1. **Node**: Represents a node in the network, equipped with RSA public-private key pairs for secure communication.
2. **User**: A collection of nodes belonging to a single user. Each user has its set of nodes for encryption and decryption of messages.
3. **EncryptSymmetric**: Function to encrypt a message using a symmetric key (AES).
4. **DecryptSymmetric**: Function to decrypt a message using a symmetric key (AES).
5. **EncryptRSA**: Function to encrypt a message using RSA asymmetric encryption.
6. **DecryptRSA**: Function to decrypt a message using RSA asymmetric encryption.
7. **Mix**: Function to mix and encrypt messages for transmission to recipient nodes.
8. **Demix**: Function to decrypt and demix messages received from sender nodes.

Encryption logic

* **Symmetric Encryption**:
  + A random symmetric key (AES) is generated for each message.
  + The message is encrypted using the symmetric key.
* **Asymmetric Encryption**:
  + The symmetric key is encrypted separately for each recipient node using their public RSA key.
  + The encrypted symmetric key is appended to the encrypted message.
* **Message Mixing**:
  + The mixed message consists of the encrypted message and the encrypted symmetric keys for each recipient.

Program lacks layered encryption, but has mixing

UserA can write a message, it will be encrypted and sent to UserB, same for userB

To run program, you can run cryptonet.exe