Программа HACK.EXE предлагается для исследования и "взлома" при помощи отладчика.

Сценарий работы программы:

У пользователя запрашивается пароль (до 9 букв, завершаемых нажатием Enter), в случае ввода неверного пароля программа завершается без выдачи каких-либо сообщений, в случае ввода корректного пароля программа выполняет "полезные действия" (выводит на экран крупную надпись "УРА!").

Пароль (5 малых латинских букв): amber

Пароль хранится в сегменте данных программы в зашифрованном виде.

Задачи, которые предлагается решить с помощью отладчика:

- выяснить алгоритм проверки пароля и сам пароль;

- выполнить ветку "полезных действий" без ввода пароля и/или при вводе любого пароля, варианты решения – подмена флагов в результате сравнения или модификация кода в памяти (jmp в обход части проверки пароля);

- выяснить, как можно было бы модифицировать двоичный исполнимый файл EXE, чтобы программа работала без ввода пароля – в отладчике посмотреть двоичный код команд, вместо которых ассемблировать JMP на "полезные действия", посмотреть получившийся двоичный код, затем при помощи двоичного редактора (в папке есть HW.EXE) найти в EXE нужный участок и заменить его.