RSA – En/decryption

- Suppose the keys are generated by Bob. Bob gives Alice its public key E and the number N.
- Alice wants to send a character “F” to Bob. She’ll use Bob’s public key to encrypt it
  - $CT = PT^E \bmod N = PT^E \bmod P*Q$
  - Alice sends $6^5 \bmod 119 = 41$
- Bob uses the following: $PT = CT^D \bmod N$
  - Bob gets $41^{77} \bmod 119 = 6$