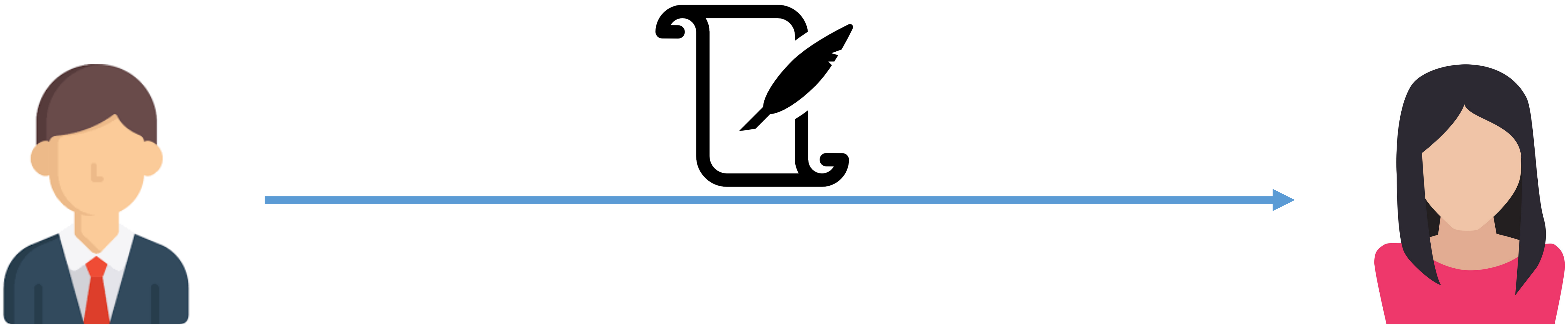
Public Key and RSA Algorithm

Shusen Wang

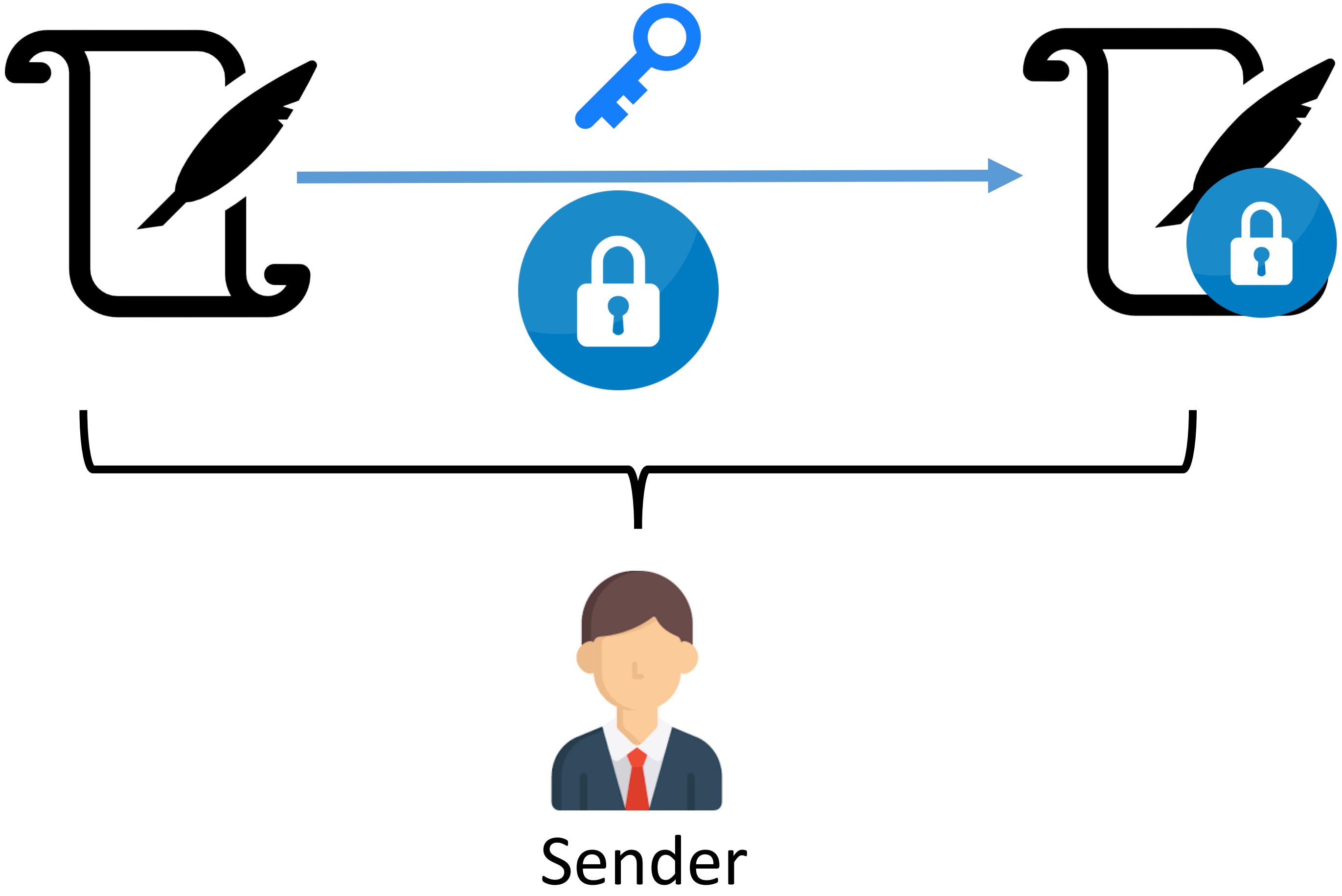
Sending Messages



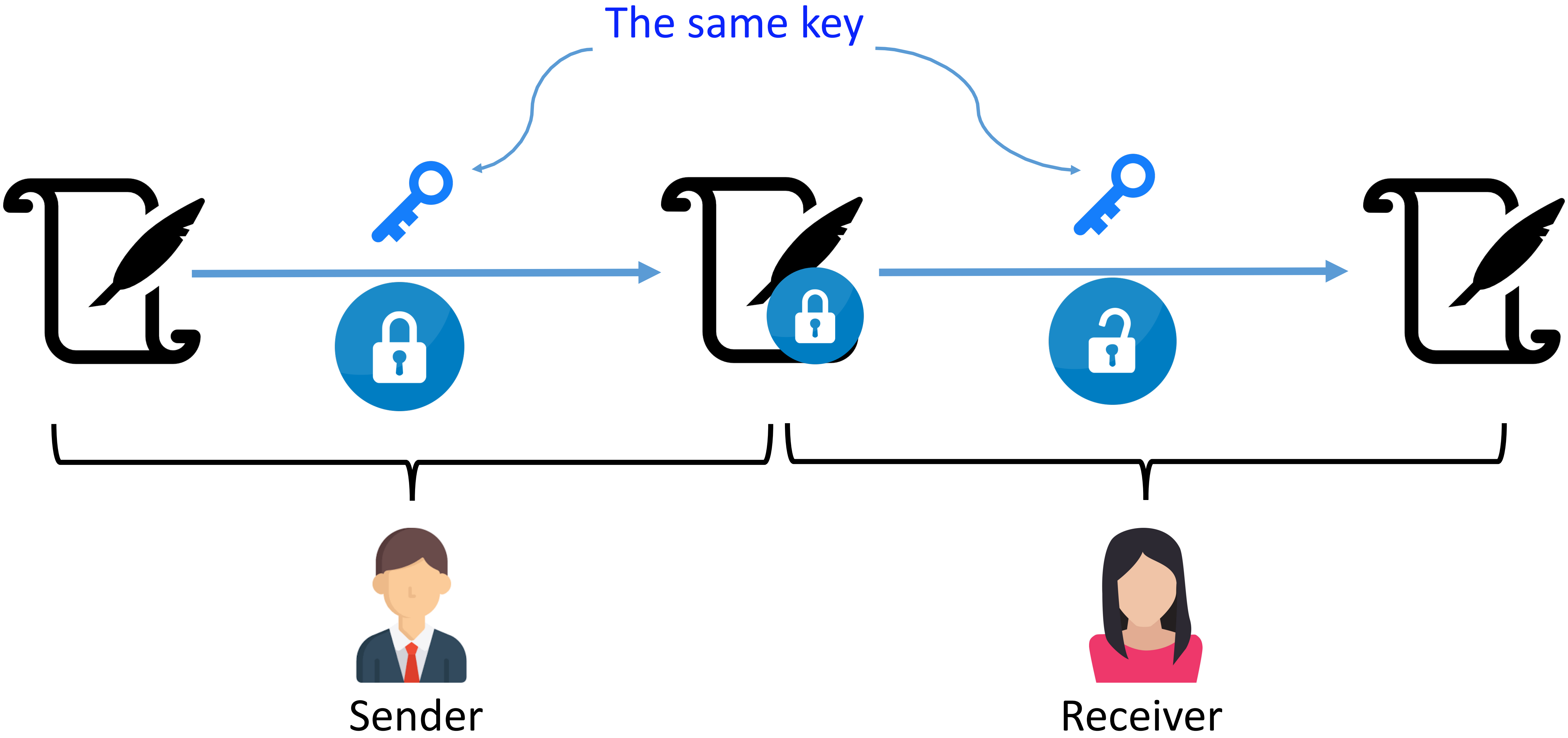
Sender

