ПРАКТИЧНА РОБОТА 24

Тема. Шифрування в документах Microsoft Office.

Мета. Ознайомити з можливостями шифрування та розшифруванням документів Microsoft Office за допомогою мови програмування Delphi.

ТЕОРЕТИЧНІ ВІДОМОСТІ

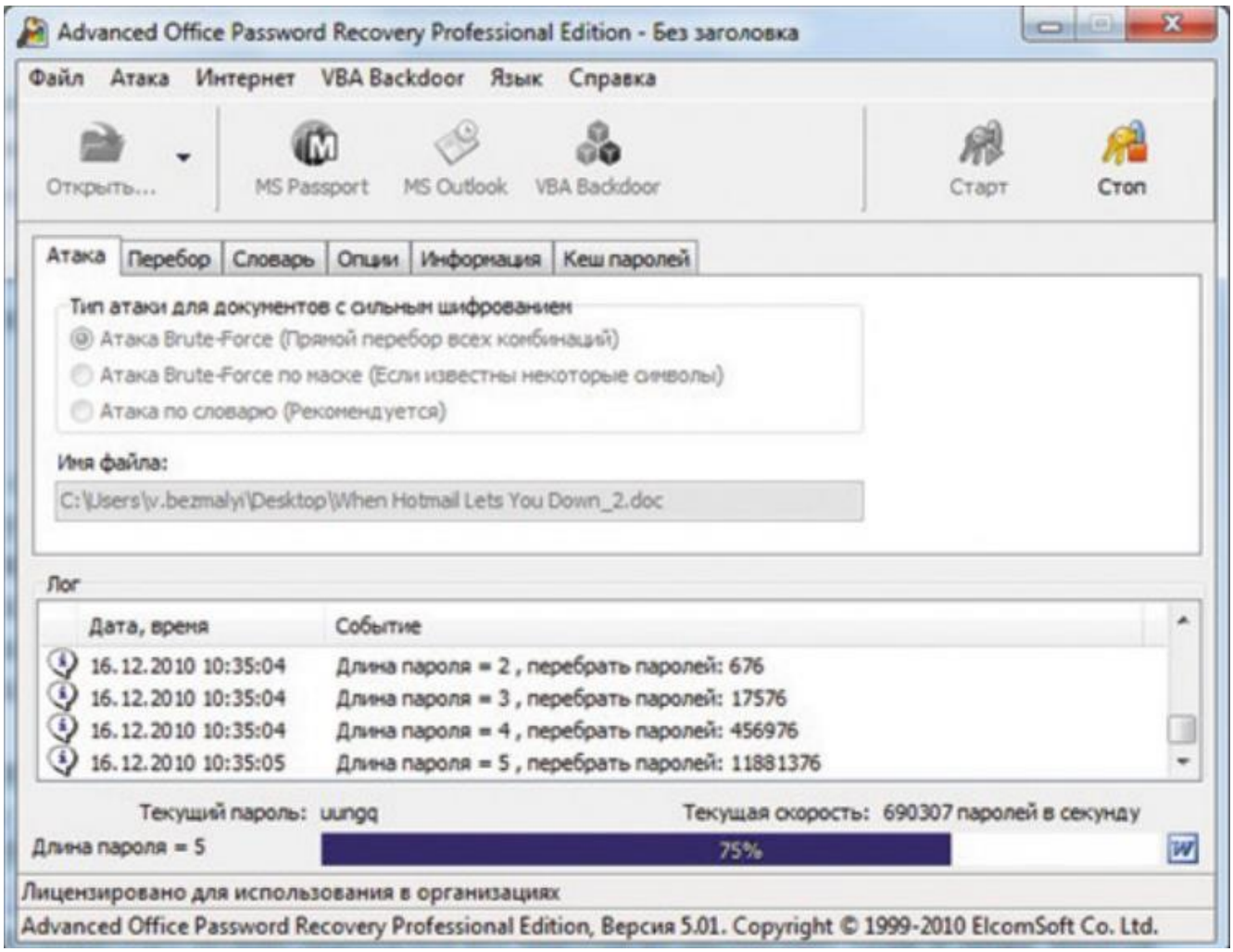
У Microsoft Office, до версії 6.0 включно, першим алгоритмом шифрування був звичайний XOR (булева функція). Звичайно ж, такий найпростіший алгоритм шифрування не забезпечував ніякого захисту, і будь-які паролі відновлювалися практично миттєво. В наступних версіях Microsoft Office 97 і 2000 використовувалися сильні криптоалгоритми MD5 і RC4. Однак у зв'язку з введенням обмежень на експорт сильної криптографії, що діяли в той час в США, криптоалгоритми, що застосовувалися за межами США, не могли використовувати ключі довше 40 розрядів. Це призвело до штучного обмеження ключів RC4 до 40 біт, а, отже, з 16 байт, отриманих на виході MD5, 11 просто затиралися в 0, і з 5 вагомих байтів і 11 нулів формувався ключ RC4. Це призвело до можливості організації атаки методом перебору (методом brute force). Для розшифровки файлу MS Word / Excel 97 / 2000 потрібно перебрати максимум 240 ключів.

