***Asymmetric Encryption (Theory + Demo)***

Asymmetric encryption, also called **public-key cryptography**, is a method of encryption that uses **two different keys**:

 **Public Key** → Shared openly and used to encrypt data

 **Private Key** → Kept secret and used to decrypt data..

This ensures that only the owner of the private key can decrypt messages encrypted with the public key. Asymmetric encryption removes the need to share a secret key, which enhances security when communicating over untrusted networks.

**How it Works :**

1. The sender gets the receiver’s **public key**.
2. The sender encrypts the message using the public key.
3. Only the receiver’s **private key** can decrypt it.

**Common Algorithms**

* **RSA (Rivest–Shamir–Adleman)** – One of the most widely used algorithms; relies on the difficulty of factoring large prime numbers; supports encryption and digital signatures.
* **ECC (Elliptic Curve Cryptography)** – Offers strong security with smaller key sizes, improving efficiency.
* **DSA (Digital Signature Algorithm)** – Primarily used for authentication and verifying message integrity.
* **ElGamal** – Used for both encryption and digital signatures; based on discrete logarithms.

***Demo***

import rsa

public\_key,private\_key=rsa.newkeys(1024)

message = "Hello, this is an RSA test!encrypt and decrypt message"

print("Original Message:", message)

encrypted\_message = rsa.encrypt(message.encode(), public\_key)

print("Encrypted Message:", encrypted\_message)

decrypted\_message = rsa.decrypt(encrypted\_message, private\_key).decode()

print("Decrypted Message:", decrypted\_message)

***Output***

Original Message: Hello, this is an RSA test!encrypt and decrypt message

Encrypted Message: b'\x04\x05\x88b^\x19\x7f\xa5,\xfai\xca\x1b\x06F\xe34\x89\xa9\xf9\x8e\x1c>\xc8\xe2\xc3\xdfe\xe9+rD\xb8\xf7\xd6\xef\xbc3c\xfe\x10\x8d\xe7\xd6f\x15Ase\xa0\xe5\x7fo\xedt\x96\xb7\xce\xe8\xb7\x91\xd0\x04\xc9\x03b\x15U\xae"\xa6\xac\xd8\xab\xbb\x18\xee\x15O\xf4\xcf\xfc\xf0\x04\x8d\x98\xc7!\xfe\xdc\xb73\x11\xace\t\xd73\x1f\xb2\xecO\xf0\xcd\xffA\xd4\xd5tr\x00\xf0\xb4\x0f=\xfb=\xbc\xd7j|\x92\xf5\xf0\xdam&,'

Decrypted Message: Hello, this is an RSA test!encrypt and decrypt message

This demo shows how RSA ensures secure communication by using a public key for encryption and a private key for decryption.