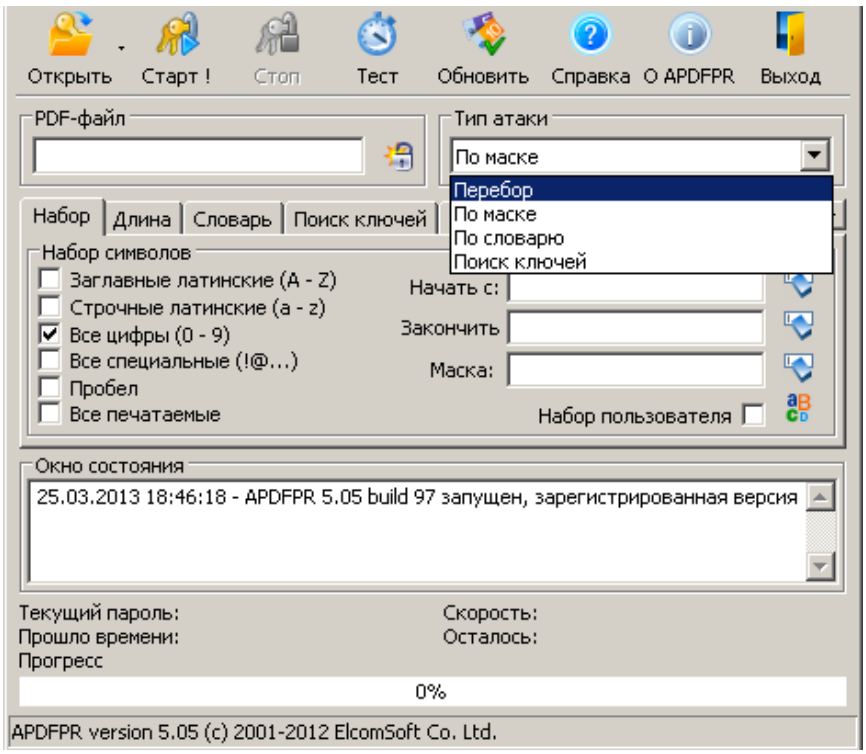

Рис. 1. Вибір виду зламу у програмі APDFPR

9. Зробіть архів файла *Proba.docx* у ZIP та RAR-архівах під назвами *Proba1.zip*, *Proba2.zip*, *Proba3.zip*, *Proba4.zip*, *Proba5.zip*, *Proba6.zip*, *ProbaS.zip*, *ProbaN.zip*, *Proba1.rar*, *Proba2.rar*, *Proba3.rar*, *Proba4.rar*, *Proba5.rar*, *Proba6.rar*, *ProbaS.rar*, *ProbaN.rar*, де остання цифра назви вказує на довжину пароля. Для цього:
   9.1. В контекстному меню файла *Proba.docx* оберіть пункт **Упаковать в архив**;
   9.2. У вікні архіватора, яке з'явиться на екрані, на закладці **Общие** вкажіть назву файла архіву та його формат, а на закладці **Дополнительно** натисніть кнопку **Установить пароль** для його задання;
   9.3. Самостійно завершіть створення архіву.
10. Самостійно підберіть паролі до створених захищених архівів за допомогою програми Advanced Archive Password Recovery (ARCHPR), використовуючи способи словника та послідовного перебору (рис. 2). Тривалість зламу в секундах, яку визначає сама програма, занесіть у відповідно у другий та третій рядки з даними порівняльної таблиці. Якщо прогнозована тривалість зламу перевищує 7 хвилин, то зупиніть процес підбору та внесіть у таблицю прогнозований час перебору.

