**Сравнительный анализ поточных шифров**

|  |  |  |  |
| --- | --- | --- | --- |
| **Характеристика** | **RC4** | **ChaCha20** | **A5/1** |
| **Год создания** | 1987 | 2008 | 1987 |
| **Тип шифра** | Поточный | Поточный | Поточный |
| **Ключевая длина** | 40-2048 бит (обычно 128 бит) | 256 бит | 64 бит |
| **Раунды/Итерации** | Не применимо | 20 (при 256 битах ключа) | Не применимо |
| **Структура ключа** | Использует ключевой поток | Использует матрицу ключа | 3 регистра сдвига |
| **Производительность** | Быстрый | Быстрый | Средний |
| **Атаки на ключи** | Возможны атаки на слабые ключи | Устойчив к известным атакам | Возможны атаки на ключи |
| **Сложность реализации** | Простая | Средняя | Сложная |
| **Распространенность** | Широко используется | Распространен | Используется в GSM и GPRS |
| **Достоинства** | Прост в реализации, быстрый | Безопасность, эффективность | Прост в реализации, применяется в GSM |
| **Недостатки** | Существуют уязвимости в некоторых реализациях | Может быть медленным на некоторых устройствах | Слабая длина ключа, неудовлетворительная стойкость |
| **Примечания** | Использование не рекомендуется в новых системах | Разработан Дэниэлем Бернштайном | Применяется в сетях GSM, но считается устаревшим |