Лабораторная работа № 3

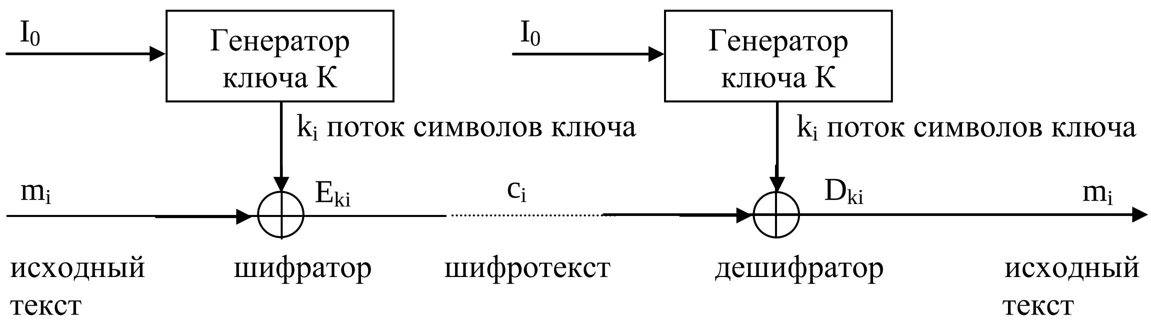
ИЗУЧЕНИЕ ПОТОКОВЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

1. Цель работы:

Изучение потоковых криптосистем, построенных на базе М-последовательностей.

2. Теоретическая часть

Синхронные потоковые шифраторы формируют ключ в виде потока (последовательности) символов $K = k_1k_2\ldots$, который несложным образом комбинируется с последовательностью символов исходного текста $M = m_1\ m_2\ \ldots$. Алгоритм формирования К должен быть детерминированным и воспроизводимым, а сама последовательность – случайной или псевдослучайной. Синхронный потоковый шифратор имеет следующую структуру:



I_0 – начальное состояние генераторов ключа. Оба генератора должны иметь одинаковое начальное состояние и функционировать синхронно.

Каждый символ шифротекста c_i является функцией от соответствующих символов исходного текста и ключа:

$$c_i = E_{ki}(m_i) = m_i \oplus k_i$$

При дешифровании выполняется обратное преобразование:

$$D_{ki}(c_i) = c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i = m_i. \qquad m_i, k_i, c_i \in \{0,1\}.$$

2.1. Генераторы М-последовательностей.

При выборе генератора ключа (ГК) необходимо учитывать следующие факторы: аппаратные затраты на реализацию ГК, временные затраты на генерацию ключа. Широкое распространение получили генераторы на основе сдвигового регистра с линейными обратными связями. Они описываются следующим выражением:

$$a_i = \sum_{i=1}^{\oplus} a_k\ a_{i-k}, \quad k=0,1,2,\ldots, \qquad (1)$$

где k – номер такта; $a_k \in \{0,1\}$ – биты формируемой последовательности; $a_i \in \{0,1\}$ – постоянные коэффициенты; $\sum^{\oplus}$ - операция суммирования по модулю 2. Генератор, описываемый отношением (1), показан на рис. 1.

Свойства генерируемой последовательности определяются постоянными коэффициентами a_i. Их можно исследовать, анализируя характеристический полином

$$g(x) = 1 \oplus a_1\ x \oplus a_2\ x^2 \oplus \ldots \oplus a_{m-1}\ x^{m-1} \oplus a_m\ x^m.$$

При соответствующем выборе коэффициентов генерируемая последовательность { a_i } будет иметь максимально возможный период, равный 2^m-1, где m – разрядность сдвигового регистра и одновременно старшая степень порождающего полинома. Последовательность максимально возможного периода называется М-последовательностью. Основная задача синтеза генератора рассматриваемого типа – нахождение характеристического полинома, формирующего М-последовательность.

