Public key cryptology, RSA, ElGamal, Elliptic Curve

Jason Pearson and

November 23, 2015

Key Terms

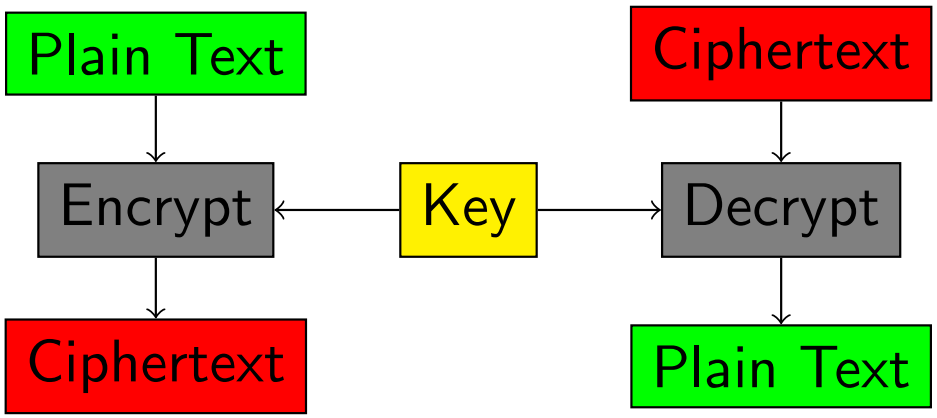
Plain text: typically a simple text such as this line
Cipher text: a message after it has been encrypted

Types of Encryption

Symmetric Encryption
Asymmetric Encryption
Hashing
Hybrid Encryption

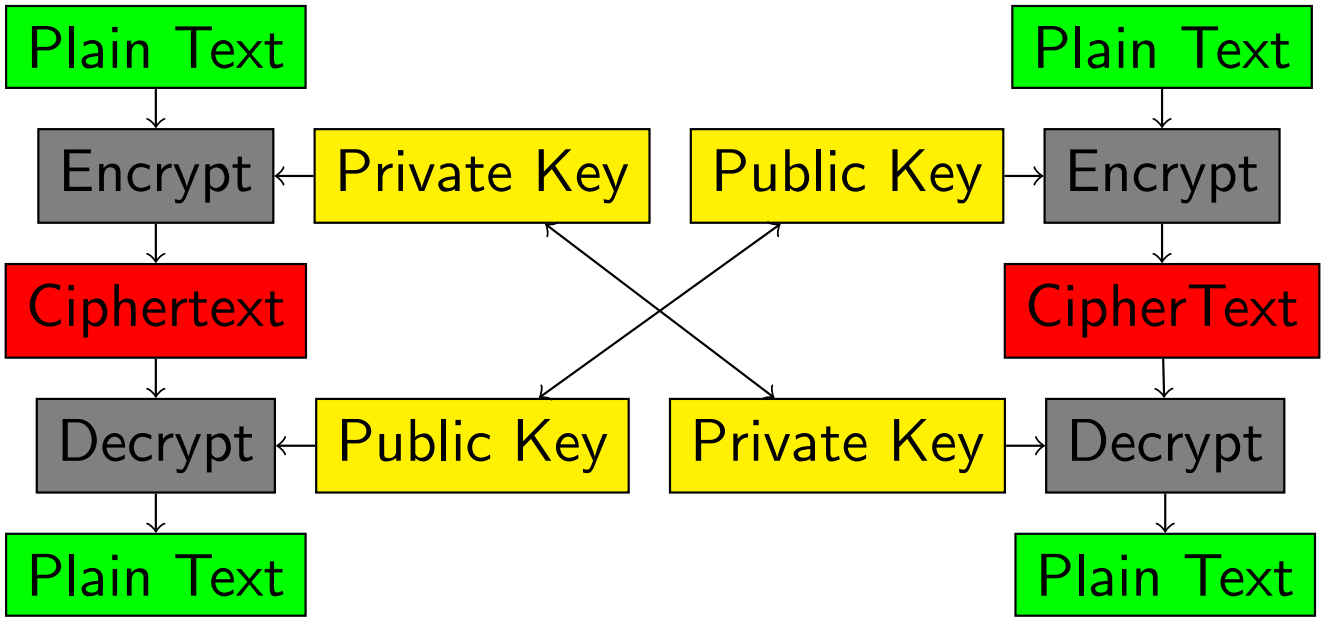
Symmetric Encryption

Encryption and Decryption use the same key



Asymmmetric Encryption

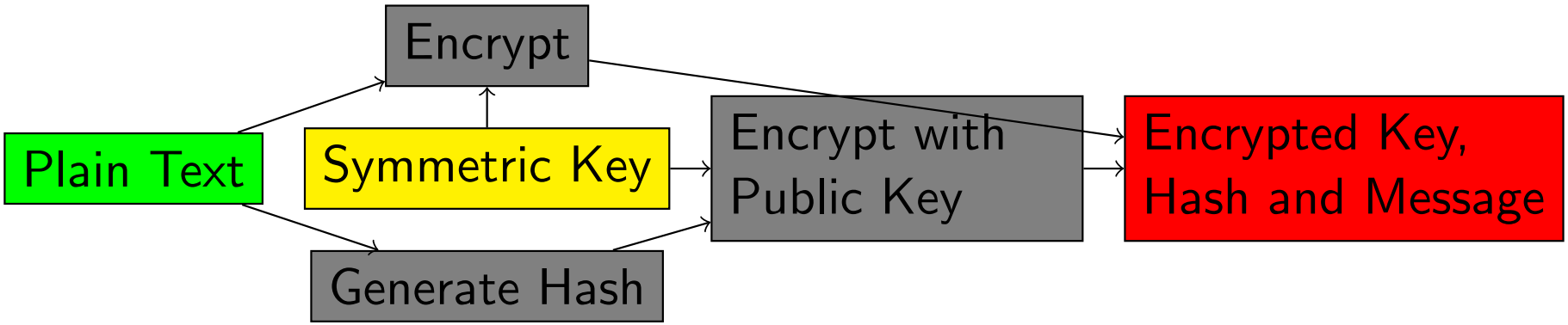
Public key and private key pair
Public key is used to encrypt a message
Private key is used to decrypt a message
Creating the key tends to be computationally expensive



Hashing

Hybrid Encryption

Uses ideas from symmetric and asymmetric encryption methods
An asymmetric cryptosystem is used for key encapsulation and an symmetric system is used for data encapsulation



Cyclic Groups

RSA Cryptosystem

ElGamal Cryptosystem

Elliptic Curve

Conclusion

Demo!

References

http://caislab.kaist.ac.kr/lecture/2010/spring/cs548/basic/B02.pdf