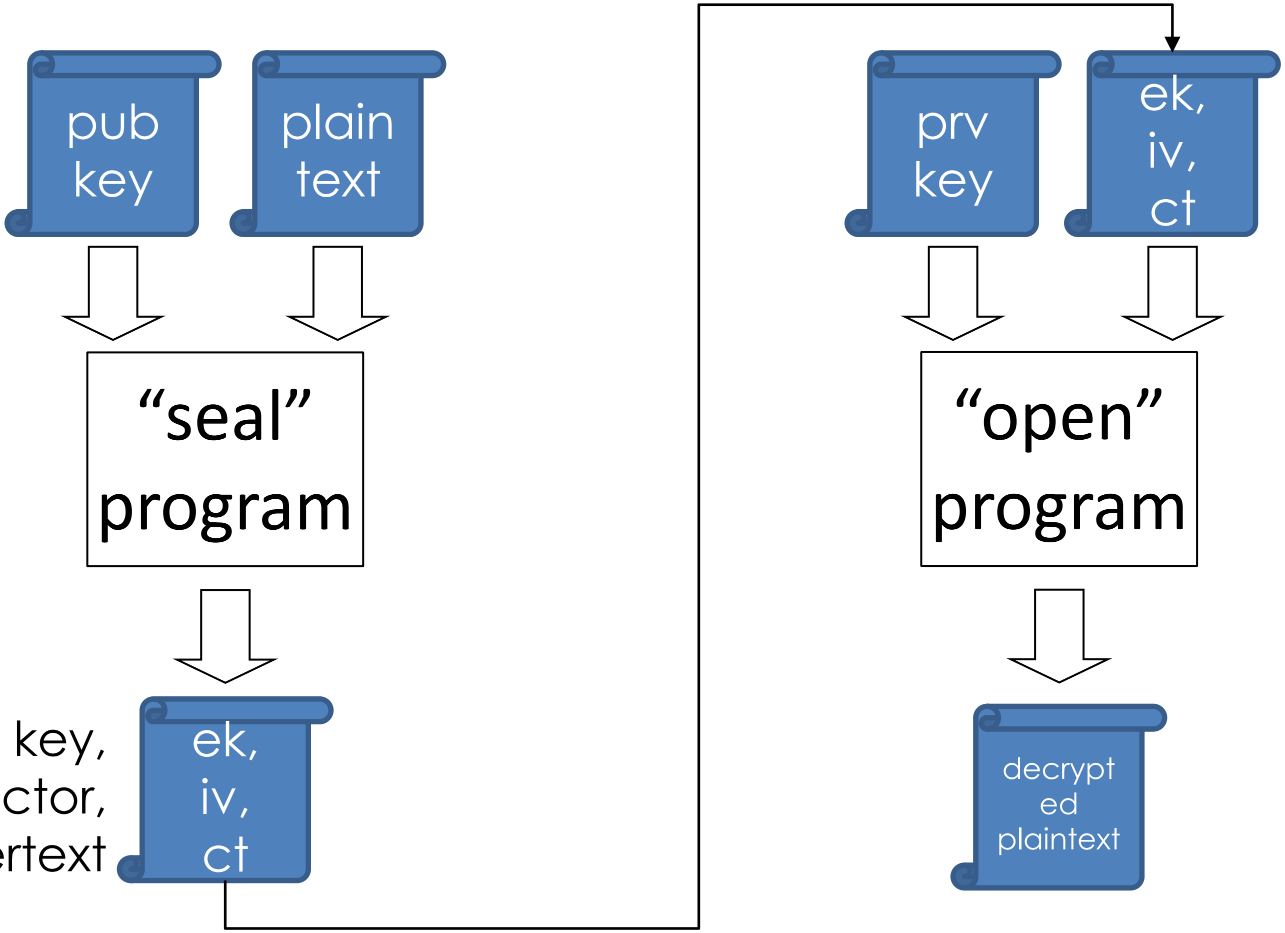
Asymmetric Encryption Exercise

- Generate a pair of 2048-bit RSA keys. Private key must be protected by a password.
- Write a “seal” program, which:
  - reads the public key and a file to encrypt;
  - encrypts the file with asymmetric encryption (AES-128 in CBC);
  - writes in another file: the encrypted symmetric key, the initialization vector, the ciphertext.
- Write an “open” program, which:
  - reads the private key;
  - reads the encrypted symmetric key, the initialization vector and the ciphertext from a file;
  - decrypts them;
  - writes the plaintext in another file;

Asymmetric Encryption Exercise



Encrypted key,
Initialization vector,
Ciphertext