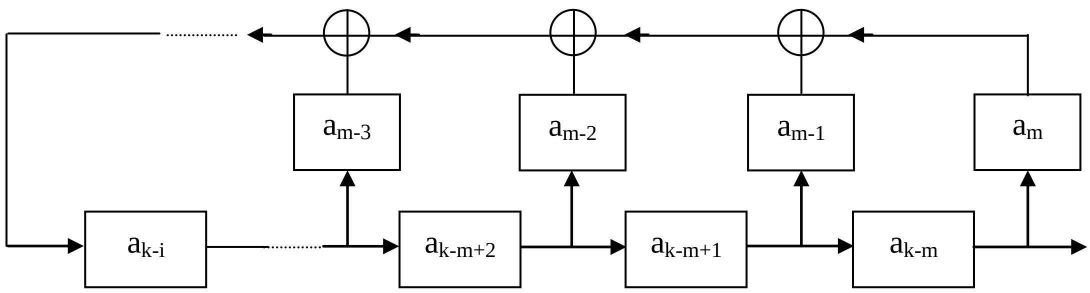


Рис. 1. ГК на основе сдвигового регистра

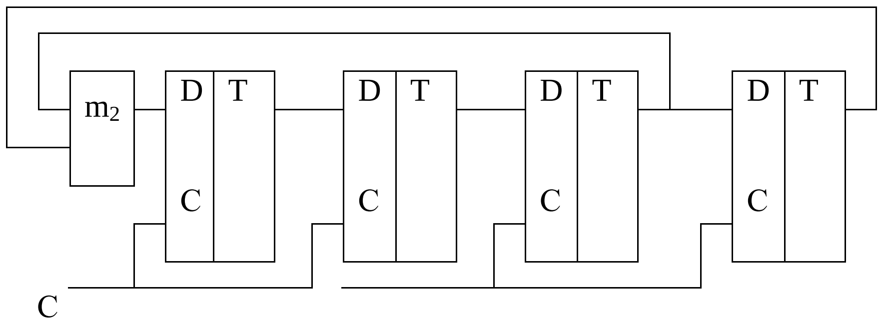


Рис. 2. Функциональная схема четырехразрядного ГК
с порождающим полиномом $g(x) = 1 \oplus x^3 \oplus x^4$

Таблица 2.1.
Примитивные полиномы

m	g(x)
3	$1 \oplus x \oplus x^3$
4	$1 \oplus x \oplus x^4$
5	$1 \oplus x^2 \oplus x^5$
6	$1 \oplus x \oplus x^6$
7	$1 \oplus x \oplus x^7$
8	$1 \oplus x \oplus x^5 \oplus x^6 \oplus x^8$
9	$1 \oplus x^4 \oplus x^9$
10	$1 \oplus x^3 \oplus x^{10}$
11	$1 \oplus x^2 \oplus x^{11}$
12	$1 \oplus x^3 \oplus x^4 \oplus x^7 \oplus x^{12}$
13	$1 \oplus x \oplus x^3 \oplus x^4 \oplus x^{13}$

Таблица 2.2.
Функционирование ГК

n	ГК	n	ГК
1	1000	9	1010
2	0100	10	1101
3	0010	11	1110
4	1001	12	1111
5	1100	13	0111
6	0110	14	0011
7	1011	15	0001
8	0101		

Полиномы, формирующие последовательность максимального периода, называются примитивными. С ростом m их количество становится очень большим. Среди множества примитивных полиномов степени m можно найти полиномы с наименьшим числом единичных коэффициентов a_i. Генераторы, построенные на их основе, имеют наиболее простую техническую реализацию. В табл. 2.1 приведен перечень полиномов с минимальным количеством ненулевых коэффициентов для значений $m \le 16$.

Схема четырехразрядного ГК, описываемого примитивным полиномом $g(x) = 1 \oplus x^3 \oplus x^4$, приведена на рис. 2.2; его работа показана в табл. 2.2.

Для формирования М-последовательности наряду с примитивным полиномом g(x) может использоваться и обратный ему полином $g^{-1}(x) = x^m g(x^{-1})$. Полученная в этом случае последовательность максимальной длины будет инверсной по отношению к последовательности, формируемой g(x). Например, для полинома $g(x) = 1 \oplus x^3 \oplus x^4$ обратным полиномом будет $g^{-1}(x) = x^4(1 \oplus x^{-3} \oplus x^{-4}) = 1 \oplus x \oplus x^4$.

Главное преимущество описываемого метода формирования псевдослучайных последовательностей – простота его реализации. Генератор М-последовательности содержит лишь m-разрядный регистр сдвига и набор сумматоров по модулю два в цепи обратной связи. Регистр сдвига выполняет функции хранения m бит М-последовательности и сдвига m-разрядного кода на один разряд вправо. Сумматоры по модулю два вычисляют очередное значение младшего разряда сдвигового регистра.

