

## 11 Режимы шифрования

### 11.1 Режим простой замены

В режиме простой замены использования блочной криптосистемы  $F = \{F_K: K \in \mathcal{K}\} \subseteq S(\{0,1\}^n)$ , открытый текст  $X \in \{0,1\}^*$ , длина которого кратна  $n$ , разбивается на блоки  $X_1, X_2, \dots, X_T \in \{0,1\}^n$ :  $X = X_1 \parallel X_2 \parallel \dots \parallel X_T$ .

Уравнение зашифрования и расшифрования:

$$Y_t = F_K(X_t), \quad X_t = F_K^{-1}(Y_t), \quad t = 1, 2, \dots, T.$$

Слово  $Y = Y_1 \parallel Y_2 \parallel \dots \parallel Y_T$  объявляется шифртекстом.

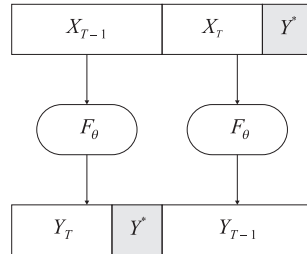
Режим простой замены называют также режимом *электронного кодового блокнота* (ECB, Electronic CodeBook).

Длина слова  $X$  может быть не кратной  $n$  и требуется организовать обработку последнего (возможно, неполного) блока данных  $X_T \in \{0,1\}^m$ ,  $m \leq n$ . Известны следующие способы такой обработки:

1. Блок  $X_T$  дополняется нулями до слова длины  $n$  и зашифровывается. Дополнительно зашифровывается блок  $X_{T+1} \in \{0,1\}^n$ , содержащий представление числа  $m$  словом из  $\{0,1\}^n$ .
2. К блоку  $X_T$  дописывается символ 1 (маркер), а затем минимальное число символов 0 до получения слова длины кратной  $n$ . Если блок  $X_T$  был полным, то будет сформирован дополнительный блок  $X_{T+1} = 100\dots 0$ , который также зашифровывается. После расшифрования нули и маркер отбрасываются.
3. При  $T \geq 2$  вычисляется  $Y^* = R_{n-m}(F_K(X_{T-1}))$  и устанавливается

$$Y_{T-1} = F_K(X_T \parallel Y^*), \quad Y_T = L_m(F_K(X_{T-1})),$$

где  $R_k, L_k$  — операторы взятия правых и левых  $k$  двоичных символов соответственно.



**Упражнение 11.1.** Как должно быть организовано расшифрование в последнем случае? □

В режиме простой замены каждый блок открытого текста обрабатывается отдельно от остальных. В связи с этим возникают, например, следующие угрозы:

1. Перестановка блоков. Виктор располагает форматами банковских документов и переставляет местами блоки с младшими и старшими цифрами суммы платежа.
2. Анализ повторов блоков. Виктор располагает форматами банковских документов и располагает информацией о повторе их блоков. Анализ повторов блоков перехваченного шифртекста позволяет Виктору установить тип документа.

Для преодоления этих недостатков используются другие режимы шифрования.

## 11.2 Режимы шифрования

В режимах

- CBC (Cipher Block Chaining, цепной обработки, сцепления блоков) и
- CFB (Cipher FeedBack, гаммирования с обратной связью, обратной связи по шифртексту)

результат зашифрования блока  $X_t$  зависит от всех предыдущих блоков открытого текста  $X_1, \dots, X_{t-1}$ . Уравнения прямого и обратного преобразований в режимах CBC и CFB имеют соответственно вид:

$$\begin{aligned} Y_t &= F_K(X_t \oplus Y_{t-1}), & X_t &= Y_{t-1} \oplus F_K^{-1}(Y_t), \\ Y_t &= X_t \oplus F_K(Y_{t-1}), & X_t &= Y_t \oplus F_K(Y_{t-1}). \end{aligned}$$

Здесь  $Y_0$  – некоторый наперед заданный *вектор инициализации* или *синхропосылка*.

Синхропосылка обеспечивает уникальность результатов криптографического преобразования на одном и том же ключе. Синхропосылка является несекретным объектом и может передаваться вместе с зашифрованными данными.