Receiver

Symmetric Encryption

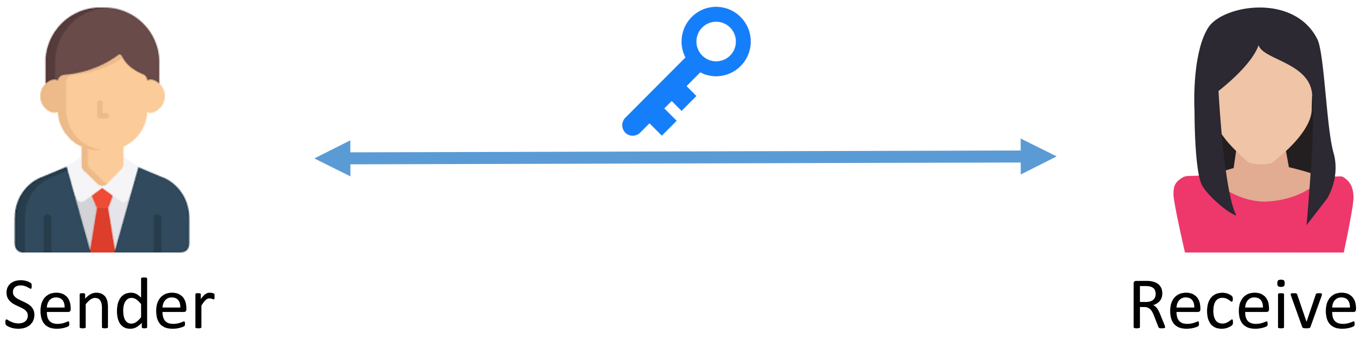


Symmetric Encryption



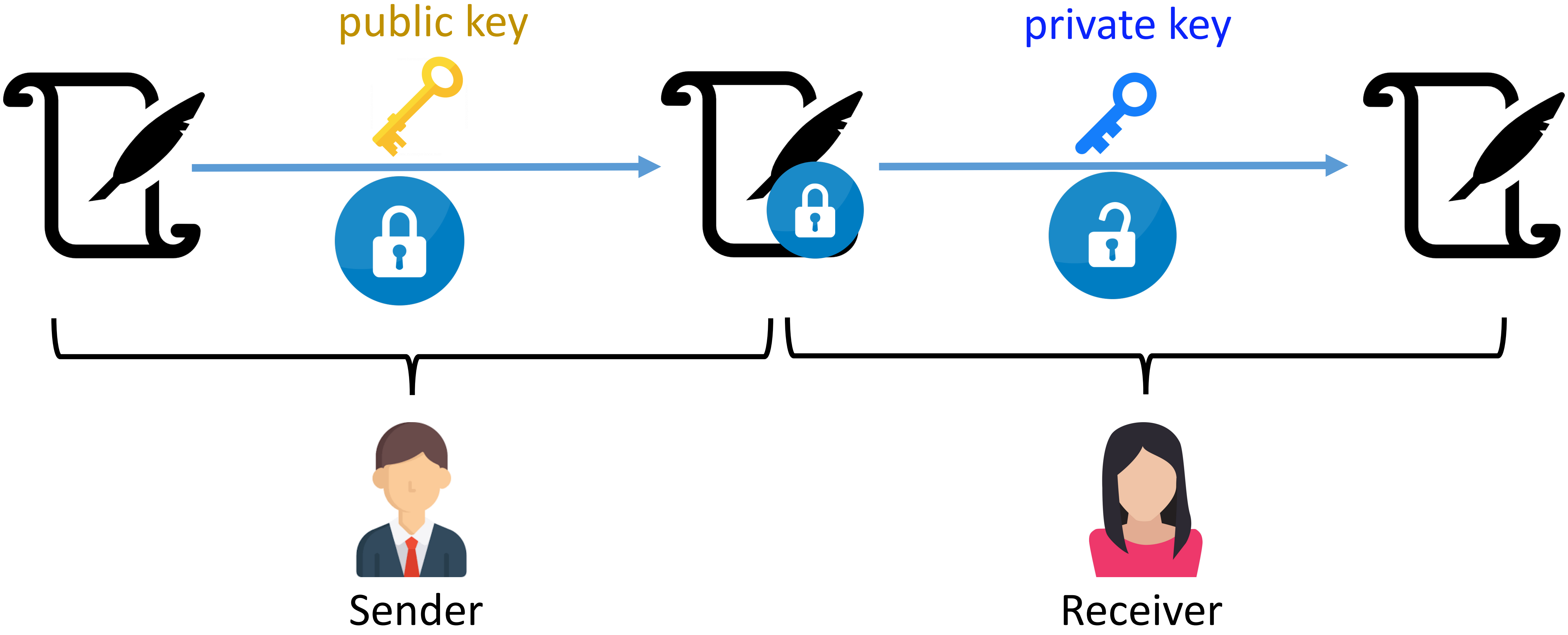
Symmetric Encryption

- The sender and receiver use the same secret key to encrypt and decrypt information.
- The sender and receiver have to agree upon the key.

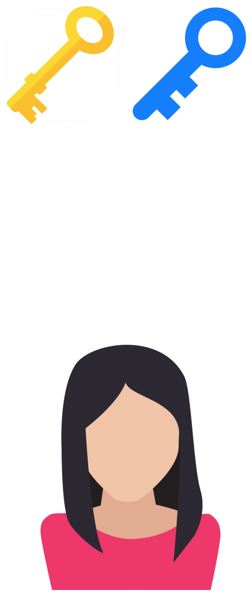


Difficulty: How to exchange the secret key safely?

