**Сравнительный анализ алгоритмов цифровых подписей**

|  |  |  |  |
| --- | --- | --- | --- |
| **Характеристика** | **RSA** | **ElGamal** | **ECDSA** |
| **Год создания** | 1977 | 1985 | 1992 |
| **Тип алгоритма** | Асимметричный | Асимметричный | Асимметричный |
| **Основан на** | Факторизации больших чисел | Дискретном логарифме в конечном поле | Эллиптических кривых |
| **Процесс подписи** | Сначала вычисляется хэш сообщения.  Затем хэш подписывается с использованием закрытого ключа. | Генерируется случайное значение (k).  Вычисляется часть подписи с использованием открытого ключа и случайного значения.  Вычисляется вторая часть подписи с использованием закрытого ключа. | Использует эллиптические кривые для операций подписи и верификации |
| **Процесс верификации** | Проверка подписи с использованием открытого ключа | Проверка подписи с использованием открытого ключа | Проверка подписи с использованием открытого ключа |
| **Длина ключа** | Обычно 1024–4096 бит | Обычно 1024–3072 бит | Зависит от уровня безопасности, но короткие ключи достаточны |
| **Стойкость к атакам** | Высокая | Высокая | Высокая |
| **Производительность** | Подписывание и проверка могут быть ресурсоемкими, особенно с длинными ключами | Подписывание и проверка могут быть ресурсоемкими, особенно с длинными ключами | Хорошая производительность, особенно с короткими ключами |
| **Достоинства** | Широко используется, высокая стойкость | Хорошая стойкость, можно использовать для шифрования и подписи | Эффективен с короткими ключами, лучшая производительность на некоторых устройствах |
| **Недостатки** | Возможны атаки, связанные с факторизацией (например, квантовые атаки) | Может быть менее эффективным по сравнению с RSA | Требует внимательного выбора параметров для обеспечения безопасности |