Криптография не занимается: защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищенных системах передачи данных.

в настоящее время методов криптографической защиты информации и способов ее реализации. Выбор для конкретных систем должен быть основан на глубоком анализе слабых и сильных сторон тех или иных методов защиты. Обоснованный выбор той или иной системы защиты в общем-то должен опираться на какие-то критерии эффективности. К сожалению, до сих пор не разработаны подходящие методики оценки эффективности криптографических систем.

Наиболее простой критерий такой эффективности - вероятность раскрытия ключа или мощность множества ключей (M). По сути это то же самое, что и криптостойкость. Для ее численной оценки можно использовать также и сложность раскрытия шифра путем перебора всех ключей. Однако, этот критерий не учитывает других важных требований к криптосистемам:

невозможность раскрытия или осмысленной модификации информации на основе анализа ее структуры, совершенство используемых протоколов защиты ,минимальный объем используемой ключевой информации, минимальная сложность реализации (в количестве машинных операций), ее стоимость, высокая оперативность.

Поэтому желательно конечно использование некоторых интегральных показателей, учитывающих указанные факторы. Но в любом случае выбранный комплекс криптографических методов должен сочетать как удобство, гибкость и оперативность использования, так и надежную защиту от злоумышленников циркулирующей в системе информации.