УКАЗАНИЕ К РЕШЕНИЮ ЗАДАЧИ № 33

Симметричные алгоритмы - и в частности DES - быстры, поэтому ими удобно шифровать большие объемы информации. Однако для передачи ключа симметричного алгоритма требуется надежный канал передачи, который очень часто отсутствует. Таким образом, преимущества таких алгоритмов сводится на нет. С другой стороны, асимметричные алгоритмы не требуют секретного канала для передачи ключа, но на практике криптосистемы с открытым ключом используются для шифрования не сообщений, а ключей. На это есть две основные причины:

1. Алгоритмы шифрования с открытым ключом в среднем работают в тысячи раз медленнее, чем алгоритмы с симметричным ключом, а также они требовательны к памяти и вычислительной мощности компьютера, поэтому большие тексты кодировать этими алгоритмами нецелесообразно.
2. Алгоритмы шифрования с открытым ключом уязвимы по отношению к криптоаналитическим атакам со знанием открытого текста. Пусть C=E(P), где C обозначает шифртекст, P – открытый текст, E – функцию шифрования. Тогда, если P принимает значения из некоторого конечного множества, состоящего из n открытых текстов, криптоаналитику достаточно зашифровать все эти тексты, используя известный ему открытый ключ, и сравнить результаты с C. Ключ таким способом ему вскрыть не удастся, однако открытый текст будет успешно определен.

Возможно следующее решение: сообщение кодируется симметричным алгоритмом, что позволяет выиграть в скорости, т.к. сообщение может быть сколь угодно большим. Ключ симметричного алгоритма (обычно маленький, для DES - 64 бита) кодируется асимметричным алгоритмом.