В режимах

- OFB (Output FeedBack, режима обратной связи по выходу) и
- CTR (CounTeR, счетчика)

зависимость от блоков  $X_1, \dots, X_{t-1}$  отсутствует. В данных режимах вырабатывается гамма — последовательность векторов  $\Gamma_1, \dots, \Gamma_T \in \{0, 1\}^n$ , которая используется как для зашифрования:

$$Y_t = X_t \oplus \Gamma_t,$$

так и для расшифрования:

$$X_t = Y_t \oplus \Gamma_t, \quad t = 1, \dots, T.$$

В режиме OFB гамма вырабатывается по правилу

$$\Gamma_t = F_K(\Gamma_{t-1}), \quad \Gamma_0 \text{ — синхропосылка.}$$

В режиме счетчика

$$\Gamma_t = F_K(S_t), \quad S_t = \varphi(S_{t-1}), \quad S_0 \text{ — синхропосылка.}$$

Здесь  $\varphi: \{0, 1\}^n \rightarrow \{0, 1\}^n$  — функция инкремента, которая выбирается так, чтобы обеспечить большой период последовательности  $S_t$ . Например, часто используют выбор  $S_{t+1} = \varphi(S_t) = S_t \boxplus 1$ .

**Упражнение 11.2.** В режиме OFB используемая подстановка  $F_K \in S(\{0, 1\}^n)$ , должна обеспечивать большой период последовательности  $\Gamma_t$ . Максимально большой период обеспечивает полноцикловая подстановка  $F_K$  для которой все элементы  $\Gamma_0, \dots, \Gamma_{2^n-1}$  различаются. Доказать, что среди элементов  $S(\{0, 1\}^n)$  имеется  $(2^n - 1)!$  полноцикловых подстановок и, таким образом, вероятность того, что наудачу выбранная  $F_K$  окажется полноцикловой равняется  $2^{-n}$ .  $\square$

Сравнительные характеристики режимов приведены в следующей таблице.

Свойства	Режимы				
	ECB	CBC	CFB	OFB	CTR
зависимость от $X_1, \dots, X_{t-1}$	–	+	+	–	–
уникальность синхропосылки <sup>1</sup>	не исп.	+	+	+	+
использование $F_K^{-1}$	+	+	–	–	–
восстановление после ошибки в шифртексте <sup>2</sup>	+	+	+	+	+
восстановление после ошибки в синхропосылке <sup>3</sup>	не исп.	+	+	–	–
распараллеливание <sup>4</sup>	+	–	–	–	+
«податливость» (malleability) <sup>5</sup>	–	$\mp$	$\pm$	+	+

<sup>1</sup> требуется обеспечивать уникальность синхропосылок. При нарушении требования возможно определение одних блоков открытого текста по шифртексту и другим известным блокам открытого текста;

<sup>2</sup> даже если один из блоков  $Y_t$  изменен при передаче, при расшифровании, начиная с некоторого  $\tau > t$ , будут получены корректные блоки  $X_\tau$ ;

<sup>3</sup> даже если синхропосылка изменена при передаче, при расшифровании, начиная с некоторого  $\tau$ , будут получены корректные блоки  $X_\tau$ ;

<sup>4</sup> шифрование различных блоков может выполняться одновременно на нескольких процессорах;

<sup>5</sup> контролируемые изменения открытого текста через манипуляции с шифртекстом (негативное свойство).

**Упражнение 11.3 (★).** В режиме СВС синхропосылка должна быть не только уникальной, но и непредсказуемой. Обосновать данное требование. Предположить, что Виктор может выбирать открытый текст и до своего выбора знает, какая будет использоваться синхропосылка. Виктору требуется проверить, что блок открытого текста  $X_t$ , соответствующий перехваченному блоку шифртекста  $Y_t$ , совпадает с определенным значением  $a$ .  $\square$

### 11.3 Имитозащита

Блочные криптосистемы могут использоваться не только для обеспечения конфиденциальности, но и для контроля целостности сообщений. Для этого по блочной криптосистеме строится *система имитозащиты*  $I = \{I_K: K \in \mathcal{K}\}$ , где  $I_K: \{0, 1\}^* \rightarrow \{0, 1\}^m$ . В англоязычной литературе системы имитозащиты называются также MAC-системами (от Message Authentication Codes).

Алиса вместе с шифртекстом  $Y$  отправляет Бобу *имитовставку*  $Z = I_K(X)$ . Боб получает шифртекст  $Y'$  (который может отличаться от  $Y$ ), находит открытый текст  $X'$ , вычисляет имитовставку  $Z' = I_K(X')$  и сравнивает ее с  $Z$ . Если имитовставки различаются, то Боб принимает решение о том, что  $Y' \neq Y$  — шифртекст был изменен в канале связи. В противном случае Боб принимает  $X'$ .

Детали могут отличаться. Например имитовставка может вычисляться не от открытого текста  $X$ , а от шифртекста  $Y$ . При этом можно сначала проверить имитовставку, а только затем при успешной проверке выполнить расшифрование.

