Public key cryptology, RSA, ElGamal, Elliptic Curve

Jason Pearson and

November 23, 2015

Key Terms

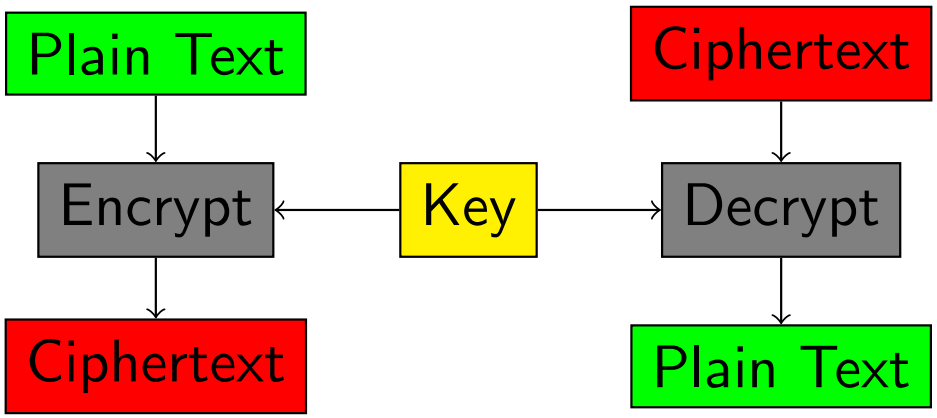
Plain text: typically a simple text such as this line
Cipher text: a message after it has been encrypted
Prime Number: a whole number that can only be divided evenly by one and itself also it is greater than one