З урахуванням появи таблиць ключів (Rainbow tables) потрібну атаку можна здійснити за обмежений час (від кількох секунд до кількох хвилин). Більше того, з'явилися сайти в Інтернеті, які надають подібні послуги, наприклад www.decryptum.com (вартість розшифровки одного файлу складає 29 дол); програмне забезпечення Guaranteed Word Decrypter (GuaWord) 1.7, Guaranteed Excel Decryptor (GuaExcel) 1.7 (виробник PSW- soft), Advanced Office Password Breaker (AOPB), Advanced Office Password Recovery (AOPR) (виробник Elcomsoft).

У Microsoft Office XP/2003 в якості алгоритму шифрування за умовчанням був залишений все той же алгоритм з 40 розрядним ключем. Разом з тим були внесені наступні зміни:

- алгоритм хешування SHA1 (замість MD5);
- ключ RC4 може мати довжину до 128 розрядів;
- довжина пароля збільшена з 16 до 255 символів.

Інша справа, що в кожному разі використовувана схема шифрування та перевірки паролів допускає високу швидкість перебору (до 1 000 000 паролів в секунду), як показано на екрані 1.

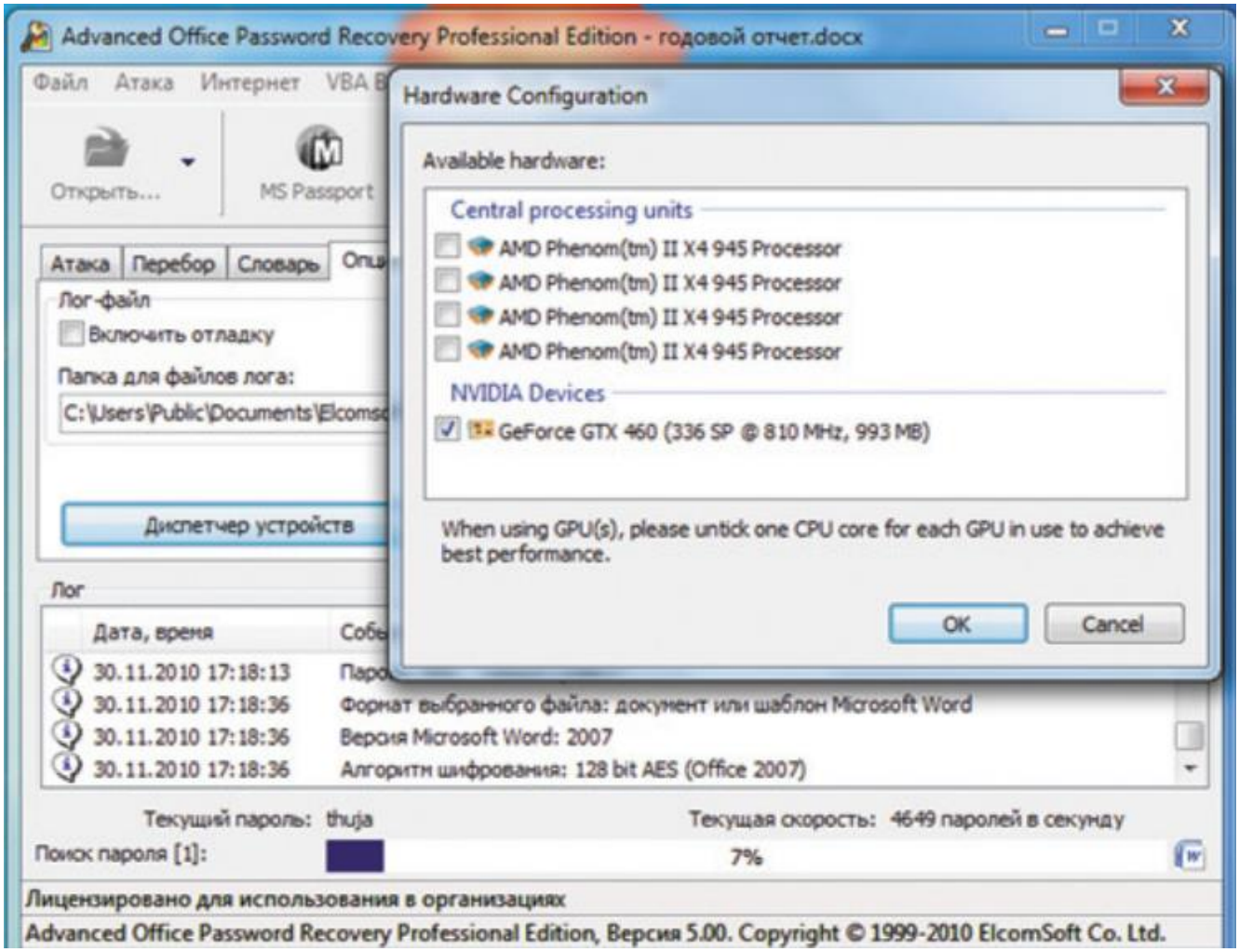


У Office 2007 була застосована нова схема шифрування, покликана боротися з високою швидкістю перебору паролів. У ній існують принципові відмінності від попередньої версії:

- на зміну алгоритму RC4 прийшов алгоритм шифрування AES з довжиною ключа 128 розрядів;
- замість одноразового хешування, пароль хешується циклічно 50 тис. разів;
- можливе застосування сторонніх алгоритмів шифрування.

У результаті вжитих заходів швидкість перебору паролів становить не більше 200 паролів в секунду, що дозволяє підібрати за розумний час паролі не довше 5-6 символів.

Разом з тим варто підкреслити, що з появою програмного забезпечення, що використовує ресурси відеокарти, швидкість перебору виростає до 5 тис. паролів в секунду, що в будь-якому випадку явно недостатньо для повноцінної атаки методом перебору (екран 2).



