Assignment #2

Asymmetrical Cryptosystems

Please coded an implementation to satisfy the followings:

- There are two parties as Alice and Bob (or sender and receiver respectively).
- First they agree on used cryptosystem for communication:
    - If they select symmetrical encryption for secrecy of communication:
        - First they create/share symmetric encryption key by DH Key exchange algorithm.
        - Second they start their communication with DES or AES with shared key. (Note: There are different DES and AES implementations in Internet. You can download and use one of them for this assignment).
    - If they select asymmetrical communication:
        - User of the application should decide to use RSA or ElGamal.
        - Alice and Bob create their private and public keys and announced their public keys to each other according to selected scheme (RSA or ElGamal).
        - Allice ask one word message from user to encrypt it with Bob's public key and sends it to Bob.
        - Bob receives encrypted word and decrypt it with his private key and shows this decrypted word to user of application.

Notes:

- You can write your code in C or Java.
- Please try to build your code for multi-precision (big) integer numbers.
- Please prepare a short report about your implementation environment and explanations for your code, your experiments and add some screen shots about selected example executions for each module.
- Submit the report, source and executable object code of your assignment under one compressed file (Cng471-StudentName-Surname-Hw2.zip).
- The last submission date for this assignment: May 13, 2018 Sunday, until 22:00.

Thank you.

Serap