**Лабораторная работа 2**

Сообщение было зашифровано следующим образом:

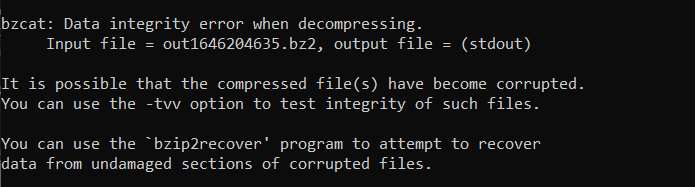
Начнем расшифровку сообщения с конца. Первым шагом будет следующее . Тут шифрование проводилось с помощью файла crypt.c и с помощью seed’а, который задавал начальное значение параметра holdrand. От этого параметра зависит очередное значение Rand(). Шифрование происходило с помощью операции XOR со строкой-ключом. Т.е. если у нас есть строка-ключ, то мы можем просто применить те же действия, что и были во время шифрования для расшифровки нашего сообщения. Это возможно, потому что операция XOR обратимая, т.е. (A ^ X)^X = A.

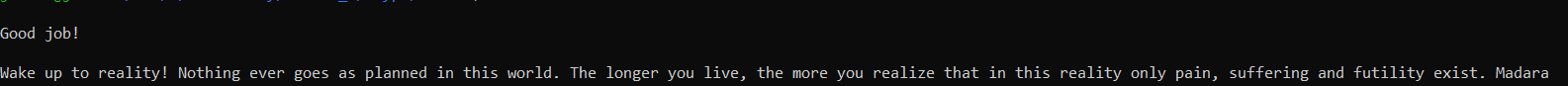
Получается, что наша задача сводится к тому, что надо найти ключ. Для этого просто переберем все возможные начальные значения holdrand. Time(NULL) возвращает количество секунд прошедших от 01.01.1970 00:00 (UTC +0). От этой даты до начала марта прошло 19052 дня, значит первый параметр(кол-во дней) перебираем от 19052 до 19083. Далее кол-во часов [0, 24), минут [0, 60), секунд [0, 60).

Теперь у нас есть все возможные зашифрованные сообщения. Как из них выбрать нужное? Для этого посмотрим на формат файла secret.bz2. У его содержания должен быть определенный формат. Для простоты будем считать, что он должен начинаться на “BZh9…”. Выведем все ключи, после применения которых расшифрованное сообщение начинается с символов выше. У меня получились ключи 1646204635 и 1647941775.

Теперь немного изменим файл crypt.c и будем передавать ему еще один параметр, который будем подставлять в Srand вместо time(null). Получились файлы out1646204635.bz2, out1647941775.bz2. С помощью команды bzcat попытаемся вывести содержимое файла.

Получилось следующее:





Вывод: ключом было значение 1647941775, сообщение получено и расшифровано.