Asymmetric Encryption

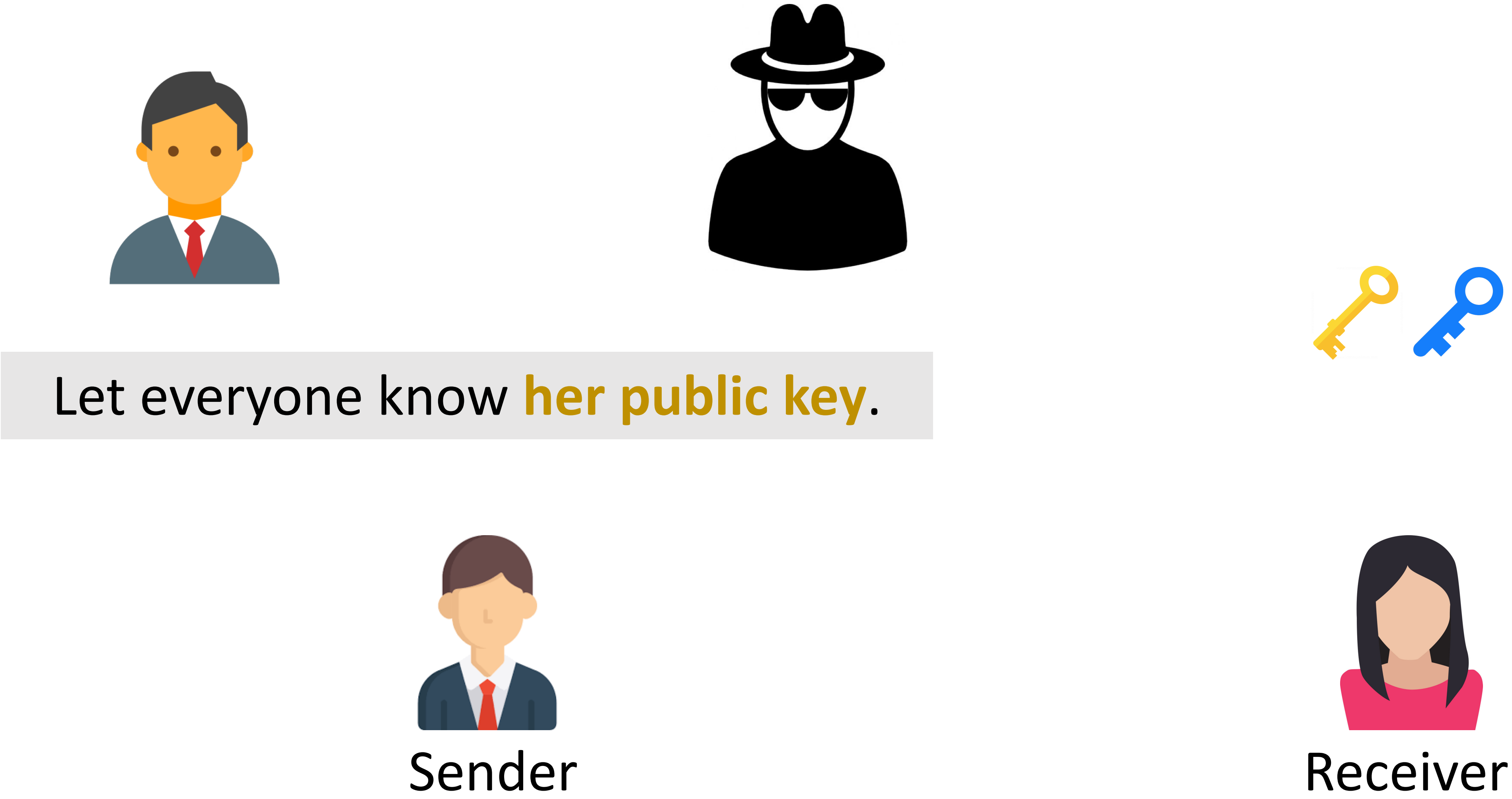


Asymmetric Encryption



Receiver

