**Теоретические сведения.**

S/Key представляет собой систему генерирования одноразовых паролей на основе стандартов MD4 и MD5. Она предназначена для борьбы с так называемыми “повторными атаками”, когда хакер подслушивает канал, выделяет из трафика аутентификатор пользователя и его пароль и в дальнейшем использует их для несанкционированного доступа.

**Протокол**

1) , при первом входе в систему Алиса вводит свое имя и значение .

2) . вычисляет и сравнивает его со значением , которое хранится в регистрационной базе. Если значения совпадают, подлинность Алисы подтверждается. Затем H заменяет в базе данных на .

3) удаляет из своего списка .

Далее при каждом входе в систему Алиса вводит последнее не вычеркнутое число из своего списка, например