В чому основне призначення генераторів випадкових послідовностей в криптографічних додатках та криптографічних протоколах та які вимоги до них?

Генераторы случайных и псевдослучайных чисел позволяют создавать последовательности случайных чисел, которые широко используются в криптографии, в частности:

- случайные числа необходимы для генерации секретных ключей, которые, в идеале, должны быть абсолютно случайными;
- случайные числа применяются во многих алгоритмах электронной подписи;
- случайные числа используются во многих схемах аутентификации.

Не всегда возможно получение абсолютно случайных чисел - для этого необходимо наличие качественных аппаратных генераторов. Однако, на основе алгоритмов симметричного шифрования можно построить качественные генераторы псевдослучайных чисел.

ребования к КСГПСЧ можно разделить на две группы: во-первых, они должны проходить статистические тесты на случайность; а во-вторых, они должны сохранять непредсказуемость, даже если часть их исходного или текущего состояния становится известна криптоаналитику. А именно:

- КСГПСЧ должен удовлетворять «тесту на следующий бит». Смысл теста в следующем: не должно существовать полиномиального алгоритма, который, зная первые *k* битов случайной последовательности, сможет предказать (*k*+1)-ый бит с вероятностью более 50 %. Эндрю Яо доказал в 1982 году, что генератор, прошедший «тест на следующий бит», пройдёт и любые другие статистические тесты на случайность, выполнимые за полиномиальное время.
- КСГПСЧ должен оставаться надёжным даже в случае, когда часть или все его состояния стали известны (или были корректно вычислены). Это значит, что не должно быть возможности получить случайную последовательность, созданную генератором, предшествующую получению этого знания криптоаналитиком. Кроме того, если во время работы используется дополнительная энтропия, попытка использовать знание о входных данных должна быть вычислительно невозможна.

Большинство генераторов псевдослучайных чисел не подходят для использования в качестве КСГПСЧ по обоим критериям. Во-первых, несмотря на то, что многие ГПСЧ выдают последовательность случайную с точки зрения разнообразных статистических тестов, они не надёжны по отношению к обратной разработке. Могут быть обнаружены специализированные, особым образом настроенные тесты, которые покажут, что случайные числа, получаемые из ГПСЧ не являются по-настоящему случайными. Во-вторых, для большинства ГПСЧ возможно вычислить всю псевдослучайную последовательность, если их состояние

скомпрометировано, что позволит криптоаналитику получить доступ не только к будущим сообщениям, но и ко всем предыдущим. КСГПСЧ разрабатываются с учётом сопротивляемости к различным видам криптоанализа.