Asymmetric Encryption

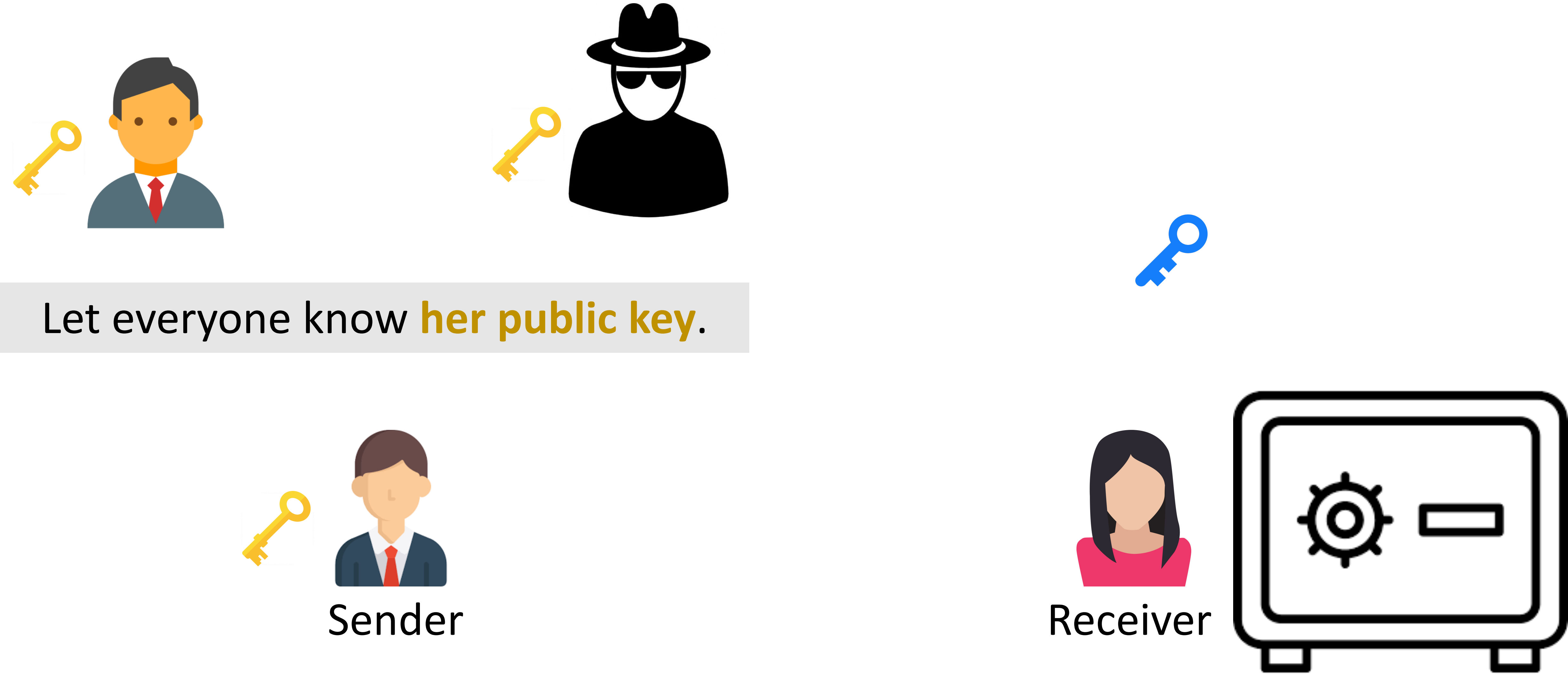


Let everyone know **her public key**.

