19 Социальная сеть

Задача. Алиса и Боб зарегистрировались в социальной сети и вошли в группу любителей рок-группы The Group. Группа секретная, все ее члены, и только они, знают секретный ключ K. Ключ используется в алгоритмах шифрования СТБ 34.101.31 (режим гаммирования с обратной связью).

С помощью K члены группы проверяют друг друга, а также обмениваются продуктами творчества The Group. Пользователь социальной сети, который хочет получить некоторый продукт, обращается с запросом к предполагаемому члену группы. В ответ ему отправляется письмо со случайной синхропосылкой и предлагается зашифровать имя отправителя, используя K и эту синхропосылку. Если имя зашифровано корректно, то далее высылается запрошенный продукт, зашифрованный на K. При шифровании снова используется случайная синхропосылка, которая отправляется вместе с данными.

Виктор не входит в группу, не знает K, он знает только, что Алиса и Боб уже который год разыскивают треки песен “Alice goes to France” и “Bronze goes to Bob”. Виктор, в свою очередь, желает получить слова секретной песни “Navajo know”. Помогите Виктору.

Решение. В режиме гаммирования с обратной связью последовательные 16-байтовые блоки открытого текста $X_1, \ldots, X_T$ зашифровываются следующим образом:

$$Y_t = F_K(Y_{t-1}) \oplus X_t, \quad t = 1, \ldots, T.$$

Здесь Y_0 — синхропосылка, $Y_1, \ldots, Y_T$ — блоки шифртекста, F_K — зашифрование отдельного блока на ключе K (подробнее см. СТБ 34.101.31).

Если Виктор умеет определять $F_K(Y)$ для произвольного блока Y, то он сможет пройти аутентификацию перед Алисой или Бобом, а также расшифровать присланные ими данные:

$$X_t = F_K(Y_{t-1}) \oplus Y_t, \quad t = 1, \ldots, T.$$

Остается описать протокол определения $F_K(Y)$:

1. Виктор регистрируется под 16-байтовым именем Id, всякий раз новым.
2. Виктор-как-Id объявляет, что является поклонником The Group и у него есть треки песен, которые разыскивают Алиса и Боб.
3. Алиса и Боб обрадованы и обращаются к Id с запросом. Пусть первой обратилась Алиса.
4. Виктор-как-Id проверяет Алису, высылая ей блок Y в качестве синхропосылки.
5. Алиса отвечает блоком $Z = F_K(Y) \oplus Id$.
6. Виктор определяет $F_K(Y) = Z \oplus Id$ и обрывает связь с Алисой.
7. Алиса разочарована и выражает Виктору-как-Id свое недоумение.
8. Виктор, заметая следы, удаляет учетную запись Id.