Состояние разрядов регистра на каждом такте можно представить в виде m-мерных векторов $A(k) = a_1(k)a_2(k)a_3(k)\ldots a_m(k)$, где $k = 0,1,2,\ldots$ - номер такта, $a_i(k)$ – состояние i-го разряда, $i = 1,m$. Тогда будет выполняться следующее соотношение:

$$\begin{pmatrix} a_1(k) \\ a_2(k) \\ a_3(k) \\ \ldots \\ a_m(k) \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_{m-1} & a_m \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & \ldots & \ldots \end{pmatrix} * \begin{pmatrix} a_1(k-1) \\ a_2(k-1) \\ a_3(k-1) \\ \ldots \\ a_m(k-1) \end{pmatrix}$$

или в более компактном виде $A(k) = VA(k-1)$, откуда для произвольного s справедливо равенство

$$A(k+s)\, V^{s+1} = A(k-1), \qquad (2)$$

где

$$V = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_{m-1} & a_m \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & 0 \end{pmatrix}$$

Для М – последовательности, описываемой полиномом $g(x) = 1 \oplus x^3 \oplus x^4$, матрица V имеет вид

$$V = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Последовательное применение соотношений (1) или (2) для s=0 позволяет формировать соответственно одно- или многоразрядные псевдослучайные последовательности, которые характеризуются рядом статических свойств.

Рассмотрим наиболее важные свойства М-последовательностей.

1. Период последовательности, описываемой выражением (1), определяется старшей степенью порождающего полинома g(x) и равен $L = 2^m - 1$.

2. Для заданного полинома g(x) существует L различных М-последовательностей, отличающихся фазовым сдвигом. Так, полиному $g(x)=1\oplus x^3\oplus x^4$ соответствует 15 М-последовательностей.

3. Количество единичных и нулевых символов a_k, k=1,1,…,L-1, М-последовательности соответственно равно 2^{m-1} и $2^{m-1}-1$. Вероятностная оценка частоты их появления определяется следующими выражениями:

$$p(a_k=1) = 2^{m-1}/(2^m-1) = 1/2 + 1/(2^{m+1}-2),$$
$$p(a_k=0) = (2^{m-1}-1)/(2^m-1) = 1/2 - (2^{m+1}-2)$$

и при увеличении m достигает значений, сколь угодно близких к 1/2.

4. Вероятности появления серий из r, $r\in\{1,2,\ldots,m-1\}$, одинаковых символов (нулей или единиц) в М-последовательности максимально близки к соответствующим вероятностям для случайной последовательности.

5. Для любого значения s ($1\le s<L$) существует такое $r\ne s$ ($1\le r<L$), что $\{a_k\} + \{a_k\text{-}s\} = \{a_k\text{-}r\}$. Данное свойство обычно называют свойством сдвига и сложения.

Использование линейных сдвиговых регистров для создания криптосистем предполагает их уязвимость, если взломщик обладает парой: исходный текст – шифротекст длиной не менее 2m бит. Действительно, имея исходный текст $M = (m_1,m_2,\ldots,m_{2m})$ и соответствующий шифротекст $C= (c_1,c_2,\ldots,c_{2m})$, мы можем получить $K=M\oplus C=(m_1\oplus c_1,m_2\oplus c_2,\ldots,m_{2m}\oplus c_{2m})=(k_1,k_2,k_3,\ldots,k_{2m})$. Тогда задача взлома криптосистемы при известном начальном состоянии сводится к решению системы из m линейных уравнений с m неизвестными, где неизвестными являются коэффициенты порождающего полинома.

Данная система имеет вид

$$a_1k_1 \oplus a_2k_2 \oplus a_3k_3 \oplus \ldots \oplus a_mk_m = k_{m+1}$$
$$a_1k_2 \oplus a_2k_3 \oplus a_3k_4 \oplus \ldots \oplus a_mk_{m+1} = k_{m+2}$$
$$a_1k_3 \oplus a_2k_4 \oplus a_3k_5 \oplus \ldots \oplus a_mk_{m+2} = k_{m+3}$$
$$\ldots$$
$$a_1k_m\oplus a_2k_{m+1}\oplus a_3k_{m+2}\oplus \ldots \oplus a_mk_{m+m-1} = k_{2m} .$$

3. Порядок выполнения работы

1. Реализовать генератор М-последовательности заданной длины.
2. Построить шифратор-дешифратор на основе полученного генератора М-последовательности.
3. Оформить лабораторную работу на листах формата А4 в соответствии с правилами оформления студенческих лабораторных работ. Отчет по лабораторной работе должен содержать:

– титульный лист (оформленный по правилам) с указанием названия работы и следующие разделы:
– цель работы;
– краткие теоретические сведения;
– задание на выполнение работы;
– алгоритм решения поставленной задачи (блок-схема и словесное описание по блокам);
– текст программы;
– описание входных / выходных данных программы;
– контрольный пример;
– выводы;
– список использованной литературы.

Необходимо разработать четкий и удобный интерфейс пользователя для задания исходных данных и вывода результатов работы программы.