Sender

Receiver

Asymmetric Encryption

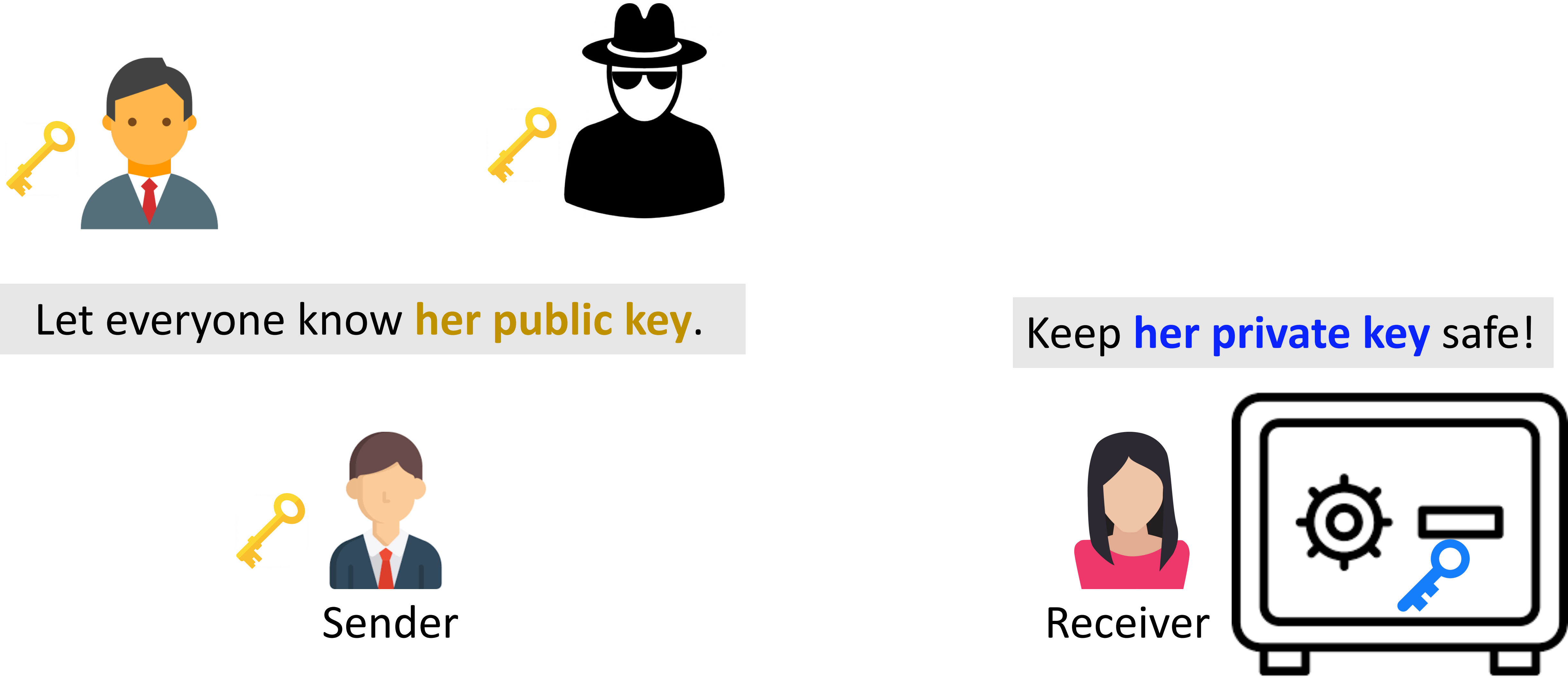


Let everyone know **her public key**.

Sender

Receiver

Asymmetric Encryption



Let everyone know **her public key**.

Keep **her private key** safe!

Sender

Receiver

Properties of Asymmetric Encryption

1. Decryption of an encrypted message gives the original message:

$$D\left(E(\text{messge})\right) = \text{message} \,.$$

Properties of Asymmetric Encryption

1. Decryption of an encrypted message gives the original message:

$$D\big(E(\text{messge})\big) = \text{message}\ .$$

2. E and D are easy to compute.

Properties of Asymmetric Encryption

1. Decryption of an encrypted message gives the original message:

$$D\big(E(\text{messge})\big) = \text{message} \, .$$

2. E and D are easy to compute.

3. Given E, one cannot easily figure out D.

   - Everyone has the public key.

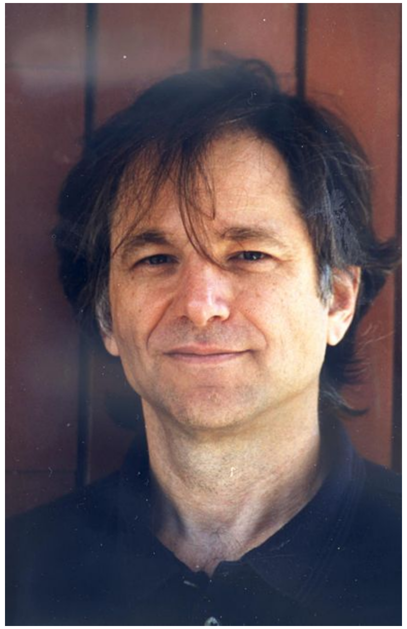
   - They cannot thereby infer the private key.

RSA Algorithm

- RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission.

Ron Rivest

Adi Shamir



Leonard Adleman

Turing Award 2002, for their ingenious contribution for making public-key cryptography useful in practice.

