Diffie Hellman exercise

Generate DH parameters of 2048-bit using the command line tool.

Write a dh.cpp program, which:

1. Generate an ephemeral DH pair using the parameters previously generated (you can paste the parameters inside the code);
2. Writes the public key into a file (let the user choose the name);
3. Loads the peer public key from a file (let the user choose the name)
4. Derives a shared secret from the generated private key and the peer public key.
5. Encrypt an existing file for the peer using the first 16 bytes of the shared secret using AES-128 in cbc mode.
6. Decrypt the file encrypted by the peer

Write a single source file and then try it by launching two different processes from the terminal.

Every 15 minutes the solution for a checkpoint will be revealed.