13 Протокол аутентификации

Алиса и Боб проводят взаимную аутентификацию, которая состоит в проверке знания общего секретного ключа θ. На этом ключе стороны выполняют шифрование пар 16-байтовых блоков. Используются алгоритмы шифрования в режиме сцепления блоков СТБ 34.101.31. При шифровании выбираются нулевые синхропосылки. Аутентификация проводится по следующему протоколу:

1. Боб выбирает случайный блок X_B и посылает его Алисе.
2. Алиса выбирает случайный блок X_A и посылает Бобу зашифрованную пару (X_A, X_B).
3. Боб выполняет расшифрование принятого сообщения, получая (X'_A, X'_B), а затем сравнивает X'_B с X_B. Если блоки отличаются, то Боб завершает протокол с ошибкой. В противном случае Боб признает подлинность Алисы и отсылает ей зашифрованную пару (X_B, X_A).
4. Алиса выполняет расшифрование принятого сообщения, получая (X''_B, X''_A), а затем сравнивает X''_A с X_A. Если блоки отличаются, то Алиса завершает протокол с ошибкой. В противном случае Алиса признает подлинность Боба.

Покажите как Виктор, который не знает θ, может ввести Алису в заблуждение, выдав себя за Боба.

Решение. Виктор поступает следующим образом:

1. Выбирает случайный блок X_B и посылает его Алисе.
2. Получает от Алисы шифртекст (C_1, C_2). Согласно правилам зашифрования в режиме сцепления блоков
$$C_1 = F_\theta(X_A), \quad C_2 = F_\theta(C_1 \oplus X_B),$$
где F_θ — зашифрование блока на ключе θ.
3. Отправляет Алисе пару (O, C_1), где O — нулевой блок.

Алиса выполняет расшифрование полученной пары:

$$X''_B = F_\theta^{-1}(O), \quad X''_A = F_\theta^{-1}(C_1) \oplus O = F_\theta^{-1}(F_\theta(X_A)) = X_A.$$

Проверочное равенство выполнено и Алиса принимает Виктора за Боба.

Описанный протокол повторяет 3-шаговый протокол стандарта ISO/IEC 9798-2 с одним исключением — в ISO/IEC на последнем шаге Алиса проводит не одну, а две проверки:

$$X''_A \stackrel{?}{=} X_A, \quad X''_B \stackrel{?}{=} X_B.$$

Дополнительная проверка блокирует атаку Виктора.