Що стосується формату захищених файлів, то його не назвеш простим і зрозумілим. Адже якщо встановлений пароль на відкриття файлу, то фактично файл являє собою OLE - контейнер, що складається з інформації про шифрування, зашифрованого потоку і допоміжної інформації. Однак, незважаючи на те що в ньому, як і в блоці шифрування в Office XP/2003, міститься ім'я криптопровайдера, назви алгоритмів хешування і шифрування, а також довжина ключа і дані для перевірки пароля і розшифровки, в Office 2007 жорстко встановлені наступні параметри:

- алгоритм шифрування AES з довжиною ключа 128 розрядів;
- алгоритм хешування SHA- 1.

При цьому шифрування і хешування забезпечує криптопровайдер Microsoft Enhanced RSA and AES Cryptographic Provider. Разом з тим слід врахувати, що при атаці послідовним перебором паролів швидкість перебору катастрофічно падає. Змінився і алгоритм перевірки паролів захисту документа від змін з доступом тільки на читання, а також книг і аркушів Excel. Раніше в документі зберігався хеш пароль, що складається з 2 байт. Відповідно було можливо його реверсування в перший підходящий пароль. Зараз же алгоритм хешування визначено записом у файлі XML і там же визначено кількість ітерацій хешу.

ХІД РОБОТИ

1. Ввести код програми в середовищі Delphi

Примітка. Всі ключі створювати за допомогою «Блокнот».

2. Встановити на комп’ютер програму Advanced Office Password Professional Edition.

3. За допомогою створеної програми у Delphi зашифрувати довільний документ формату doc.

4. Розшифрувати даний файл за допомогою програми Advanced Office Password Professional Edition.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Які існують можливості захисту в Microsoft Office 2003?
2. Які існують можливості захисту в Microsoft Office 2007?
3. Які зміни внесли в процес шифрування в Microsoft Office 2003?
4. Які зміни внесли в процес шифрування в Microsoft Office 2007?
5. Пригадайте функцію хешування SHA- 1.