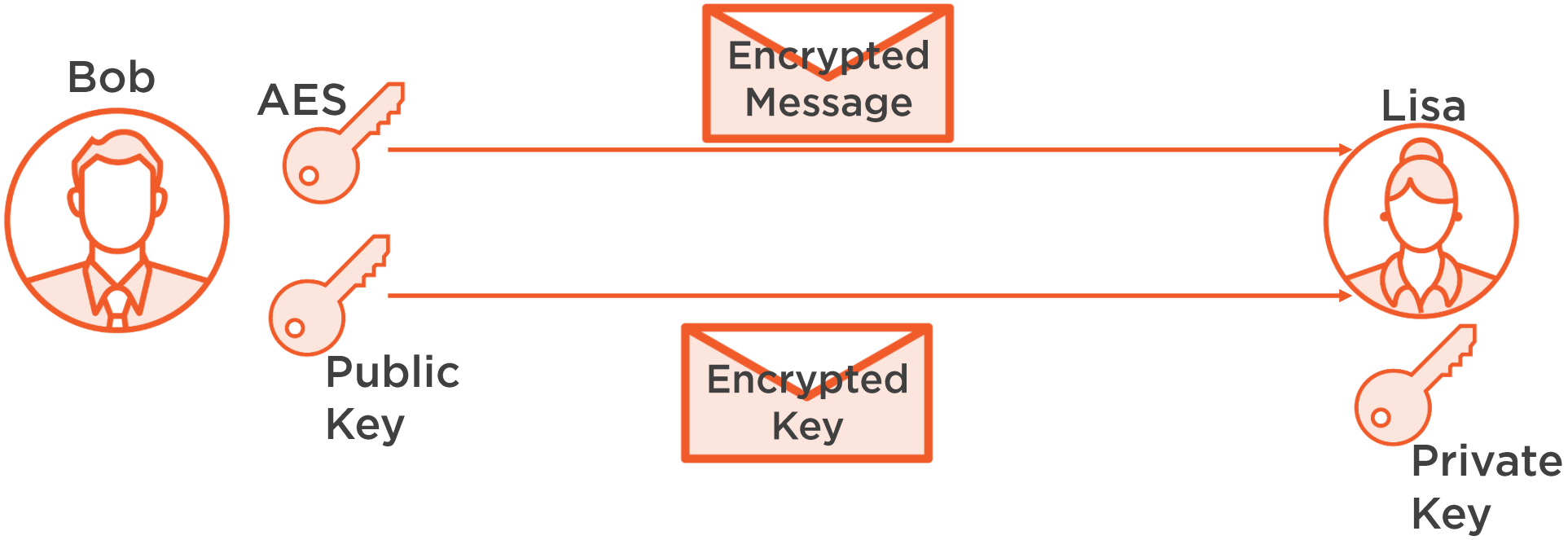
Asymmetric Encryption

Gus Khawaja

Gus.Khawaja@guskhawaja.me
www.ethicalhackingblog.com

Asymmetric Encryption

Example


Bob
AES
Encrypted Message
Lisa
Public Key
Encrypted Key
Private Key

Asymmetric Encryption

Public Key

- Share with everyone
- Not secret
- Encrypt data

Private Key

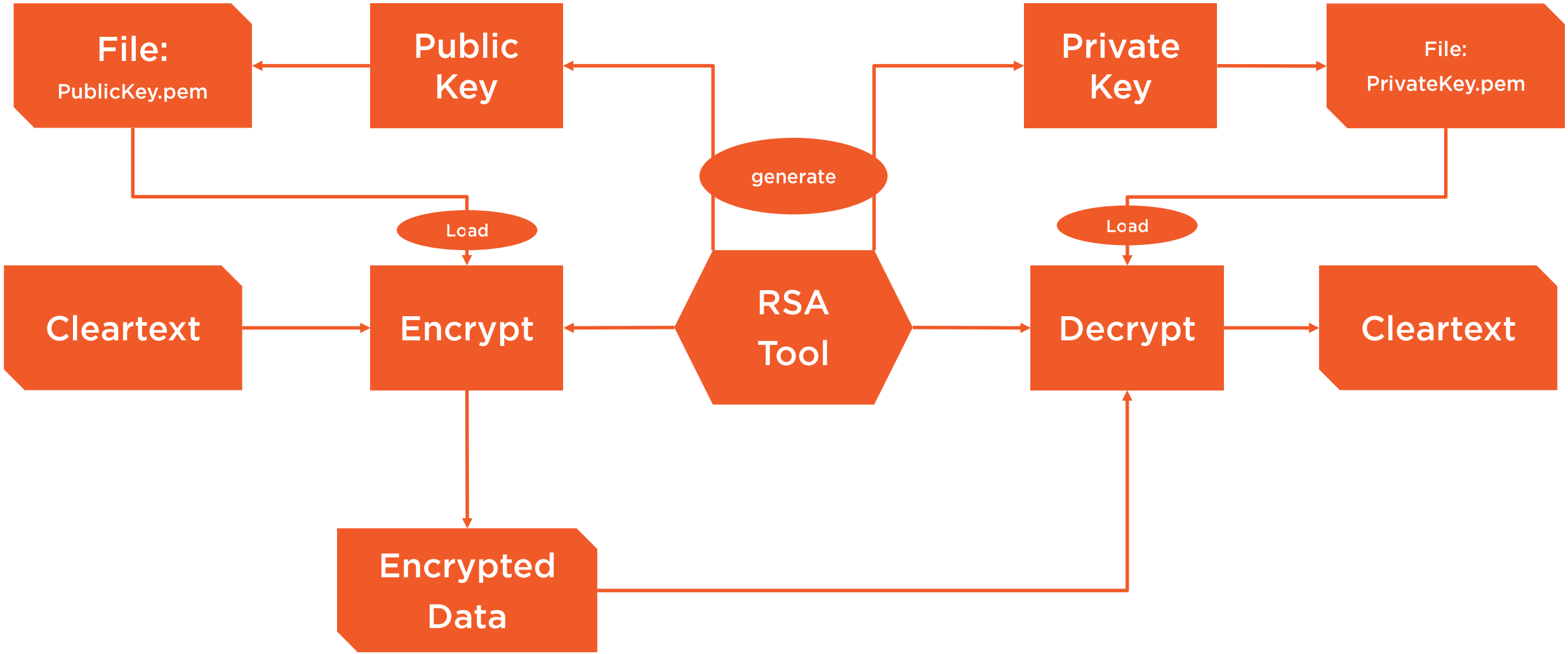
- Cannot share
- It's secret
- Decrypt data

Asymmetric Encryption

- Slow
- RSA – 2048,4096 bits
- ECC (Elliptic Curve Cryptography)