Рассмотрим два распространенных способа построения систем имитозащиты.

**СВС-МАС.** Выполняются вычисления, аналогичные вычислениям в режиме СВС:

$$Y_t = F_K(X_t \oplus Y_{t-1}), \quad Y_0 = 0^n.$$

Имитовставкой объявляется слово  $Y_T$ .

**Пример 11.1.** Режим СВС-МАС используется в ГОСТ 28147-89 с некоторыми уточнениями:

- разрешается использовать  $T \geq 2$  блоков;
- используется  $l \leq 32$  символов  $Y_T$ ;
- преобразования  $F_K$  являются 16-тактовыми (при зашифровании применяется 32 такта).  $\square$

**Система Вигмана — Картера.** Имитовставка вычисляется по правилу:  $Z = f_X(H) \oplus F_K(S)$ , где  $f_X$  — многочлен над полем  $\mathbb{F}_{2^n}$ , который определяется по  $X$ ;  $H = F_K(0^n)$  — секретная точка (интерпретируется как элемент  $\mathbb{F}_{2^n}$ );  $S$  — синхропосылка.

Многочлен  $f_X$  строится так, что  $1 \leq \deg f_X \leq D \ll M$  и различным сообщениям соответствуют различные многочлены. Например, для  $X = X_1 \parallel X_2 \parallel \dots \parallel X_T$  ( $T + 1 \leq D$ ) многочлен

$$f_X(\lambda) = X_1\lambda^{T+1} + X_2\lambda^T + \dots + X_T\lambda^2 + X_{T+1}\lambda = ((\dots (X_1\lambda + X_2)\lambda + \dots + X_T)\lambda + X_{T+1})\lambda.$$

Здесь  $X_{T+1}$  — дополнительный блок, который содержит представление  $|X|$ .

Использование многочленов такого вида гарантирует, что для случайной секретной точки  $H$  и различных  $X, X'$  вероятность

$$\mathbf{P}\{f_X(H) = f_{X'}(H)\} = \mathbf{P}\{H - \text{корень } f_X - f_{X'}\} \leq \frac{\deg(f_X - f_{X'})}{2^n} \leq \frac{D}{2^n},$$

т. е. невелика. Данный факт позволяет получить обоснование надежности системы Вигмана — Картера.

Значение  $f_X(H)$  зашумляется секретным значением  $F_K(S)$ . Если этого не делать, то по известной имитовставке  $Z$  противник может получить  $H$  как один из корней полиномиального уравнения  $f_X(\lambda) - Z = 0$ .

## 11.4 «Податливость»

Пусть зашифрование блоков открытого текста  $X_1, X_2, \dots$  выполняется в режиме

$$\text{Mode} \in \{\text{ECB}, \text{CBC}, \text{CFB}, \text{CTR}, \text{OFB}, \dots\}.$$

Пусть в результате зашифрования получены блоки  $Y_1, Y_2, \dots$

Блоки шифртекста передаются по открытому каналу связи, который контролирует противник. Что произойдет при расшифровании, если противник изменит один из блоков шифртекста? Например, заменит  $Y_t$  на  $Y'_t = Y_t \oplus \alpha$ ,  $\alpha \neq 0$ .

В режиме ECB получатель (Боб) вместо  $X_t$  получит  $X'_t = F_K^{-1}(Y_t \oplus \alpha)$ . Противник не знает  $K$  и поэтому, вообще говоря, не знает, как связаны между собой  $X_t$  и  $X'_t$ . Говорят, что режим не является «податливым» — противник не может контролировать изменения в открытом тексте при изменениях в шифртексте.

В режиме CTR Боб вместо  $X_t$  получит  $X'_t = X_t \oplus \alpha$  (почему?). Противник точно знает, к чему приведет изменение шифртекста. Режим является «податливым».

Очевидно, что «податливость» является отрицательным свойством. Представим себе, что Алиса отправляет Бобу зашифрованную экзаменационную ведомость. Виктор знает формат ведомости, знает поставленные оценки и может «подкрутить» некоторые из них.

В режиме CBC Боб вместо  $X_t$  получит  $X'_t = F_K^{-1}(Y'_t) \oplus Y_{t-1}$ . «Податливости» нет. Но изменение следующего блока открытого текста оказывается под контролем противника:

$$X'_{t+1} = F_K^{-1}(Y_{t+1}) \oplus Y'_t = F_K^{-1}(Y_{t+1}) \oplus Y_t \oplus \alpha = X_{t+1} \oplus \alpha.$$

В таких случаях говорят о частичной «податливости».

**Упражнение 11.4.** Оценить «податливость» режимов CFB и OFB. □