УДК 621.391

СТАНДАРТИЗАЦИЯ ИНТЕРФЕЙСА И ФОРМАТА ДАННЫХ

Алексей Остапченко
ЗАО "Битис"

Анотація: **Наведено рекомендації стосовно розробки інтерфейсу та формату даних для реалізації Національного стандарту цифрового підпису.**
Summary: **Interface and data format to implement the National digital signature standard DSTU 4145-2002 recommendation.**
Ключові слова: **Цифровий підпис, еліптичні криві, зображення даних, перетворення даних.**

Стандарт цифровой подписи ДСТУ 4145-2002 определяет обязательный набор функций, определяющих ввод исходных данных и вывод результатов вычислений. Стандарт определяет также формат структур данных, используемых в стандарте, и правила преобразования данных разного типа друг в друга. Соблюдение этих правил обеспечивает взаимодействие реализаций стандарта, созданных разными разработчиками для разных платформ.

При реализации стандарта цифровой подписи ДСТУ 4145-2002 рекомендуется разрабатывать некоторый нормативный набор функций для инициализации и выполнения основных действий датчика случайных чисел и цифровой подписи в формате, указанном ниже. Реализация датчика случайных чисел должна содержать набор функций, доступных для вызова пользователями:

1) инициализация датчика случайных чисел;
2) получение случайной последовательности бит.

Инициализация датчика случайных чисел

Функция инициализации датчика случайных чисел должна обеспечивать ввод таблицы замены и ключа для алгоритма ГОСТ 28147-89, ввод поля состояния и поля даты. Функция предназначена для загрузки начального состояния датчика случайных чисел и инициализации внутренних переменных. Формат представления таблиц замены и ключей должны отвечать стандарту ГОСТ 28147-89. Поле начального состояния и поле даты представляется по правилам, которые стандарт ГОСТ 29147-89 устанавливает для блоков открытого и шифрованного текста.

Получение случайной последовательности бит

Функция получения случайной последовательности должна при каждом обращении возвращать один байт данных, содержащий очередной бит случайной последовательности. Исходным материалом для получения случайных целых чисел и случайных элементов основного поля является случайная последовательность R_{t-1}, K, R_0, полученная в результате t обращений к датчику случайных последовательностей. Стандарт определяет, что R_0 есть результат первого обращения к датчику случайных последовательностей, R_1 есть результат второго обращения к датчику и т. д.

Реализация стандарта цифровой подписи должна содержать набор функций, доступных для вызова пользователем:

1) вычисление базовой точки эллиптической кривой;
2) вычисление пары ключем;
3) сжатие нормализованной точки *P*;
4) восстановление сжатой точки *P*;
5) вычисления цифровой подписи;
6) проверка цифровой подписи;
7) преобразование элемента основного поля в целое число;
8) преобразование хеш-кода в элемент основного поля;
9) преобразование пары целых чисел, представляющих цифровую подпись, в массив байт;
10) преобразование массива байт, содержащего цифровую подпись, в пару целых чисел.

Вычисление базовой точки эллиптической кривой согласно п. 7.3 стандарта

Функция вычисления базовой точки эллиптической кривой содержит в качестве аргументов коэффициенты эклиптической кривой A, B и порядок базовой точки n, формат представления которых

определен стандартом. Функция должна возвращать базовую точку эллиптической кривой P в формате, определенном стандартом независимо от использованного в конкретной реализации внутреннего представления.

Вычисление пары ключей согласно п. п. 9.1 и 9.2 стандарта

Функция вычисления пары ключей содержит в качестве аргументов базовую точку эллиптической кривой P в формате, определенном стандартом независимо от использованного в конкретной реализации внутреннего представления. Функция должна возвращать открытый ключ Q, который вычисляется как $Q = -dP$ и секретный ключ d как случайное не нулевое целое число в виде последовательности байтов.

Сжатие нормализованной точки *P* согласно п. 6.9 стандарта

Функция сжатия нормализованной точки P содержит в качестве аргументов точку P нечетного простого порядка n с координатами (x_P, y_P). Функция должна возвращать сжатое отображение точки в виде байтовой последовательности.

Восстановление сжатой точки *P* согласно п. 6.10 стандарта

Функция восстановления сжатой точки P содержит в качестве аргументов сжатое отображение точки и коэффициенты эллиптической кривой (A, B). Функция должна возвращать восстановленную нормализованную точку P с координатами (x_P, y_P) эллиптической кривой из сжатого состояния.

Вычисление цифровой подписи согласно п. п. 11 и 12 стандарта

Функция вычисления цифровой подписи содержит в качестве аргументов секретный ключ цифровой подписи d, сообщение T длиной $L_T > 0$, хеш функцию H в соответствии с п. 6.2. Функция должна возвращать пару целых чисел (r, s), преобразованных в цифровую подпись D длиной L_D в соответствии с п. 5.10 сообщения T.

Проверка цифровой подписи согласно п. 13 стандарта

Функция проверки цифровой подписи содержит в качестве аргументов открытый ключ цифровой подписи Q, подписанное сообщение (iH, T, D) длинной $L = L(iH) + L_T + L_D$, хеш функцию хеширования H в соответствии с п. 6.2. Функция должна возвращать целое число, которое принимает одно из двух значений – цифровая подпись верна, не верна.

