МИКРОПРОЦЕССОРНЫЙ ГЕНЕРАТОР ПАРОЛЕЙ НА МИКРОКОНТРОЛЛЕРЕ PIC16F877A

Токарев М.Г., к.т.н., доц. Подорожняк А.А.
Национальный технический университет «ХПИ», Харьков

Современная информатика широко использует псевдослучайные числа в самых разных приложениях – от метода Монте-Карло и имитационного моделирования до криптографии. При этом от качества используемых псевдослучайных последовательностей чисел (ПСЧ) напрямую зависит качество получаемых результатов.

В докладе рассмотрены принципы генерации ПСЧ, генерация псевдослучайный последовательностей с помощью хеш-функций и применение ПСЧ и хеш функций для генераторов паролей. Важность выбора надежного источника энтропии и его влияние на распределенность генерируемых последовательностей и следовательно паролей. Рассмотрены сильные и слабые стороны некоторых популярных существующих решений (C random, xxHash).

Предложен оригинальный алгоритм генерации паролей с использованием интервалов нажатия клавиш в качестве надежного источника энтропии. Представлены результаты исследования известных и предложенного алгоритма. Проведенный анализ показал, что данный алгоритм позволяет генерировать значительно более надежные пароли чем существующие на данный момент решения.

Было разработано устройство, позволяющее генерировать 16-значные пароли несколькими способами, в том числе и с использованием датчика температуры и предложенного метода генерации. Проведено моделирование его работы в системе Proteus и тестирование на микропроцессорном стенде PIC EASY.

Целью дальнейших исследований является повышение надежности полученных результатов и уменьшение времени генерации пролей.