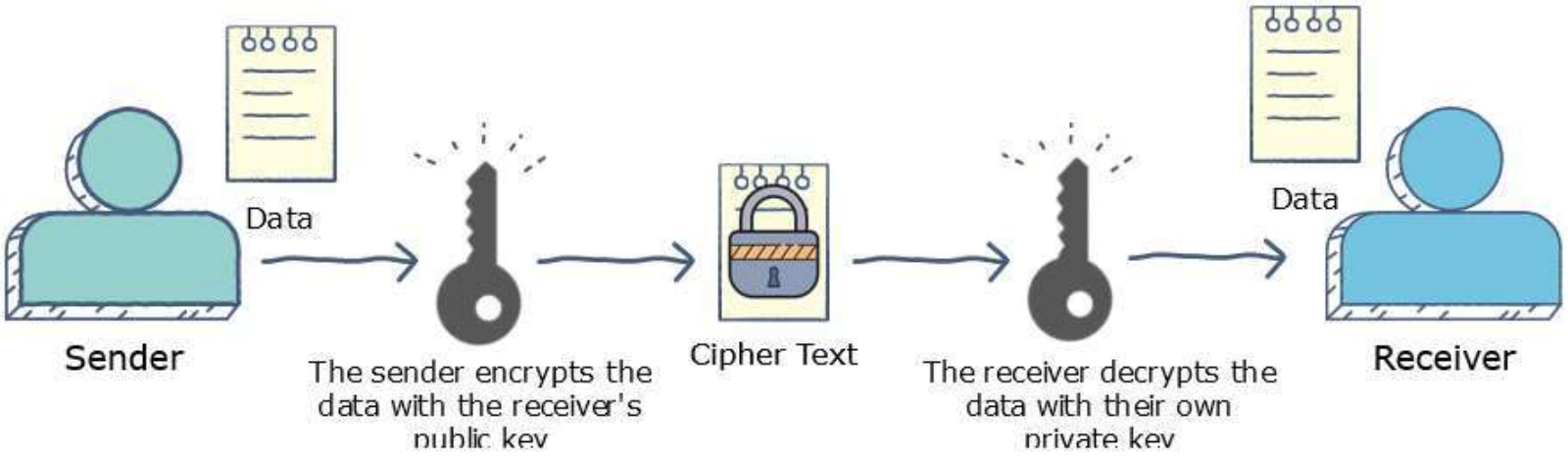
- The **RSA algorithm** is an asymmetric cryptography algorithm; this means that it uses a public key and a private key (i.e two different, mathematically linked keys).
- As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.
- The RSA algorithm is named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman.



STEPS INVOLVED

STEP-1

At sender side,

- Sender encrypts the message using receiver’s public key.
- The public key of receiver is publicly available and known to everyone.
- Encryption converts the message into a cipher text.
- This cipher text can be decrypted only using the receiver’s private key.

STEP-2

- The cipher text is sent to the receiver over the communication channel.

- **Step-03:**

At receiver side,

- Receiver decrypts the cipher text using his private key.
- The private key of the receiver is known only to the receiver.
- Using the public key, it is not possible for anyone to determine the receiver's private key.
- After decryption, cipher text converts back into a readable format.

- **Advantages-**

  - The advantages of public key cryptography are-
  - It is more robust.
  - It is less susceptible to third-party security breach attempts.

- **Disadvantages-**

  - It involves high computational requirements.
  - It is slower than symmetric key cryptography.

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute $\varphi(n) = (p - 1) * (q - 1) = 2 * 10 = 20$
- Choose e such that $1 < e < \varphi(n)$ and e and $\varphi(n)$ are coprime. Let e = 7
- Compute a value for d such that $(d * e) \% \varphi(n) = 1$. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$