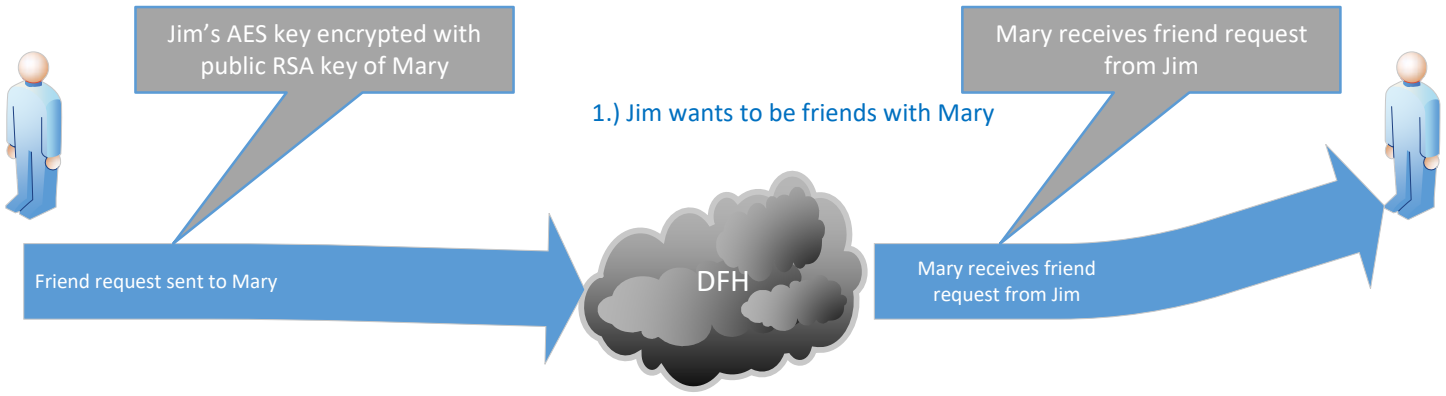
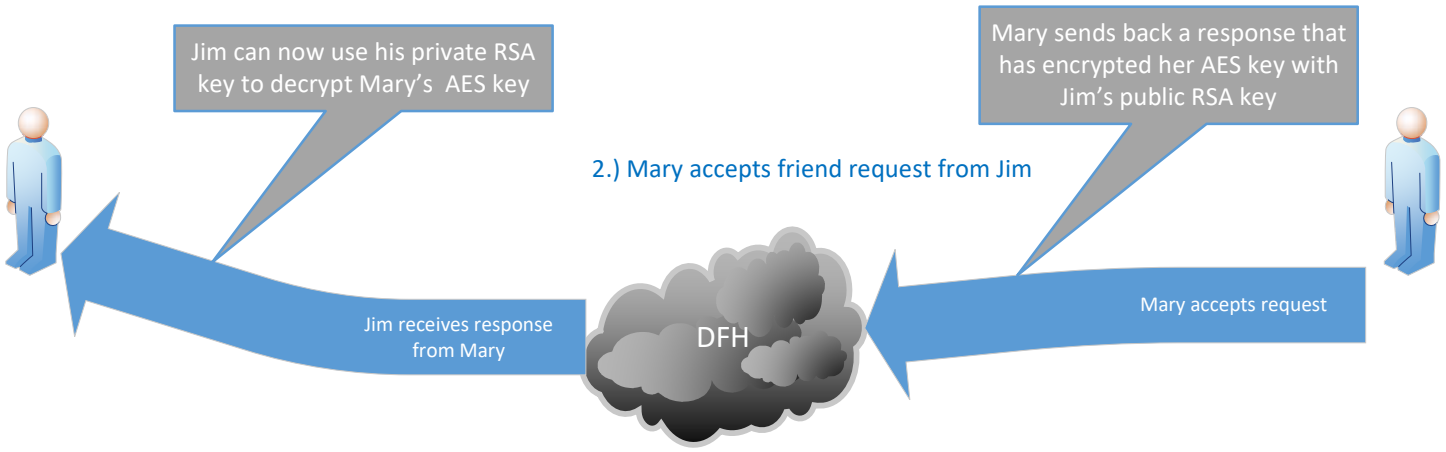
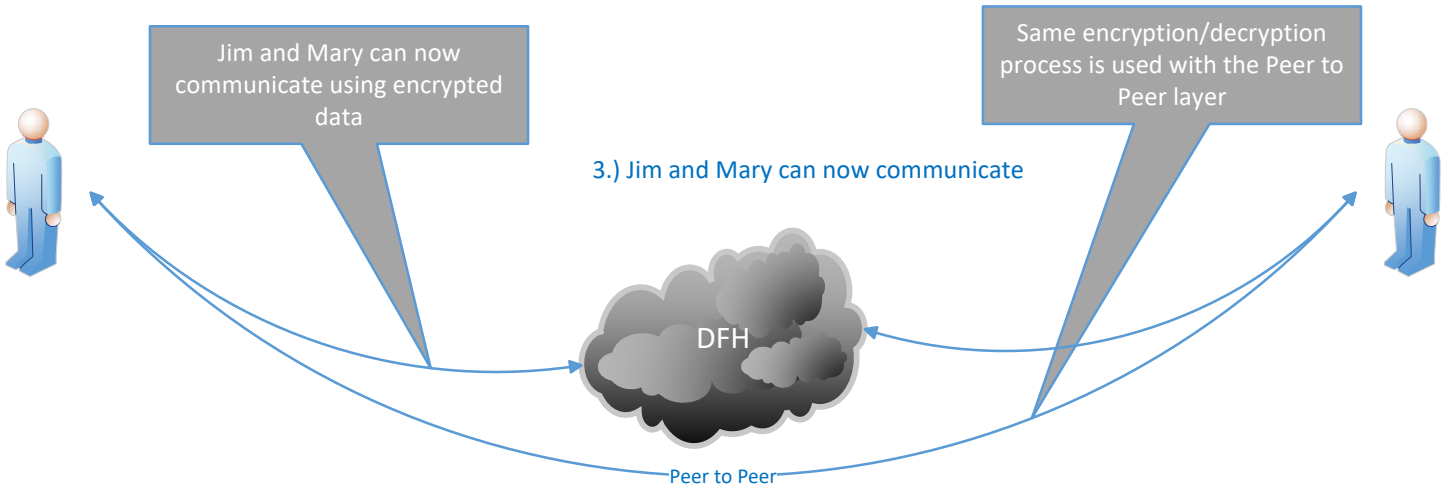
Project XIII makes use of both AES and RSA keys for data encryption. The RSA keys exist to facilitate the exchange of AES keys between friends. They provide key encapsulation. The RSA keys means these two people do not have to depend or trust a third party to keep the initial exchange of keys secure. The RSA keys are symmetrical; there is a public key and a private key. The public key is used to encrypt data. The private key is used to decrypt it. So if Jim wants to send Mary an encrypted message he encrypts the message with Mary's public key. She has the private key; so she is able to decrypt that message securely; knowing that she is the only one who can decode it.

RSA keys have a limit to the amount of data that they can encrypt that is related to the key size. To enable encryption of larger records the AES key is used. Project XIII uses the AES key to encrypt all communication between friends with the exception of the initial AES key exchange. Project XIII takes the public RSA key on the DFH and encrypts the AES key of 'Friend A' with the public RSA key of 'Friend B.' When 'Friend B' accepts the friendship request the AES key of 'Friend A' can now be decoded by the private RSA key of 'Friend B.' The AES key of 'Friend B' is now encrypted by the public RSA key of 'Friend A' and the sent through the Data Flow Hub (DFH). Now each friend has a copy of each others' AES key. They can now encrypt and decrypt documents, chats, E-VOIP, etc.







For further information on AES keys please see: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
For more information on RSA keys please see: http://en.wikipedia.org/wiki/RSA
Please see http://en.wikipedia.org/wiki/Key_encapsulation for more details on key encapsulation