Лабораторная работа №5

Для каждого пункта, кроме первого, можно написать свою небольшую программу и затем запускать эти программы по отдельности. Если вы работаете в Visual Studio, каждую такую программу можно оформить как отдельный проект в составе одного решения.

1) Возьмите любой криптопровайдер, который поддерживает операции шифрования, цифровой подписи и ключевого обмена. (Не берите криптопровайдеры, у которых для ключевого обмена используется алгоритм Диффи – Хеллмана, – в названии таких криптопровайдеров есть словосочетание Diffie-Hellman или DH. Дело в том, что алгоритм Диффи – Хеллмана на самом деле не предназначен для обмена ключами, а используется для безопасной выработки общего ключа, поэтому работа с этим алгоритмом в CryptoAPI осуществляется не так, как с другими алгоритмами ключевого обмена.)

2) Создайте у выбранного провайдера три ключевых контейнера под названием `Container1`, `Container2` и `Container3`.

3) Подключитесь к первому контейнеру и создайте в нём экспортируемую ключевую пару для обмена ключами, причём, длину ключей выберите такой, чтобы она была чуть меньше максимально возможной.

4) Экспортируйте открытый ключ пары для обмена ключами из первого контейнера в public key BLOB и сохраните его в файле **KeyX Public.bin**. Отключитесь от первого контейнера. Изучите содержимое полученного файла (просмотрите его байты в любом бинарном редакторе, например FAR Manager, и сравните то, что вы увидите, с описанием формата, который приведён в презентации).

5) Подключитесь ко второму контейнеру и создайте в нём экспортируемую ключевую пару для цифровой подписи с длиной ключа по умолчанию. Экспортируйте открытый ключ этой пары в public key BLOB и сохраните его в файле **DS Public.bin**. Отключитесь от второго контейнера. Изучите содержимое этого файла (откройте его в бинарном редакторе и сравните с описанием формата).

6) Подключитесь к криптопровайдеру, не используя никакой контейнер. Выберите какой-нибудь симметричный алгоритм, который поддерживает криптопровайдер, и сгенерируйте случайным образом экспортируемый сеансовый ключ для этого алгоритма. Экспортируйте его в plaintext key BLOB и сохраните в файле **Session Key Plaintext.bin**. Затем импортируйте открытый ключ для ключевого обмена из файла **KeyX Public.bin** и экспортируйте тот же сеансовый ключ в simple key BLOL, зашифровав его с помощью открытого ключа для ключевого обмена. Сохраните полученный simple key BLOB в файле **Session Key Encrypted.bin**. Отключитесь от криптопровайдера. Изучите содержимое файлов **Session Key Plaintext.bin** и **Session Key Encrypted.bin**, сравнив их с описанием того формата, к которому они относятся.

7) Подключитесь к первому контейнеру и импортируйте сеансовый ключ из файла **Session Key Encrypted.bin**, расшифровав его с помощью секретного ключа пары для ключевого обмена, хранящейся в этом контейнере. Также импортируйте незашифрованный сеансовый ключ из файла **Session Key Plaintext.bin**. Проверьте, одинаковы ли оба сеансовых ключа. Это можно сделать несколькими способами. Например, можно вызвать для каждого из них функцию `CryptHashSessionKey` и сравнить полученные хэш-значения либо экспортировать оба ключа в plaintext key BLOB и сравнить их содержимое. Отключитесь от первого контейнера.

8) Подключитесь ко второму контейнеру и экспортируйте ключевую пару для цифровой подписи в незашифрованный private key BLOB. Сохраните его в файле **DS Private Unencrypted.bin**.

Затем придумайте какой-нибудь пароль и сформируйте на его основе сеансовый ключ. Снова экспортируйте ключевую пару для цифровой подписи в private key BLOB, но на этот раз зашифруйте её сеансовым ключом. Сохраните второй BLOB в файле **DS Private Encrypted.bin**. Отключитесь от второго контейнера. Изучите содержимое файлов **DS Private Unencrypted.bin** и **DS Private Encrypted.bin**.

9) Подключитесь к третьему контейнеру и импортируйте в него ключевую пару для цифровой подписи из файла **DS Private Encrypted.bin**. (Для этого придётся заново сформировать сеансовый ключ, который вы использовали на шаге 8, и расшифровать с его помощью BLOB.) Убедитесь, что импортированная ключевая пара записалась в контейнер. (Можете для этого запустить программу из лабораторной работы №4.) Отключитесь от третьего контейнера.

10) Подключитесь к первому контейнеру и экспортируйте хранящуюся в нём пару для ключевого обмена в незашифрованный private key BLOB. Сохраните его в файле **KeyX Private Unencrypted.bin**. Отключитесь от первого контейнера. Изучите содержимое полученного файла, сравнив его с описанием формата.

11) Подключитесь к третьему контейнеру и импортируйте в него пару для ключевого обмена из файла **KeyX Private Unencrypted.bin**. Убедитесь, что ключевая пара сохранилась в контейнере. (Для этого можете запустить программу из лабораторной работы №4.) Отключитесь от третьего контейнера.

Ответьте на дополнительные вопросы.

a) Можно ли выгрузить сеансовый ключ в simple key BLOB, зашифровав его не открытым ключом для ключевого обмена, а другим сеансовым ключом (т. е. используя не асимметричный, а симметричный алгоритм)?

b) Можно ли выгрузить ключевую пару для цифровой подписи в private key BLOB, зашифровав её не сеансовым ключом, а открытым ключом для ключевого обмена (т. е. используя не симметричный, а асимметричный алгоритм)?

c) Можно ли выгрузить сеансовый ключ в simple key BLOB, зашифровав его не открытым ключом для ключевого обмена, а открытым ключом для цифровой подписи?

d) Создайте файл, который полностью имитирует plaintext key BLOB, и укажите в нём какой-нибудь слабый сеансовый ключ (например, ключ, все байты которого одинаковы). Попробуйте затем импортировать этот ключ. Получится ли это сделать?