ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к программе-кодеру паролей passcoder

Программа работает в трёх режимах:

1. Режим регистрации пользователя. Позволяет генерировать открытый и секретный ключи для шифрования паролей криптосистемой Рабина. Для секретного ключа предусмотрена защита паролем. По результатам выполнения программы в данном режиме создаются файлы user\_private\_key.txt и user\_public\_key.txt, содержащие сгенерированные открытый и закрытый ключи, соответственно. С целью оптимизации по времени, генерирование секретного ключа осуществляется путем выбора двух случайных простых чисел заданной длины из факторной базы, после чего открытый ключ генерируется путем перемножения выбранных чисел. Альтернативно можно было бы реализовать выбор случайного числа произвольного вида (простого и составного) и последующее применение тестов на простоту (к примеру, теста Миллера-Рабина или теста Соловея-Штрассена), что, однако, не представляется оптимальным.

Программа содержит собственную пару открытый-секретный ключ, что позволяет осуществлять подписывание генерируемого в данном режиме открытого ключа пользователя электронно-цифровой подписью ЭЦП RSA. При необходимости, программа поддерживает также неосновной четвертый режим, используемый для смены собственной пары ключей (генерации новой по алгоритму RSA).

Начальные значения параметров для удобства написания и тестирования программы выбраны как:

program\_public\_key = (107981, 193339)  
program\_private\_key = 134693

Однако, на практике необходимо использование существенно больших значений: общепринятой нормой на настоящий момент является использование 2048-битных, либо 4096-битных ключей RSA. Теоретически, при использовании достаточно большой факторной базы (см. файл “primes.txt”) в программе возможна генерация произвольно длинных значений ключей. При использовании той же факторной базы в программе RSASecAnalyzer любой ключ, сгенерированный в режиме изменения ключей, можно индивидуально проверить на стойкость к наиболее распространенным алгоритмам атак на RSA: к атаке факторизации (*р –* 1)- и ρ-методами Полларда, и с использованием итерации процесса шифрования, атаке восстановления шифртекста, атаке Винера. Тем не менее, при использовании достаточно больших (2048-битных и более) ключей наличие нестойкости к данным атакам представляется маловероятным.

2. Режим шифрования. Программа запрашивает путь к файлу с открытым ключом и ввод пароля. После этого производится вывод пароля, зашифрованного на открытом ключе пользователя по алгоритму криптосистемы Рабина. Шифр-текст представлен в кодировке base32.

3. Режим расшифрования. Запрашивается путь к файлу с секретным ключом и шифр-текст пароля. Шифр-текст представлен в кодировке base32. По результатам работы программы в данном режиме происходит вывод пароля на экран.

Безопасность криптосистемы Рабина обеспечивается сложностью поиска квадратных корней в кольце остатков по модулю составного числа. Как и в случае RSA, сложность взлома криптосистемы Рабина определяется сложностью задачи факторизации соответствующего открытого ключа. Главным недостатком криптосистемы является то, что в результате расшифрования, помимо необходимого сообщения, появляются также три ложных результата, что в ситуации, когда зашифрованное сообщение не является осмысленным текстом или другим легко распознаваемым объектом, приводит к неоднозначности расшифрования. По данной причине криптосистема не получила широкого практического применения, несмотря на то, что в отличие от RSA, является доказуемо стойкой к атаке на основе подобранного открытого зашифрованного текста, тогда и только тогда, когда задача о разложении целого числа на простые множители является трудноразрешимой (что не доказано для RSA).

Для криптосистемы Рабина, как и для криптосистемы RSA, представляется необходимым использование 2048-битных ключей для обеспечения большей стойкости против атак, использующих факторизацию.