THE EVOLUTION OF ASYMMETRIC KEY CRYPTOGRAPHY

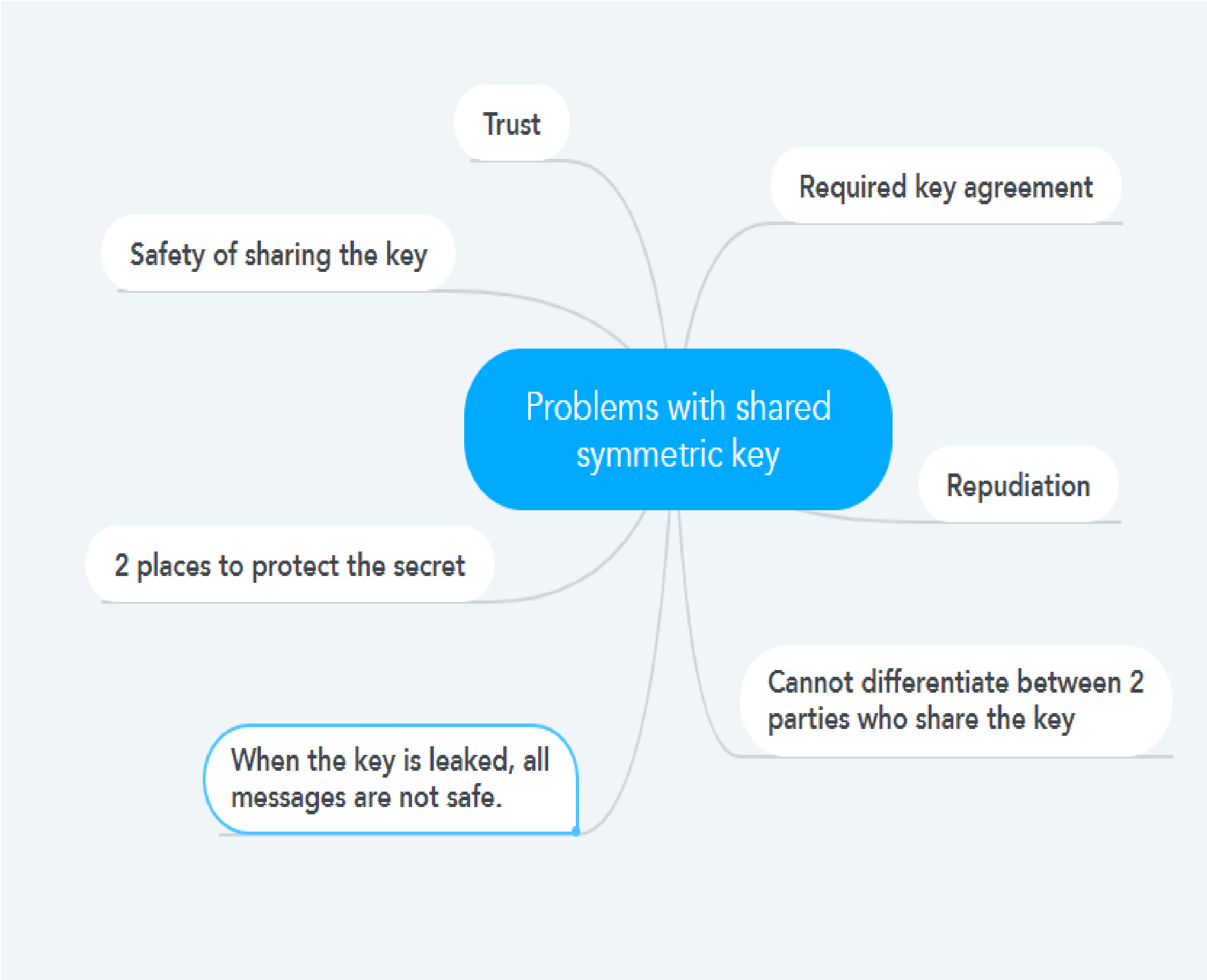
Tidarat Thanapakpawin

THE RISE OF ASYMMETRIC CRYPTOGRAPHY

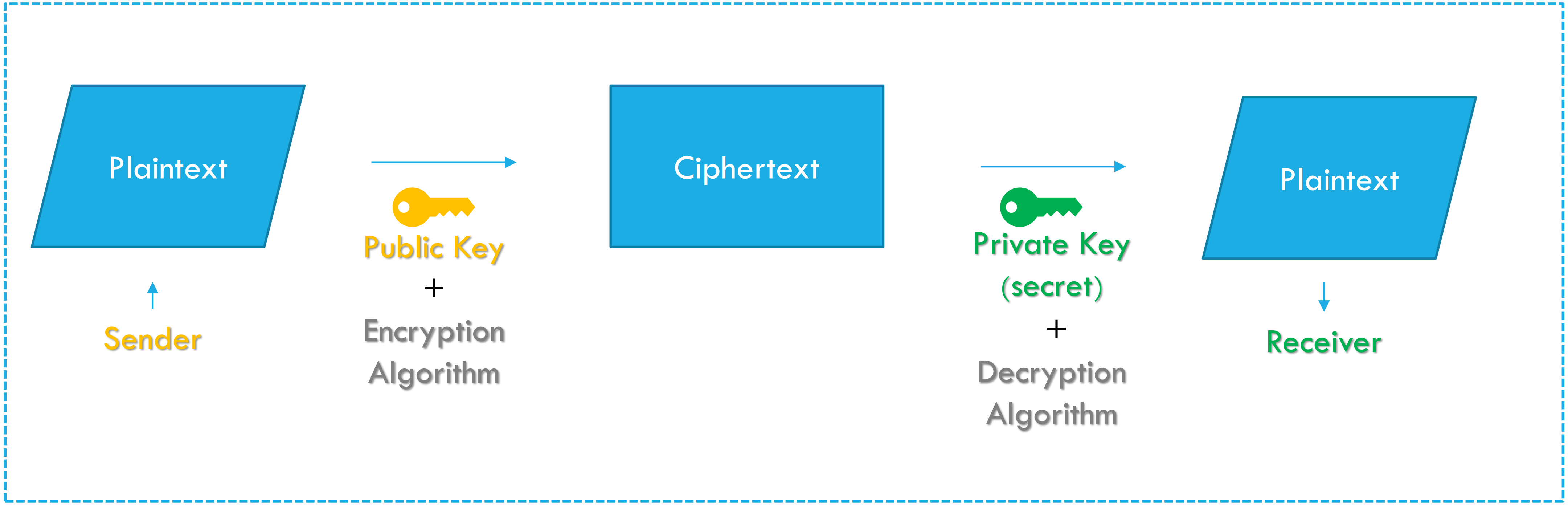
To solve the problem of shared symmetric key, Asymmetric cryptography was invented. This method replace a single shared key with a pair of keys, which are:

- mathematically related

- composed of a public key (can be shared to anyone/ senders) and a private key (known only to the owner/ recipient).