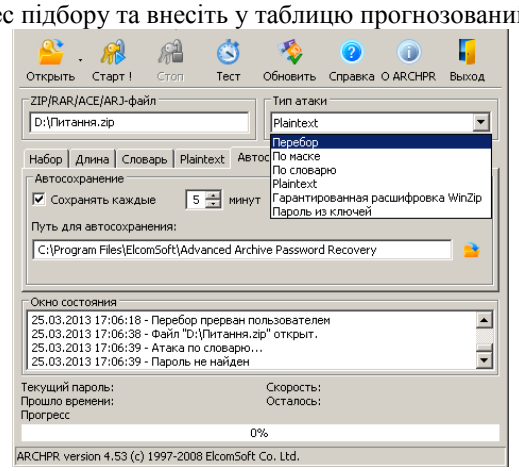

Рис. 2. Вибір виду зламу у програмі ARCHPR

11. Зробіть спільний ZIP-архів файлів *Proba.docx* та *ZaxLR6.doc* з надійним паролем та назвою *ProbaSumisn.zip*, попередньо виділивши ці файли у вікні провідника. Зробіть архів без пароля файлу *ZaxLR6.doc* у ZIP-архів *ZaxLR6.zip*.
12. Зробіть підбір паролю архіву *ProbaSumisn.zip* методом підбору на основі частини "відомого тексту". Для цього:

12.1. Завантажте програму ARCHPR;
12.2. За допомогою кнопки **Открыть** оберіть файл *ProbaSumisn.zip* для зламу;
12.3. У списку **Тип атаки** оберіть вид зламу **Plaintext** (рис. 2);
12.4. Перейдіть на закладку **Plaintext** та оберіть на ній файл *ZaxLR6.zip*, як такий, що містить частину "відомого тексту";
12.5. Для початку підбору натисніть кнопку **Старт**.

13. Зробіть висновки про надійність паролів архіву декількох файлів, якщо вони містять доступні файли.
14. Самостійно збережіть файл *Proba.docx* під назвами *Proba1.docx*, *Proba2.docx*, *Proba3.docx*, *Proba4.docx*, *Proba5.docx*, вказавши **паролі для їх відкриття** відповідної довжини.
15. Самостійно збережіть файл *Proba.docx* під назвами *Proba6.docx*, *ProbaS.docx*, *ProbaN.docx*, використовуйте відповідно **паролі для шифрування** довжиною 6 символів, послідовності символів та надійний пароль.
16. Самостійно підберіть паролі до створених захищених архівів за допомогою програми Advanced Office Password Recovery (AOPR), для чого використовуйте способи словника та послідовного перебору (рис. 3). Тривалість визначення паролю у секундах, яку визначає сама програма, занесіть у порівняльну таблицю. Якщо прогнозована тривалість визначення паролю перевищує 7 хвилин, то зупиніть процес підбору та внесіть у таблицю прогнозований час перебору.

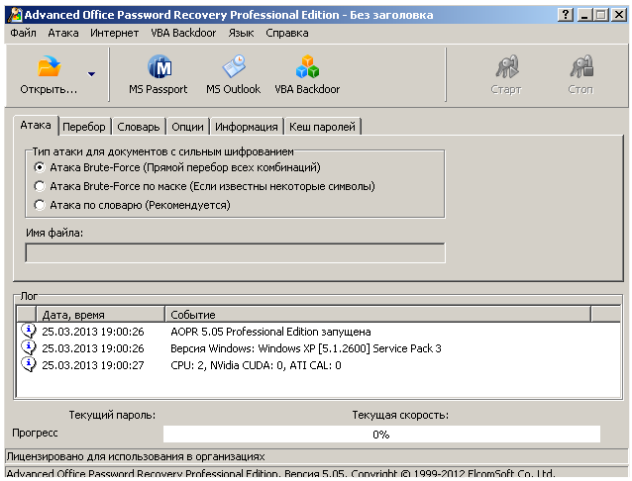

Рис. 3. Вибір виду підбору паролю у програмі AOPR

17. На основі даних порівняльної таблиці побудуйте графіки залежностей тривалості процесу визначення паролю від його довжини для різних форматів файлів. Визначте тип залежності? Спрогнозуйте тривалість процесу визначення паролю при його довжині 10 символів.
18. Надайте звіт з виконаної роботи.

Контрольні запитання

1. Які види підбору паролів використовуються для документів та архівів, що мають захист?
2. Який додатковий вид підбору паролів застосовується до архівів? Як такий він реалізується?
3. Які вимоги висуваються до надійних паролів?
4. Чому недоцільно дозволяти програмам запам’ятовувати паролі?
5. Чому не варто встановлювати один пароль для різних ресурсів?
6. Які файли недоцільно включати у спільні архіви при шифруванні паролем? Чому?