Технический комитет по стандартизации
«Криптографическая защита информации»
(ТК 26)

ПРОЕКТ МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ

МЕХАНИЗМЫ ВЫРАБОТКИ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Москва
2016

Содержание

Введение

В рамках данного документа приводятся рекомендации по построению механизмов выработки псевдослучайных последовательностей с использованием криптографической функции хэширования.

Ранее в ТК 26 подобные рекомендации не разрабатывались. Они представляют несомненный интерес в связи с активным использованием псевдослучайных чисел и последовательностей при реализации механизмов обеспечения безопасности в различных системах обработки информации.

Методические рекомендации подготовлены специалистами в/ч 43753.

Описание предлагаемого решения

Обозначения

Введём следующие обозначения:

V^*	множество всех двоичных строк конечной длины, включаю пустую строку;
V_x	множество всех двоичных строк длины x, где x – целое неотрицательное число. Нумерация подстрок и компонент строки осуществляется справа налево начиная с нуля;
$\|A\|$	длина (число компонент) строки $A \in V^*$;
θ	пустая строка (строка длины 0);
$A\|\|B$	конкатенация строк $A, B \in V^*$, т.е. строка из $V_{\|A\|+\|B\|}$, в которой левая подстрока из $V_{\|A\|}$ совпадает со строкой A, а правая подстрока из $V_{\|B\|}$ совпадает со строкой B;
A^t	конкатенация t экземпляров строки A;
m	параметр криптографической функции хэширования, называемый длиной блока;

h	параметр криптографической функции хэширования, называемый длиной хэш-кода;
$H : V^* \to V_h$	отображение, реализующее применение криптографической функции хэширования;
$\mathrm{LSB}_s : V^* \setminus \bigcup_{i=0}^{s-1} V_i \to V_s$	отображение, ставящее в соответствие строке $z_{r-1}\|\| \ldots \|\|z_1\|\|z_0, r \geq s$ строку $z_{s-1}\|\| \ldots \|\|z_1\|\|z_0$, $z_i \in V_1$, $i = 0, 1, \ldots, r-1$.

Примечание – Для простоты изложения двоичные строки в ряде случаев будут отождествляться с целыми числами. При этом соответствие задаётся с использованием преобразований, описанных в национальном стандарте Российской Федерации ГОСТ Р 34.11-2012.

Общая схема механизмов выработки псевдослучайных последовательностей

Общая схема механизмов выработки псевдослучайных последовательностей включает следующие основные элементы:

- источник случайности (*некоторый (физический) датчик случайных чисел с обоснованными криптографическими свойствами*);
- внутреннее состояние (*значение, которое используется при выработке псевдослучайных последовательностей*);
- функция инициализации (*некоторое отображение, с использованием которого на основе полученной от источника случайности информации формируется значение (части) внутреннего состояния*);
- функция преобразования внутреннего состояния (*некоторое преобразование, описывающее изменение внутреннего состояния в процессе выработки псевдослучайных последовательностей*);
- функция выработки выхода (*некоторое отображение, описывающее способ выработки псевдослучайного выхода с использованием данного значения внутреннего состояния*).

С использованием указанных элементов схема выработки псевдослучайной последовательности длины t может быть описана при помощи следующего алгоритма:

1. При помощи источника случайности и функции инициализации выработать начальное значение для (части) внутреннего состояния.
2. До тех пор, пока суммарная длина выхода не будет равна t, выполнять следующие действия:
   (a) применить функцию преобразования внутреннего состояния;
   (b) с использованием значения внутреннего состояния, при помощи функции выработки выхода осуществить выработку псевдослучайного выхода.

Примечание – Построение источников случайности с гарантированными криптографическими свойствами является отдельной сложной задачей, которая не рассматривается в данных методических рекомендациях. В дальнейшем предполагается, что подобный источник существует и доступен.

Таким образом, для описания конкретного механизма выработки псевдослучайных последовательностей необходимо указать в явном виде представленные ранее основные элементы.

Описание семейства $\mathcal{PH}$ механизмов выработки псевдослучайных последовательностей с использованием криптографической функции хэширования

В механизмах из данного семейства предполагается использование некоторой криптографической функции хэширования с длиной блока $m \geq 512$ и длиной хэш-кода h.

Примечание – Механизмы из данного семейства, вообще говоря, могут рассматриваться как режимы работы криптографической функции хэширования.

Опишем требуемые элементы на качественном уровне. С использованием источника случайности необходимо выработать двоичную строку длины s, $256 \leq s \leq m - 128$.

– В качестве внутреннего состояния используется двоичная строка U длины $m-1$;

– в качестве функции инициализации используется дополнение выработанной двоичной строки до строки длины $m-1$;

– в качестве функции преобразования внутреннего состояния используется операция сложения значения U с 1 по модулю 2^{m-1};

– в качестве функции выработки выхода используется операция применения криптографической функции хэширования.

Примечание – Значение внутреннего состояния для данного механизма должно сохраняться в секрете.

Для выбранного и зафиксированного значения параметра s, а также значений m и h, определяемых используемой функцией хэширования, опишем механизм выработки псевдослучайной двоичной последовательности R длины t.

Пусть $t = q \cdot h + r$, $q, r \in \mathbb{Z}$, $0 \le r < h$. Тогда рассматриваемый механизм может быть записан с помощью следующей последовательности действий:

Механизм $\mathcal{PH}_{s,m,h}$:

1. Положить $R = \theta$.
2. С использованием источника случайности выработать двоичную строку $K \in V_s$.
3. Положить $U_0 = (K \| 0^l)$, $l = m - s - 1$.
4. Если $q = 0$, перейти на шаг 5, иначе для $i = 1, 2, \ldots, q$ вычислить:
   (а) $U_i = U_{i-1} + 1 (\mathrm{mod}\ 2^{m-1})$;
   (б) $C_i = H(U_i)$.
   (в) Положить $R = C_i \| R$.
5. Если $r = 0$, перейти на шаг 6, иначе вычислить:
   (а) $U_{q+1} = U_q + 1 (\mathrm{mod}\ 2^{m-1})$;

(б) $C_{q+1} = H(U_{q+1})$.

(в) Положить $R = R \| \mathrm{LSB}_r(C_{q+1})$.

6. Выход: R.

Примечание – Исходя из действующих национальных стандартов Российской Федерации, целесообразно использовать значения $s \in \{256, 320, 384\}$, при этом, $m = 512$, $h \in \{256, 512\}$.

Заключительные положения

В данном документе содержится описание семейства механизмов выработки псевдослучайных последовательностей с использованием криптографической функции хэширования.

Криптографические качества результирующих последовательностей могут существенным образом зависеть от свойств используемой функции хэширования; криптографических качеств используемого источника случайности, а также от длин последовательностей, которые вырабатываются с использованием одного значения исходного внутреннего состояния.

Устойчивость к известным методам криптографического анализа механизмов выработки псевдослучайных последовательностей может быть обеспечена только в случае сохранения в секрете используемых значений внутреннего состояния.