HOW THE ASYMMETRIC CRYPTOGRAPHY WORKS



ASYMMETRIC KEY

Algorithm

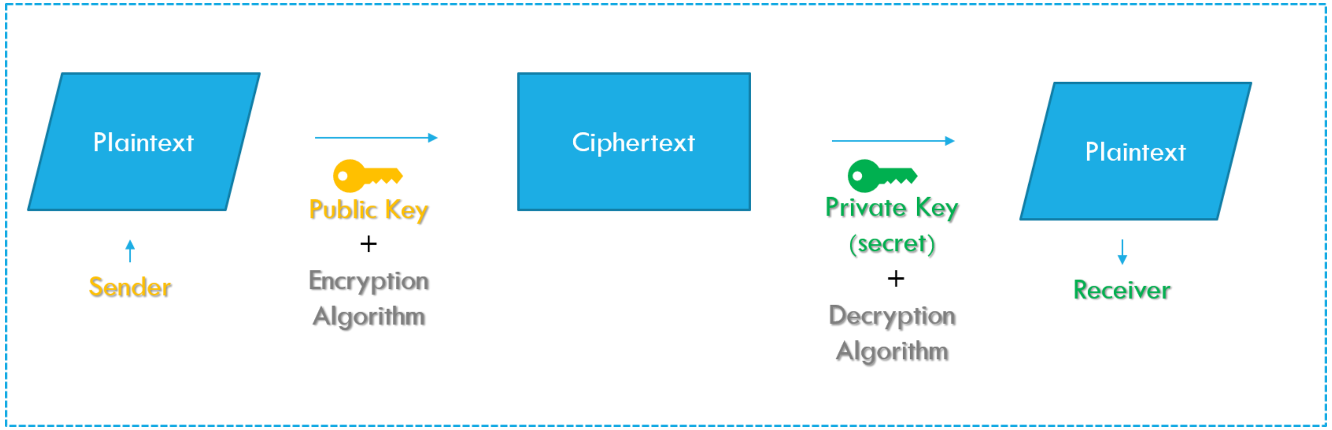
RSA PUBLIC KEY CRYPTOGRAPHY

[Rivest, Shamir, and Adleman]

- The public key and private key are inverse of each other.

- Using private key to "encrypt" the message means anyone with public key can "read" the message. This is call "Digital Signature"

- Digital Signature is used to ensure that the massage really come from the sender that knows the private key.



The Public and Private Key could be used interchangeable. This means both could be used to encrypt or decrypt the message while another is used to do the other function.

1. Two large prime numbers "p" and "q" are chosen.
2. N = p * q
3. $\phi(N)$ = (p-1)*(q-1)
4. Randomly choose public key "e"
5. Find private key d. d must satisfy

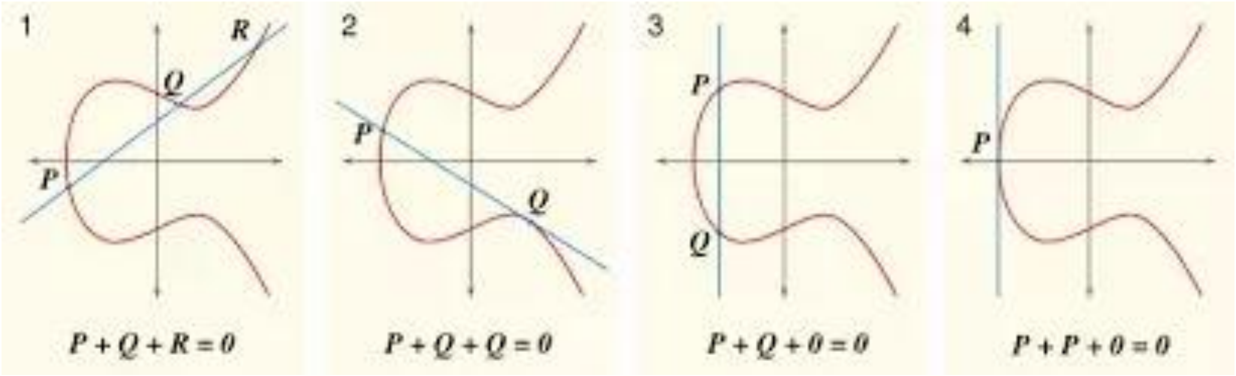
$$e.d = 1 \mod \phi(N)$$

RSA

- The strength of RSA depends on how difficulty it is to factor N into p and q. Therefore, N needs to be a very large number.

- The drawback is that RSA is much slower than symmetric cryptosystems due to the size of N.

ELLIPTICAL CURVE CRYPTOGRAPHY (ECC)



An elliptic curve is the set of points that satisfy a specific mathematical equation.

- Instead of increasing the size of N, using a more difficult mathematical problem is an alternative.
- ECC is based on the algebraic structure of "elliptic curves" over finite fields.
- ECC use shorter key to provide equal security level with RSA.
- Website use ECC to secure customers' hypertext transfer protocol connection.
- It also could be use to encrypt "time stamp"

THE COMPARISON BETWEEN SYMMETRIC & ASYMMETRIC ENCRYPTIONS

	SYMMETRIC	ASYMMETRIC
Computational requirements	Faster	
Ease of distribution (securely)		Easier

Hybrid Cryptosystems employ the advantages of both systems to provide better solution for modern file transfer systems. A secret file (especially the large one) will be encrypted by “symmetric cryptosystem” while using “asymmetric cryptosystem” to encrypt the symmetric key.

