Лабораторная работа 4. Шифрование с открытым ключом

В лабораторной работе необходимо зашифровать свою фамилию с помощью следующих шифров:

- алгоритма RSA;

- алгоритма на основе задачи об укладке ранца;

- алгоритма шифрования Эль-Гамаля.

При оформлении отчета необходимо привести исходное сообщение (фамилию) и таблицы генерации ключей, шифрования и расшифрования.

Для первого и третьего способов принять код символа в соответствии с его положением в алфавите, для второго – с кодировкой Windows 1251.

Для алгоритма шифрования Эль-Гамаля случайные числа k для каждой буквы исходного сообщения должны быть разными.

Контрольные вопросы

1. В чем заключается суть и основная предпосылка появления шифрования с открытым ключом?
2. Основные требования, предъявляемые к криптосистемам с открытым ключом.
3. Перечислите типы односторонних преобразований, применяемых при асимметричном шифровании.
4. Что означает обратное число по модулю?
5. В чем отличие вероятностного шифрования с открытым ключом от детерминированного?
6. В чем суть задачи дискретного логарифмирования?