Преобразование элемента основного поля в целое число согласно п. 5.8 стандарта

Функция преобразования элемента основного поля в целое число содержит в качестве аргументов элемент основного поля $x \in GF(2^m)$, $x = (x_{m-1}, \text{K}, x_0)$ и порядок базовой точки эллиптической кривой n. Функция должна возвращать целое число $a = (a_{L-1}, \text{K}, a_0)$, которое удовлетворяет условию $L = L(a) < L(n)$.

Преобразование хеш-кода в элемент основного поля согласно п. 5.9 стандарта

Функция преобразования хеш-кода в элемент основного поля содержит в качестве аргументов хеш код $(h_{L_H-1}, \text{K}, h_0)$, при этом длина хеш-кода должна быть кратна 32 бит.

Функция должна возвращать элемент основного поля $x \in GF(2^m)$, $x = (x_{m-1}, \text{K}, x_0)$.

Преобразование пары целых чисел, представляющих цифровую подпись, в массив байт согласно п. 5.10 стандарта

Функция преобразования пары целых чисел, представляющих цифровую подпись, в массив байт содержит в качестве аргументов пару целых чисел (r, s) в двоичном представлении: $r = (r_{L(r)-1}, \text{K}, r_0)$,

$s = (s_{L(s)-1}, \text{K}, s_0)$, $0 < r < n$, $0 < s < n$, длину цифровой подписи L_D: $L_D \geq 2L(n)$, кратную 16. Функция должна возвращать цифровую подпись $D = (D_{L_D-1}, \text{K}, D_0)$ длиной L_D.

Функция предназначена для выполнения преобразование цифровой подписи в байтовую последовательность, где части (r, s) следуют друг за другом (старший байт первым), для однозначной интерпретации различными программными продуктами.

Преобразование массива байт, содержащего цифровую подпись, в пару целых чисел согласно п. 5.11 стандарта

Функция преобразования массива байт, содержащего цифровую подпись, в пару целых чисел содержит в качестве аргументов двоичный ряд $D = (D_{L_D-1}, \text{K}, D_0)$ четной длины L_D. Функция должна возвращать пару целых чисел $r = (r_{L(r)-1}, \text{K}, r_0)$ и $s = (s_{L(s)-1}, \text{K}, s_0)$.

Функция предназначена для выполнения преобразования байтовой последовательности (где части (r, s) следуют друг за другом – старший байт первым) в числа (r, s) цифровой подписи – для однозначной интерпретации различными программными продуктами.

УДК 612.391

ПРО НАПОВНЕННЯ ЗМІСТУ ПРОФІЛЮЮЧИХ НАВЧАЛЬНИХ ДИСЦИПЛІН СПЕЦІАЛІЗАЦІЇ “ЕЛЕКТРОННІ АПАРАТИ БАНКІВСЬКИХ СИСТЕМ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ”

Юрій Зіньковський, Вадим Клименко
НТУУ „КПІ”

Анотація: **Приведені дані профілюючої дисципліни навчального плану спеціалізації.**
Summary: **The date of profile subject of educational curriculum specialization.**
Ключові слова: **Спеціалізація “Електронні апарати банківських систем і засоби захисту інформації”, профілююча дисципліна.**

Відповідно до Постанови КМУ № 664 від 23. 04. 1999 р. “Про розроблення та запровадження науково-обґрунтованої системи підготовки спеціалістів в галузі технічного захисту інформації” в Національному технічному університеті України “Київський політехнічний інститут” на Радіотехнічному факультеті на кафедрі Радіоконструювання і виробництва радіоапаратури відкрита нова спеціалізація “Електронні апарати банківських систем і засоби захисту інформації”. Нині відбудеться перший випуск спеціалістів нової спеціалізації. Нормативні матеріали навчального процесу створені для забезпечення необхідної якості підготовки спеціалістів нового навчального напряму, яка б відповідала сучасним вимогам.

Профілюючою дисципліною навчального плану спеціалізації є дисципліна “Методи та апаратура захисту інформації”.

Дисципліна читається для спеціалістів та магістрів спеціалізації “Електронні апарати банківських систем і засоби захисту інформації” спеціальності “Виробництво електронних засобів” у десятому семестрі кафедрою Радіоконструювання і виробництва радіоапаратури обсягом 135 навчальних годин (68 – аудиторних; 67 – курсова робота та самостійна робота студентів). Аудиторні години: 51 – лекції; 17 – лабораторні заняття.

Мета вивчення дисципліни — надати випускникам спеціалізації (спеціалістам та магістрам) необхідні знання в галузі захисту інформації, що дозволить їм розробляти та запроваджувати необхідні методи та технічні рішення щодо захисту інформації в процесах та операціях інформаційної діяльності. Курс дисципліни має за мету вивчення організаційно-методичних, аналітичних, фізичних, інженерно-фізичних, теоретико-інформаційних, алгоритмічних, програмно-технічних аспектів проблеми, а основних можливих каналів витоку та несанкціонованого вилучення інформації; пошуку, нейтралізації та знешкодження каналів можливої втрати інформації. Метою також є вивчення методів упорядкування діяльності, стандартизації та сертифікації в галузі захисту інформації.

До складу тематичного плану дисципліни увійшло одинадцять розділів: