**Сравнительный анализ блочных шифров**

|  |  |  |  |
| --- | --- | --- | --- |
| **Характеристика** | **DES** | **AES** | **Twofish** |
| **Год создания** | 1977 | 2002 | 1998 |
| **Тип шифра** | Блочный | Блочный | Блочный |
| **Размер блока** | 64 бита | 128 бит | 128, 192, 256 бит |
| **Размер ключа** | 56 бит (фактически 64 бита, 8 бит используются для контроля четности) | 128, 192, 256 бит | 128, 192, 256 бит |
| **Раунды/Итерации** | 16 | 10 (128 бит ключ), 12 (192 бит ключ), 14 (256 бит ключ) | 16 |
| **Структура ключа** | Изначально 56 бит, но 8 бит используются для контроля четности | Различные по ключу и блоку данных | Подстановки и перестановки |
| **Производительность** | Относительно низкая | Высокая | Средняя |
| **Атаки на ключи** | Существуют эффективные атаки, такие как атака на временную сложность | Устойчив к широкому спектру атак | Устойчив к большинству атак |
| **Сложность реализации** | Легко реализовать | Легко реализовать | Средняя |
| **Распространенность** | Использовался широко, но теперь считается устаревшим | Широко используется в различных приложениях | Используется в некоторых приложениях |
| **Достоинства** | Историческое значение, легкость реализации | Высокая производительность, широкое применение | Гибкость, высокая производительность |
| **Недостатки** | Короткий ключ, уязвимость к современным атакам | Возможны атаки на реализации (не на сам алгоритм) | Может потребовать больше ресурсов |
| **Примечания** | Считается устаревшим, не рекомендуется для новых систем | Рекомендуется к использованию | Надежный шифр, но AES предпочтителен из-за широкой поддержки и стандартизации. |