Задание на лабораторную работу

- В соответствие с вариантом выберите и установите одну из программ:
    1. CryptoAPP,
    2. GPG4Win,
    3. КриптоАРМ.
- Изучите «Руководство пользователю»
- Ознакомьтесь с работой программы. Внимательно изучите процессы создания ключей, распространения открытых и сохранения в тайне закрытых ключей, схему разделения и сборки ключей.
- Создайте свою собственную пару ключей (открытый и закрытый). Распространите в группе свой открытый ключ. Например, выложите открытый ключ в общей папке в локальной сети.
- Всеми членами группы осуществить последовательно действия:
    - подготовить документ (файл), который необходимо переслать другому пользователю;
    - подписать файл цифровой подписью;
    - зашифровать подписанный файл с помощью открытого ключа другого пользователя;
    - передать зашифрованный файл пользователю, чей ключ использовался при шифровании;
    - получатель должен расшифровать файл и проверить достоверность ЭЦП;

- Напишите отчёт по работе (если какие либо из заданных пунктов выполнить в выбранной вами программе не возможны, отобразите это в отчёте).
- Прикрепите к отчёту полученные в ходе работы файлы. Кратко поясните их назначение.

Контрольные вопросы

- Что такое – электронная цифровая подпись?
- Основное назначение сертификата открытого ключа?
- Что включает в себя сертификат?
- Что привело к необходимости создания PKI.
- Какие задачи позволяет решать PKI.
- Основные компоненты PKI и их функции