ОПИС
генератора випадкових послідовностей

Робота генератора випадкових двійкових послідовностей (далі - Генератор) базується на вимогах додатка А до національного стандарту України ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння», затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі - ДСТУ 4145-2002), із застосуванням криптографічного перетворення відповідно до національного стандарту України ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення», затвердженого наказом Міністерства економічного розвитку і торгівлі України від 29 грудня 2014 року № 1484 (далі - ДСТУ 7624:2014).

Генератор використовується для отримання випадкових цілих чисел, випадкових елементів основного поля і випадкових точок еліптичних кривих.

Генератор за одне звернення до нього видає випадковий рядок довжини t = 1.

Як криптографічне перетворення в Генераторі застосовується алгоритм криптографічного перетворення згідно з ДСТУ 7624:2014 у режимі «Калина-256/256-ECB» (проста заміна відповідно до розділу 6 ДСТУ 7624:2014).

Умови отримання та використання особистого ключа мають унеможливлювати доступ до нього або його частини, модифікацію, підміну або знищення.

Особистий ключ криптографічного перетворення згідно з ДСТУ 7624:2014, що використовується в Генераторі, не можна використовувати для іншої мети.

Позначимо через $E_k()$ шифрування двійкового рядка завдовжки 256 двійкових розрядів алгоритмом ДСТУ 7624:2014 в режимі «Калина-256/256-ECB» на ключі k завдовжки 256 двійкових розрядів. Нехай s, I, x - двійкові рядки завдовжки 256 двійкових розрядів, D - двійковий рядок завдовжки 64 двійкові розряди. Перед застосуванням задають початковий стан Генератора випадкових послідовностей.

Встановлення початкового стану Генератора

Встановлення початкового стану Генератора здійснюється за таким алгоритмом:

задають початкове значення s Генератора.

Для цього використовують фізичне джерело випадковості.

Як фізичне джерело випадковості можна використовувати, наприклад, квантові ефекти в напівпровідниках (шумові діоди тощо), сигнал від мікрофонного входу з відключеним мікрофоном, часові інтервали між натисканнями на клавіші клавіатури, часові інтервали між натисканнями на клавіші миші.

Початковий стан Генератора є таємним.

Умови отримання початкового стану Генератора мають унеможливлювати доступ до нього або його частини, модифікацію, підміну або знищення;

задають значення двійкового рядка D.

Для цього використовують поточні значення дати і часу з точністю 64 двійкові розряди;

обчислюють двійковий рядок $I = E_k(0^{192} || D)$.

Використання Генератора

При кожному зверненні до Генератора виконують такі обчислення (символ $\oplus$ позначає порозрядне додавання за модулем 2 двійкових рядків завдовжки 256 двійкових розрядів):

$$x = E_k(I \oplus s);$$

$$s = E_k(x \oplus I).$$

Випадковим двійковим рядком є двійковий рядок довжини 1, який складається з крайнього правого розряду x_0 двійкового рядка $x = (x_{255},...,x_0)$.».