Public Key Cryptography

What is Cryptography

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.

(Kaspersky)

Type of Cryptography

Symmetric Key Cryptography

Fast

Key Exchange is risky

Asymmetric Key Cryptography (Public Key Cryptography)

► Slow

Key Exchange is not risky

Public Key Cryptography Use Cases

- Digital Signature
- Key Exchange
- ► Blockchain
- Public Key Infrastructure(PKI)

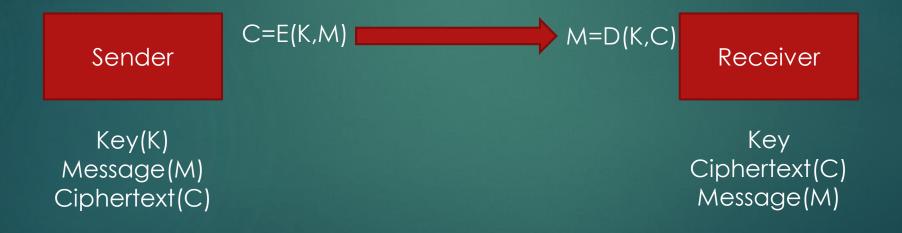
Symmetric Key Cryptography

Sender

Key Message Receiver

Key

Symmetric Key Cryptography



Public Key Cryptography

Sender

Public Key(Reciver)

Receiver

Public Key(Receiver) Private Key(Receiver)

Public Key Cryptography



RSA (Rivest– Shamir–Adleman)

Phases of RSA

Generating Keys

Encryption and Decryption

Generating Keys

- 1. Choose two distinct prime numbers 'p' and 'q'
- 2. Compute 'n = p * q'
- 3. Compute Euler's Totient $\varphi(n)$

 $\varphi(n) = |\{k: 1 \le k \le n, gcd(n,k) = 1\}|$

For numbers that multiplication of two relatively prime number like n ;

 $\phi(n) = p^*q - p - q + 1$

= (p-1)*(q-1)

Example: $n=3*5=15 \quad \varphi(15) = 15-5-3+1=8$

3, 6, 9,12,15 and 5,10,15

 $k = \{1, 2, 4, 7, 8, 11, 13, 14\}$

Generating Keys

- 4. Choose a public exponent e (Fermat Primes) $(10001)_2 = 65537$ e < $\varphi(n)$ and gcd(e, $\varphi(n)$)=1
- 5. Compute a private exponent d (Extended Euclidean Algorith) ed = 1 (mod $\varphi(n)$)



Private Key d (private exponent) p, q, φ(n), n

Encryption and Decryption

- 1. Sender takes public key of receiver (n, e)
- 2. Sender encrypts message
 - 0 < m < n
 - $c = E(m) = m^e \pmod{n}$
- 3. Receiver receives ciphertext
- 4. Receiver decrypts ciphertext $m = D(c) = c^d \pmod{n} = m^{ed} \pmod{n}$

Proof of Decryption Step

- This proof works only when <u>gcd(m, n) = 1</u>
- ▶ D(c) = m^{ed} (mod n)
 - ► $ed \equiv 1 \pmod{\varphi(n)}$
 - $ed = 1 + k * \phi(n)$
- ► $D(c) = m^{(1 + k * \phi(n))} \pmod{n}$
- ► $D(c) = m * m^{(k * \phi(n))} \pmod{n}$
 - $m^{\varphi(n)} \equiv 1 \pmod{n}$ (Euler-Fermat Theorem)
- D(c) = m * 1^k (mod n)
- ▶ D(c) = m

References

- https://www.kaspersky.com/resource-center/definitions/what-iscryptography
- https://blog.keyfactor.com/symmetric-vs-asymmetric-encryption
- https://www.di-mgt.com.au/rsa_theory.html
- https://www.youtube.com/watch?v=reH9zrGcXXM&ab_channel=Pr ofessorMacauley