HYBRID CRYPTOSYSTEMS

File transfer

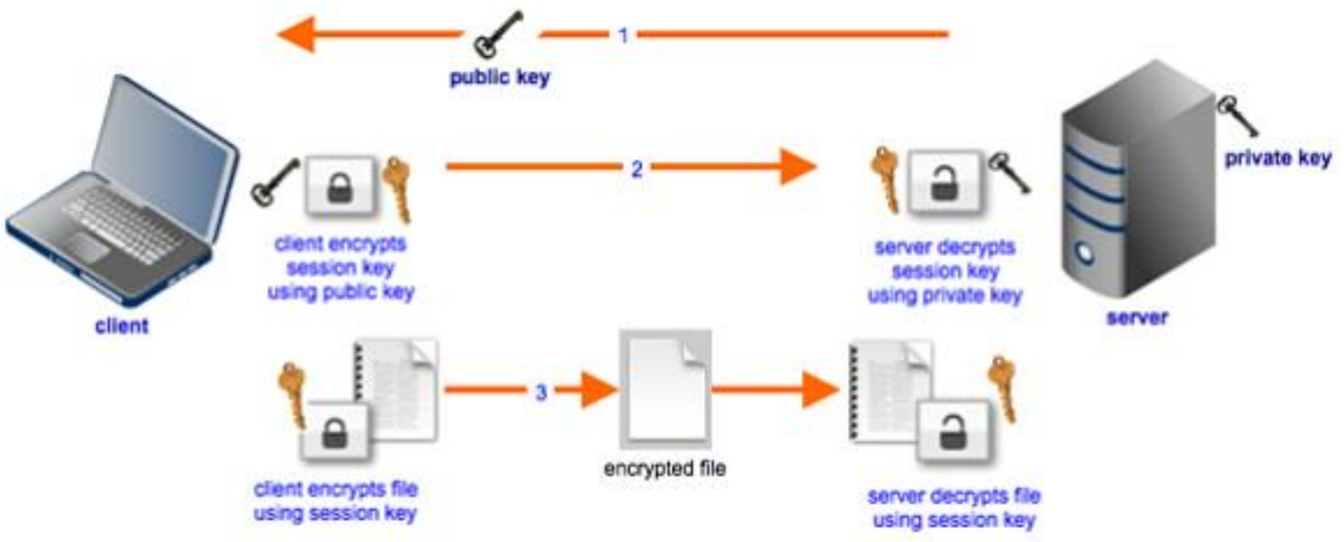
HYBRID CRYPTOSYSTEMS

- SSL (used in FTPS and HTTPS)

  <website>

- SSH (used in SFTP)
- PGP or GPG <Email>
- Bitcoin <wallet>

1. Server sends “public key” to client
2. Client generates a “session key”
3. Client encrypts “a copy of session key” using the “public key” and send that to the server.
4. Server receives its “copy of session key” and both of them use that “session key” to encrypt/ decrypt “files exchanged within that session.



DIFFIE-HELLMANN KEY EXCHANGE

(EXPONENTIAL KEY EXCHANGE)

- Use "public key" techniques to allow the exchange of a private encryption key
- Both parties agreed on the prime number (p) and primitive root (g)
- Sender selects "private key" (s)
- Receiver selects "private key" (r)
- (s) and (r) must be less the prime number (p)
- Public Key for sender (Ps) = g^s mod p
- Public Key for receiver (Rs) = g^r mod p

If p = 17, g = 3, s= 15, r= 13

We want to find "secret" (symmetric key) "
Given symmetric key = k

Ps = g^s mod p = 3^15 mod 17 = 6

Rs = g^r mod p = 3^13 mod 17 = 12

S sends Ps (44) to R

k = (Ps)^r mod p = 6^13 mod 17 = 10

R sends Rs (56) to S

k' = (Rs)^s mod p = 12^15 mod 17 = 10

APPLICATION OF ASYSMETRIC KEY

REFERENCE

1. Evolution of Cryptography by Mohd Zaid Waquiyuddin Mohd Zulkifli, January 17, 2007.

2. https://www.sciencedirect.com/topics/computer-science/diffie-hellman