RSA In Python

RSA

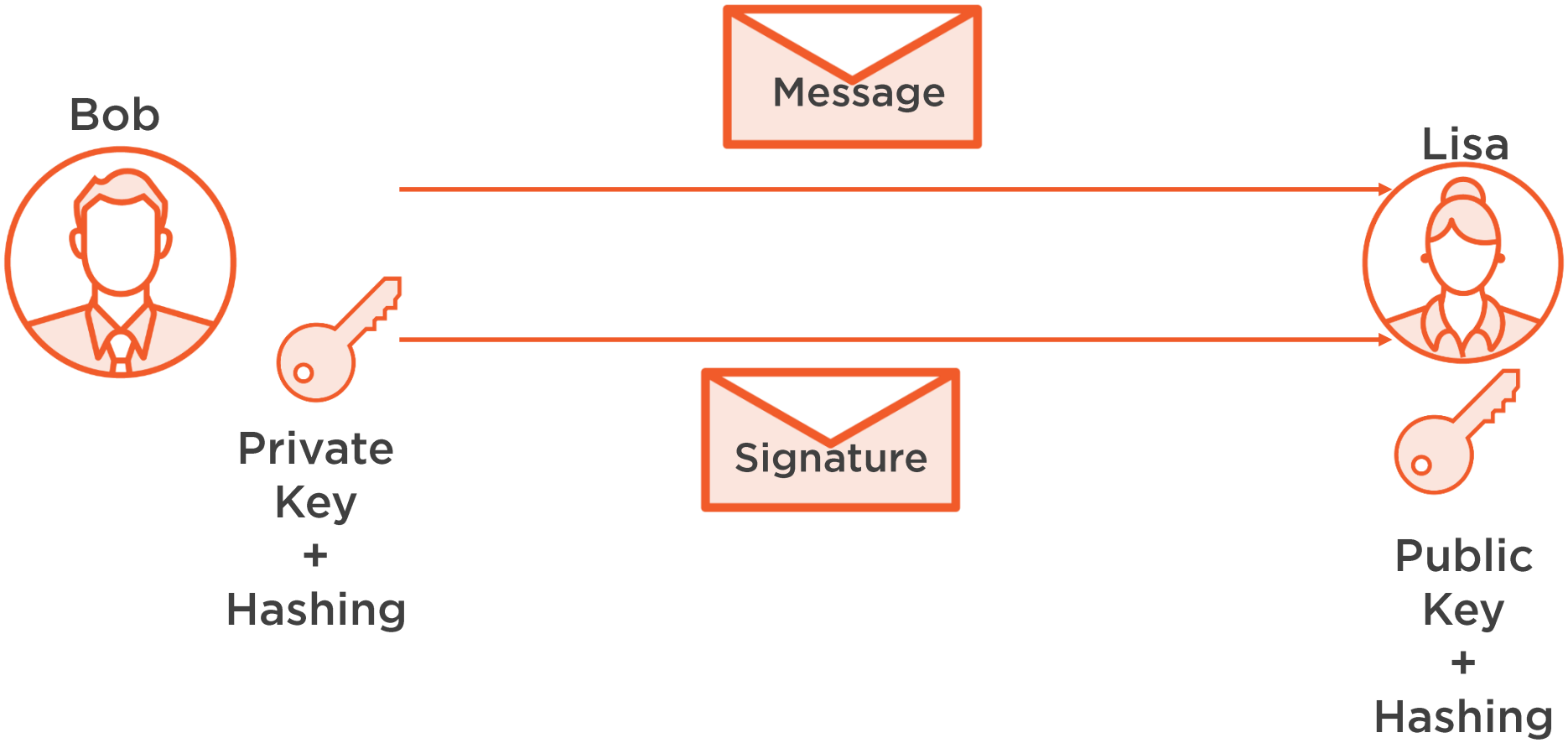

File:
PublicKey.pem
Public
Key
Private
Key
File:
PrivateKey.pem
generate
Load
Load
Cleartext
Encrypt
RSA
Tool
Decrypt
Cleartext
Encrypted
Data

Digital Signature In Python

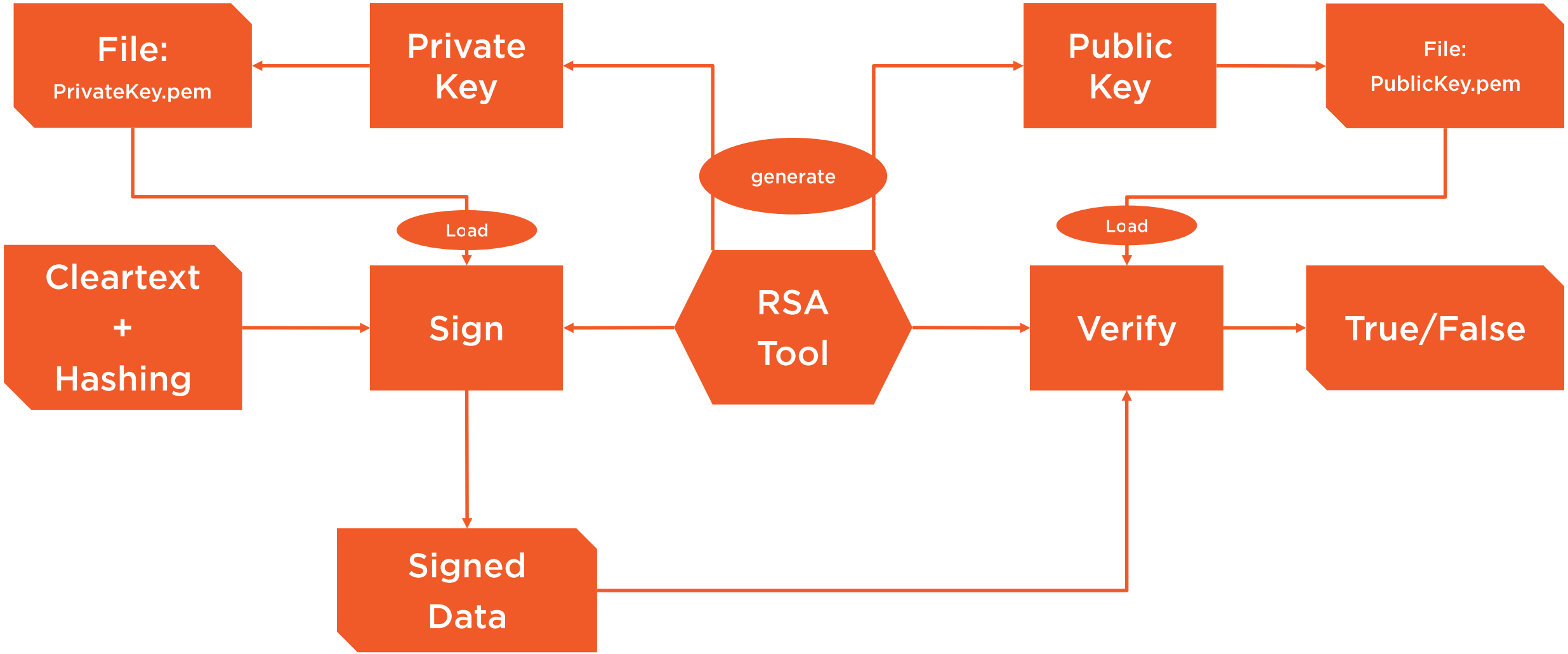
Digital Signature

- **Authentication**
- **Non-repudiation**
- **Integrity**

Example


Bob
Message
Lisa
Private
Key
+
Hashing
Signature
Public
Key
+
Hashing

Digital Signature In RSA



Summary

Asymmetric Encryption

- Overview
  - Public / Private keys.
  - RSA → 2048, 4096 bits
- RSA in Python
- Digital Signature in Python