Types of Encryption

Symmetric Encryption
Asymmetric Encryption
Hashing
Hybrid Encryption

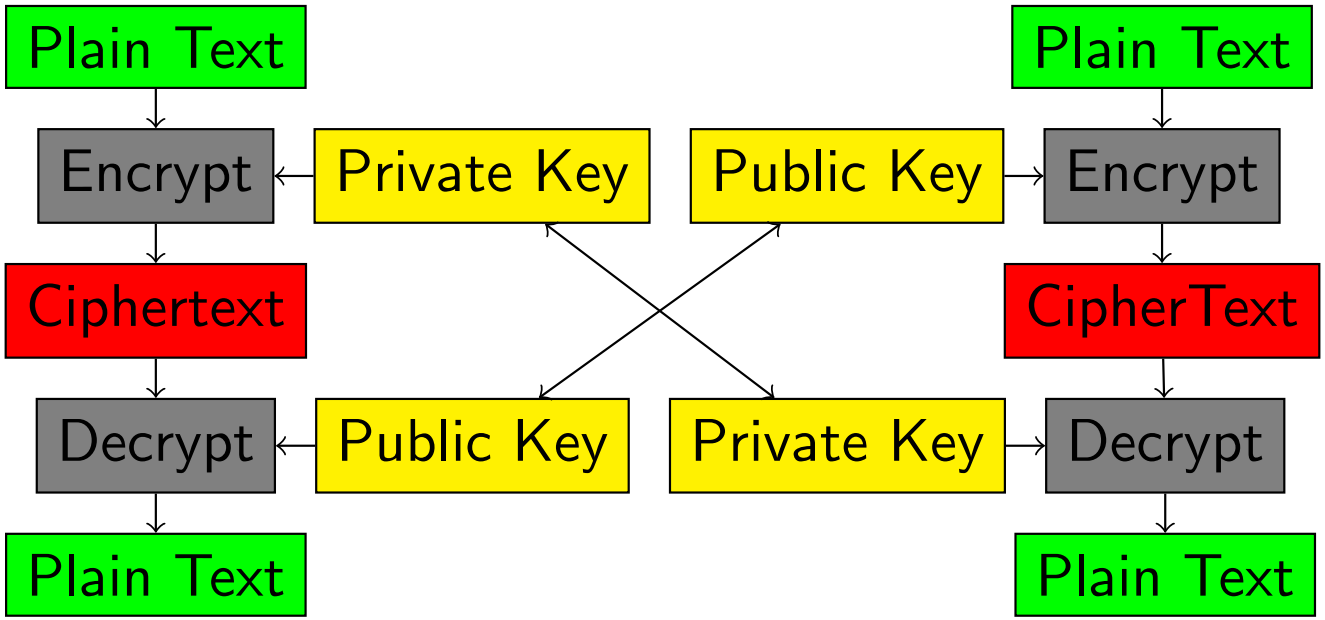
Symmetric Encryption

Encryption and Decryption use the same key



Asymmmetric Encryption

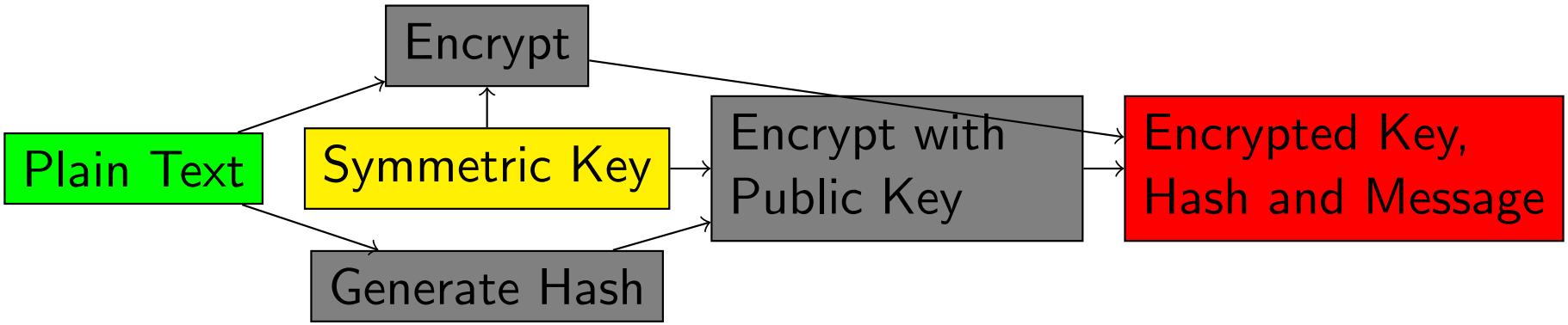
Public key and private key pair
Public key is used to encrypt a message
Private key is used to decrypt a message
Creating the key tends to be computationally expensive



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

Padding Schemes

RSA Cryptosystem

First designed in 1973 and declassified in 1997.
Named after its founders Ron Rivest, Adi Shamir and Leonar Adleman
Uses large prime numbers to create a private and public key
Security arises from the presumed difficulty of factoring large prime numbers

Background Mathmatics

NOT SURE IF I WANNA SPEND TIME ON BACKGROUND MATH WILL DETERMINE AFTER SOME DRY RUNS

The Set Of Integers Modulo P

Integer Remainder After Dividing

Multiplicative Inverse And The Greatest Common Divisor

Prime Numbers

Euler's Totient

RSA Generating Public and Private Keys

Generate Two Large Prime Numbers
Compute n
Compute Euler's Totient Function
Create Public Key
Create Private Key

Generating Large Prime Numbers

Generate two large prime numbers.
Typically uses AKS testing for prime numbers
These two values we will call p and q
$p = 991$
$q = 821$

Computing n and Euler's Totient

We calculate n = p * q
We then can determine Euler's totient value by using the following equation.
$\phi(n) = \phi(p)\phi(q) = (p-1)(q-1) = n - (p+q-1)$
So we have n = 991 * 821 = 813611
And for $\phi(n) = 81180$

Create Public and Private Keys

To create a public key we pick an arbitrary number e between $1 < e < \phi(n)$ for example we will use e $= 7423$
To create a private key we need to find the modular multiplicative inverse of e.
This is commonly done using the Extended Euclidean Algorithm.

$d \equiv e^{-1} \pmod{(\phi(n))}$
This makes our value of d $= 788287$

ElGamal Cryptosystem

Elliptic Curve

Conclusion

References

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