Задание выполнил Улитин Иван Владимирович, 531 группа

# Аутентификация по программе SKEY (на основе однонаправленных функций)

SKEY - это программа удостоверения подлинности, обеспечивающая безопасность с помощью однонаправленной функции.

Регистрируясь в системе, Алиса задает случайное число $R$. Компьютер вычисляет $f(R), f(f(R)), f(f(f(R)))$, и так далее, около сотни раз. Обозначив эти значения как $x_1, x_2, ..., x_{100}$, компьютер печатает список этих чисел, и Алиса прячет его в безопасное место. Компьютер также открытым текстом ставит в базе данных подключения к системе в соответствие Алисе значение $x_{101}$.

Подключаясь впервые, Алиса для аутентификации вводит $x_{100}$. Компьютер рассчитывает $f(x_{100})$ и сравнивает его с $x_{101}$, если значения совпадают, права Алисы подтверждаются. Затем Компьютер заменяет в базе данных $x_{101}$ на $x_{100}$. Алиса вычеркивает $x_{100}$ из своего списка.

Алиса при каждом подключении к системе вводит последнее невычеркнутое число из своего списка: $x_i$. Компьютер рассчитывает $f(x_i)$ и сравнивает его с $x_{i+1}$, хранившемся в базе данных. Так как каждый номер используется только один раз, Ева не сможет добыть никакой полезный информации. Аналогично, база данных бесполезна для взломщика. Как только список Алисы исчерпается ей придется перерегистрироваться в системе.