44 Определить режим

Задача. Шифратор `Amgine` реализует алгоритмы СТБ 34.101.31. Известно, что шифрование выполняется либо в режиме сцепления блоков (CBC), либо в режиме гаммирования с обратной связью (CFB), либо в режиме счетчика (CTR). Виктору требуется определить, какой из трех режимов используется. Разрешается подать на вход шифратора два открытых текста вместе с синхропосылками и получить соответствующие шифртексты. Помогите Виктору.

Примечание. Синхропосылки повторять нельзя.

Решение. Виктор подает синхропосылку $S = 0^{128}$ и открытый текст $X = 0^{256}$. В ответ получает $Y = Y_1 \parallel Y_2$, $Y_i \in \{0,1\}^{128}$. В режимах CBC и CFB

$$Y_1 = F_\theta(0^{128}), \quad Y_2 = F_\theta(Y_1).$$

Затем Виктор зашифровывает Y_1, используя синхропосылку Y_1, и получает шифртекст $Y_3 \in \{0,1\}^{128}$. В режиме CBC

$$Y_3 = F_\theta(Y_1 \oplus Y_1) = F_\theta(0^{128}) = Y_1,$$

в режиме CFB

$$Y_3 = F_\theta(Y_1) \oplus Y_1 = Y_2 \oplus Y_1,$$

а в режиме CTR

$$Y_3 = F_\theta(F_\theta(Y_1) \boxplus 1).$$

Виктор принимает решение в пользу CBC, если $Y_3 = Y_1$, в пользу CFB, если $Y_3 = Y_1 \oplus Y_2$, и в пользу CTR, если не выполняется ни первое ни второе равенства.

Ошибки распознавания возможны, но маловероятны. Например, режим CFB будет ошибочно признан режимом CBC, если $Y_2 = 0$. Вероятность этого события при случайном θ близка к 2^{-128}.

□