RSA Algorithm

- e, d, n: positive integers satisfying certain properties.
- Public key (e, n).
- Private key (d, n).

RSA Algorithm

- e, d, n: positive integers satisfying certain properties.
- Public key (e, n).
- Private key (d, n).

- M (integer between 0 and $n - 1$): the message.
- Encryption: $E(M) = M^e \bmod n$.
- Decryption: $D(C) = C^d \bmod n$.

RSA Algorithm

- e, d, n: positive integers satisfying certain properties.
- Public key (e, n).
- Private key (d, n).

- M (integer between 0 and $n - 1$): the message.
- Encryption: $E(M) = M^e \bmod n$.
- Decryption: $D(C) = C^d \bmod n$.

Theorem: $D\big(E(M)\big) = M$ for certain e, d, n.

RSA Algorithm: The Math

How to construct e, d, n?

RSA Algorithm: The Math

How to construct e, d, n?

1. Randomly generate large primes p and q.

RSA Algorithm: The Math

How to construct e, d, n?

1. Randomly generate large primes p and q.
2. $n = pq$.
3. $t = (p - 1)(q - 1)$.

RSA Algorithm

How to construct e, d, n?

1. Randomly generate large primes p and q.
2. $n = pq$.
3. $t = (p - 1)(q - 1)$.
4. Find a large integer d such that $gcd(d\ ,\ t) = 1,$ where gcd means greatest common divisor.
5. Find e such that $mod(d * e\ ,\ t) =\ 1.$

Thank You!