Foundations of Cybersecurity Asymmetric Encryption with OpenSSL

Michele La Manna
Dept. of Information Engineering
University of Pisa
michele.lamanna@phd.unipi.it
Version: 2022-05-09

Asymmetric Encryption Exercise

Today you will write two programs: one that asymmetrically encrypts an already existing file, and one that decrypts the resulting ciphertext.

First of all, generate a pair of 2048-bit RSA keys with the command-line tool.

The Private key must be protected by a password.

Asymmetric Encryption Exercise

"seal" program, which:

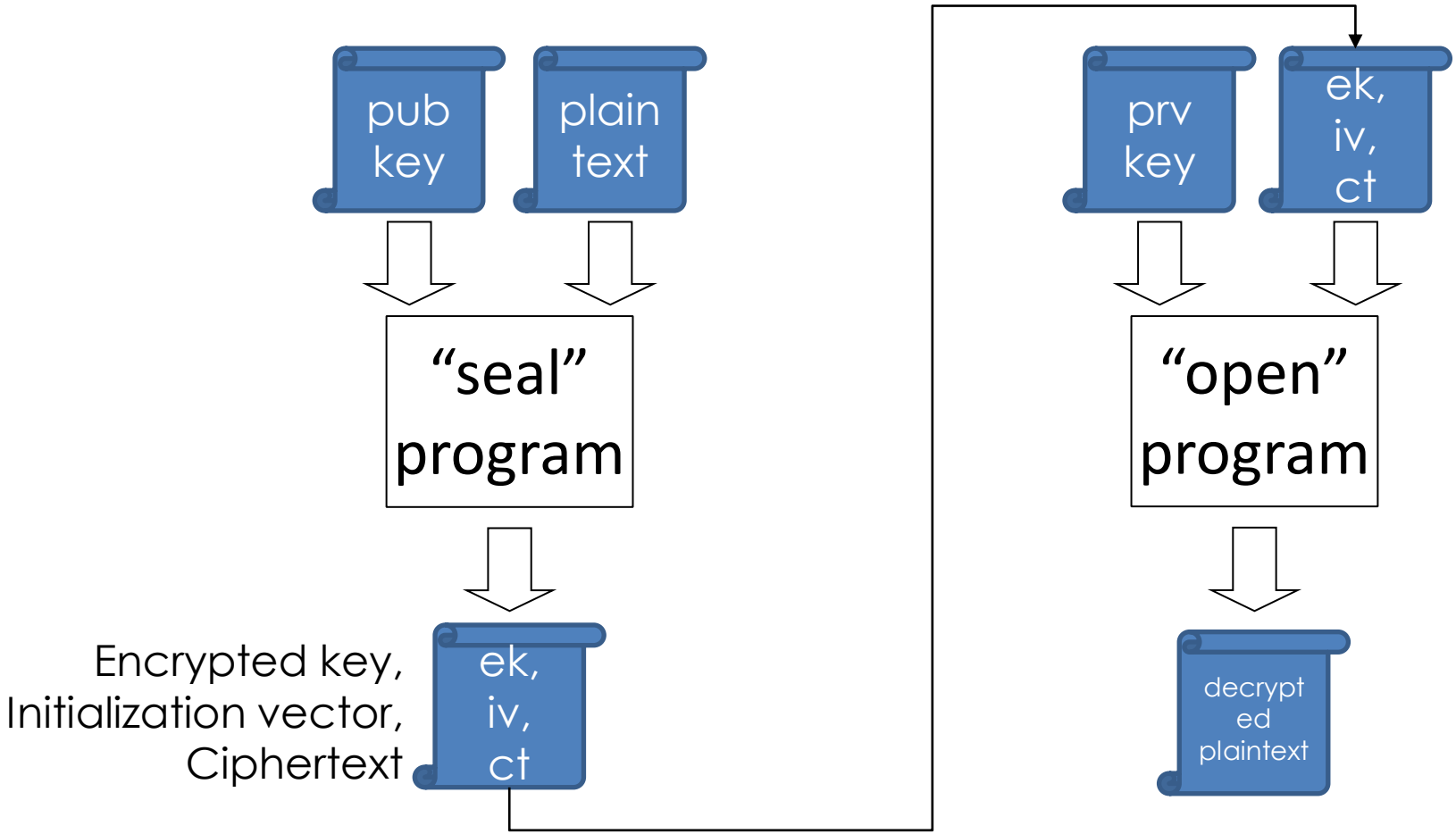
- reads the public key and a file to encrypt;
- encrypts the file with symmetric encryption (AES-128 in CBC);
- writes in another file: the encrypted symmetric key, the initialization vector, the ciphertext.

"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

UNIVERSITÀ DI PISA



Digital Envelope (Asymmetric Encryption)

Generate a pair of 2048-bit RSA keys with the command-line tool.
The Private key must be protected by a password.

5 minutes

Checkpoint 1 (1/1)

UNIVERSITÀ DI PISA

Generate a private key protected by a password:

```
>openssl genrsa -aes128 -f4 -out key.pem
```

(a prompt asking the password will appear)

Extract a public key from a file:

```
>openssl rsa -in key.pem -outform PEM -pubout -out public.pem
```

Digital Envelope (Asymmetric Encryption)

Write a "seal" program, which:
reads the public key and a file to encrypt;
encrypts the file with symmetric encryption (AES-128 in CBC);
writes in another file: the encrypted symmetric key, the initialization vector, the ciphertext.

20 minutes

Digital Envelope (Asymmetric Encryption)

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;

20 minutes