Пояснительная записка

Беспалова Анастасия

3 июня 2020 г.

1 Процедура регистрации пользвателя

1. Пользователь вводит в аргументы командной строки глобальный пароль *password* (не менее 10 символов);

2. Программа генерирует открытый и закрытый ключ RSA. Ключи имеют размер 1024 бита;

3. Открытый ключ RSA и модуль шифрования RSA записываются в файл без изменений (*public_RSA.txt*) в кодировке base32;

4. Преобразованный закрытый ключ RSA и модуль шифрования побитово складываются с хэшем пароля — функция SHAKE128 (*private_RSA.txt*), выдающая хэш длины закрытого ключа + модуля шифрования;

5. Программа генерирует открытый и закрытый ключ криптосистемы Рабина;

6. Метка M1 — захардкоженный текст;

7. Открытый ключ Рабина с меткой программы M1 подписывается RSA и сохраняется (*public_Rabin.txt*)

8. Закрытый ключ Рабина конкатенируется с глобальным паролем, зашифровывается RSA и сохраняется (*private_Rabin.txt*).

2 Процедура смены ключа подписи программы

1. Пользователь вводит в аргументы командной строки глобальный пароль *password* и новый глобальный пароль не менее 10 символов (если пользователь не хочет менять глобальный пароль, он вводит тот же);

2. Программа вычисляет хэш пароля заданной длины, вычисляет секретный ключ RSA (из $private_RSA.txt$), проверяет корректность секретного ключа RSA (расшифровывает закрытый ключ Рабина из $private_Rabin.txt$ и проверяет метку в виде глобального пароля). Если метка пароля и введенный пароль совпадают — проверка пройдена;

3. Если был передан файл с паролями, то они расшифровываются, затем генерируются новые ключи RSA и новые файлы для них, перешифровывается закрытый ключ Рабина и переподписывается открытый ключ Рабина, перешифровывается файл с паролями.

3 Процедура шифрования пароля

1. В аргументы командной строки путь к файлу *public_Rabin.txt* и путь к открытому ключу RSA $public_RSA.txt$
2. Проверяется подпись (*public_Rabin.txt* расшифровывается открытым ключом RSA — если метка M1 совпала, то проверка пройдена);
3. Запрашивается шифруемый пароль (не менее 10 символов);
4. Пароль с меткой M2 (захардкожена) шифруется на открытом ключе Рабина и либо записывается в файл с паролями, либо выдается пользователю.

4 Процедура расшифрования пароля

1. Запрашивается путь к файлу *private_Rabin.txt*;
2. Запрашивается глобальный пароль пользователя;
3. Программа вычисляет хэш пароля, вычисляет секретный ключ RSA, проверяет корректность секретного ключа RSA по метке из закрытого ключа Рабина — если пароли совпали, то проверка пройдена;
4. Программа пароль Рабином (из файла или из командной строки) и выдает пользователю.

5 Доказательство 80-битной стойкости

Рассмотрим возможные угрозы. Противник может путем подбора раскрыть глобальный пароль. Однако при выборе пользователем глобального пароля более 10 символов, противнику потребуется перебрать 2^{80} различных комбинаций.

Противник может попробовать подменить ключи криптосистемы Рабина. Однако открытый ключ криптосистемы Рабина подписан RSA. Допустим, он попытается сфальсифицировать подпись и подменить открытый и закрытый ключ RSA. Однако для подмены ключа RSA ему потребуется знать глобальный пароль.

Противник может зашифровывать пароли. Однако шифруемые пароли должны быть также длины не менее 10 символов, так что для их подбора ему потребуется также не менее 2^{80} различных комбинаций.

Согласно рекомендациям NIST для достижения стойкости 80 бит модуль шифрования RSA должен быть около 1024 бит. Для параметров p и q программа выбирает минимум 512-битные простые числа, что предоставляет стойкость в 80 бит.