Сутність основних проблем теорії та практики криптології? Які критерії та показники можна застосувати для оцінки стійкості та складності ЕЦП?

В настоящее время в современной криптографии существуют следующие проблемы:

1. Ограниченность числа рабочих схем. В отличие от алгоритмов классической криптографии, которые могут быть созданы в неограниченном количестве путем комбинирования различных элементарных преобразований, каждая "современная" схема базируется на определенной "нерешаемой" задаче. Как следствие, количество рабочих схем криптографии с открытым ключом весьма невелико.
2. Постоянная "инфляция" размера блоков данных и ключей, обусловленная прогрессом математики и вычислительной техники. Так, если в момент создания криптосистемы RSA считался достаточным размер чисел в 512 бит, то сейчас рекомендуется не менее 4 Кбит. Иными словами, "безопасный" размер чисел в RSA вырос практически на порядок; похожая картина наблюдается и для других схем, тогда как в традиционной криптографии этот размер увеличился всего вдвое.
3. Потенциальная ненадежность базиса. В настоящее время теорией вычислительной сложности исследуется вопрос о возможности решения задач данного типа за полиномиальное время (гипотеза P = NP). В рамках теории уже доказана связь большинства используемых вычислительно сложных задач с другими аналогичными задачами. Это означает, что, если будет взломана хотя бы одна современная криптосистема, многие другие также не устоят.
4. Отсутствие дальней перспективы. Уже известен предполагаемый "могильщик" современной криптографии - это квантовые вычисления, с помощью которых оказалось возможным решать многие задачи гораздо быстрее, чем на традиционных компьютерах. Правда, в настоящее время

они существуют лишь в теории, из практических достижений можно отметить только успешную факторизацию числа 15 "микромакетом" квантового вычислителя. Специалисты полагают, что "серьезные" квантовые компьютеры появятся примерно через 25-30 лет, и за пределами этого срока будущее современной криптографии туманно. Из всего вышесказанного следует, что для современной криптографии актуальна проблема повышения стойкости и уменьшения размера блоков данных путем модификации уже существующих криптосистем.

Для оцінкі ЕЦП можна використовувати наступне:

- Стійкість геш-функції
- Стійкість ключа ЕЦП