Менеджер паролей

Программа работает в трех режимах:

1. Регистрация – генерация ключевой пары.

   Входным параметром функции является пароль пользователя от закрытого ключа. Размер ключей фиксируется в коде программы. В результате работы данной функции создаются два файла "public_key.txt"и "privat_key.txt содержащие открытый и закрытый ключи соответственно. Закрытый ключ записывается в файл под защитой маски, основанной на пароле пользователя. Маска представляет собой случайное число, битовая длина которого равна сумме битовых длин чисел p, q, которые являются закрытым ключом.

2. Шифрование нового пароля.

   Входным параметром функции является путь к файлу, содержащему открытый ключ пользователя, а также пароль, который необходимо зашифровать. В результате работы данная функция возвращает зашифрованный пароль, представленный в кодировке base64.

3. Расшифрование пароля.

   Входными параметрами функции являются: путь к файлу, содержащему открытый ключ пользователя, путь к файлу, содержащему закрытый ключ пользователя, пароль пользователя от закрытого ключа, а также шифртекст пароля, представленный в кодировке base64, который необходимо расшифровать. В результате работы данная функция возвращает расшифрованный пароль.

Сложность взлома криптосистемы Рабина эквивалентна сложности задачи факторизации. Поэтому стойкость реализуемой системы основана на использовании в качестве открытого ключа числа, для которого задача разложения на множители является трудной. Используемое в качестве открытого ключа число не должно раскладываться на множители с помощью известных алгоритмов, например, p-1 метода Полларда, ро-метода Полларда.

Опишем реализованный алгоритм создания ключевой пары.

1. Генерируется два случайных простых числа p, q вида $4k + 3$. Проверка на простоту выполняется с помощью вероятностного теста Миллера-Рабина с количеством раундов, равным целой части снизу двоичного логарифма проверяемого числа. Полученные простые числа являются закрытым ключом.

2. Открытый ключ является результатом умножения полученных чисел p, q.