Лабораторная работа №3

Использование функций криптографического интерфейса Windows для защиты информации

Содержание задания

1. При запуске программы файл с учетными данными должен расшифровываться во временный файл (или в файл в оперативной памяти), который после завершения работы программы должен быть снова зашифрован для отражения возможных изменений в учетных записях пользователей. «Старое» содержимое файла учетных записей при этом стирается.
2. После ввода парольной фразы при запуске программы, генерации ключа расшифрования и расшифрования файла с учетными данными зарегистрированных пользователей правильность введенной парольной фразы определяется по наличию в расшифрованном файле учетной записи администратора программы.
3. При вводе неправильной парольной фразы или отказе от ее ввода работа программы должна завершаться с выдачей соответствующего сообщения.
4. Временный файл на диске с расшифрованными учетными данными после завершения работы программы удаляется.
5. Варианты использования алгоритмов шифрования и хеширования выбираются в соответствии с выданным преподавателем заданием.

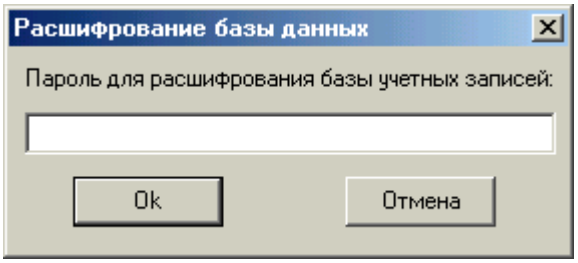
Индивидуальные варианты заданий

№	Тип симметричного шифрования	Используемый режим шифрования	Добавление к ключу случайного значения	Используемый алгоритм хеширования
1	2	3	4	5
1	Блочный	Электронная кодовая книга	Да	MD2
2	Потоковый	-	Да	MD2
3	Блочный	Сцепление блоков шифра	Да	MD2
4	Потоковый	-	Да	MD5
5	Блочный	Обратная связь по шифротексту	Да	MD2
6	Потоковый	-	Да	SHA
7	Блочный	Электронная кодовая книга	Да	MD4
1	2	3	4	5
8	Потоковый	-	Нет	MD2
9	Блочный	Сцепление блоков шифра	Да	MD4
10	Потоковый	-	Нет	MD5
11	Блочный	Обратная связь по шифротексту	Да	MD4
12	Потоковый	-	Нет	SHA

13	Блочный	Электронная кодовая книга	Да	MD5
14	Блочный	Сцепление блоков шифра	Да	MD5
15	Блочный	Обратная связь по шифротексту	Да	MD5
16	Блочный	Электронная кодовая книга	Да	SHA
17	Блочный	Сцепление блоков шифра	Да	SHA
18	Блочный	Обратная связь по шифротексту	Да	SHA
19	Блочный	Электронная кодовая книга	Нет	MD2
20	Блочный	Сцепление блоков шифра	Нет	MD2
21	Блочный	Обратная связь по шифротексту	Нет	MD2
22	Блочный	Электронная кодовая книга	Нет	MD4
23	Блочный	Сцепление блоков шифра	Нет	MD4
24	Блочный	Обратная связь по шифротексту	Нет	MD4
25	Блочный	Электронная кодовая книга	Нет	MD5
26	Блочный	Сцепление блоков шифра	Нет	MD5
27	Блочный	Обратная связь по шифротексту	Нет	MD5
28	Блочный	Электронная кодовая книга	Нет	SHA
29	Блочный	Сцепление блоков шифра	Нет	SHA
30	Блочный	Обратная связь по шифротексту	Нет	SHA

Возможный вид дополнительной диалоговой формы программы

Окно запроса парольной фразы для расшифровки файла с учетными данными



Может быть создано на основе шаблона Password Dialog, выбираемого с помощью команды File | New | Dialogs систем программирования Borland Delphi или Borland C++ Builder. Для повышения безопасности эта форма должна быть исключена из списка автоматически создаваемых форм проекта (команда Project | Options | Forms) и создаваться (уничтожаться) в программе явным образом. В указаниях по выполнению лабораторных работ эта форма имеет имя Form6.