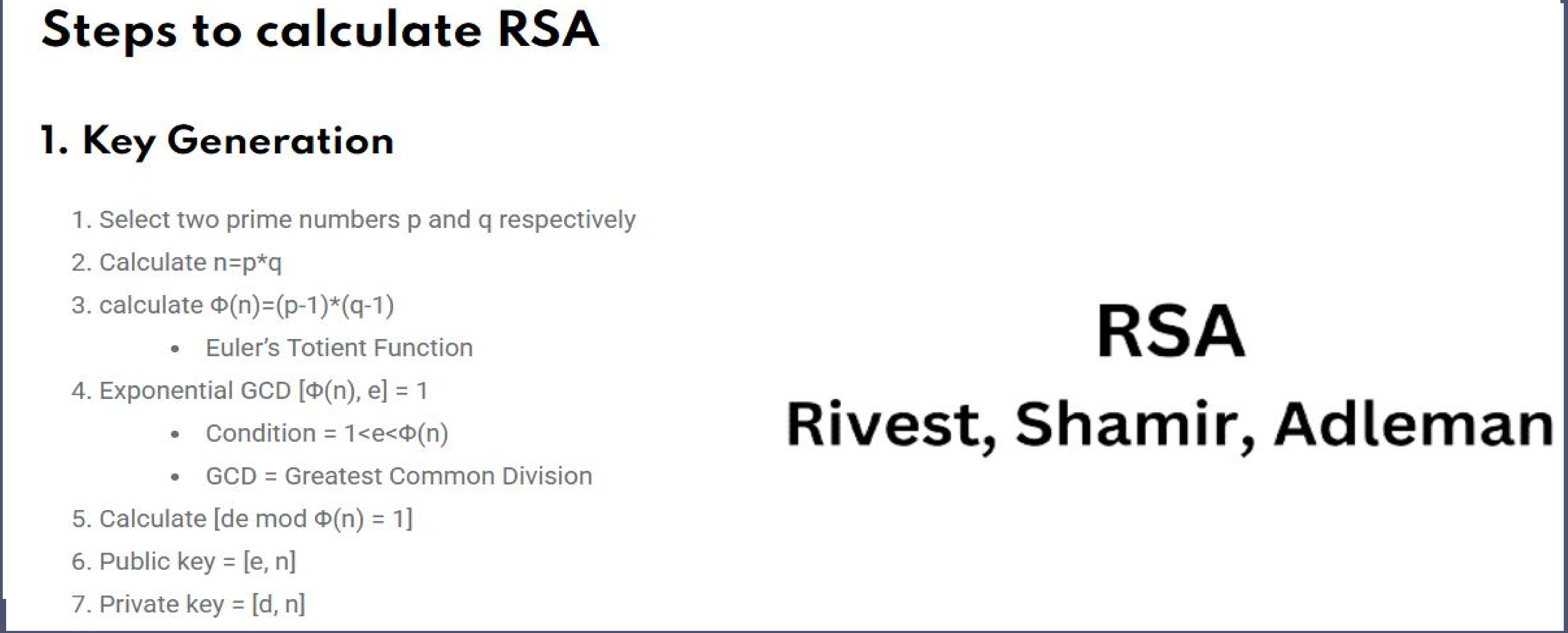
UNIT-3

RSA Algorithm

RSA (Rivest, Shamir, Adleman) algorithm was first described in 1977. It is an asymmetric cryptography algorithm with private and public keys in it. The public key is used for encryption and the private key is used for decryption.



Steps to calculate RSA

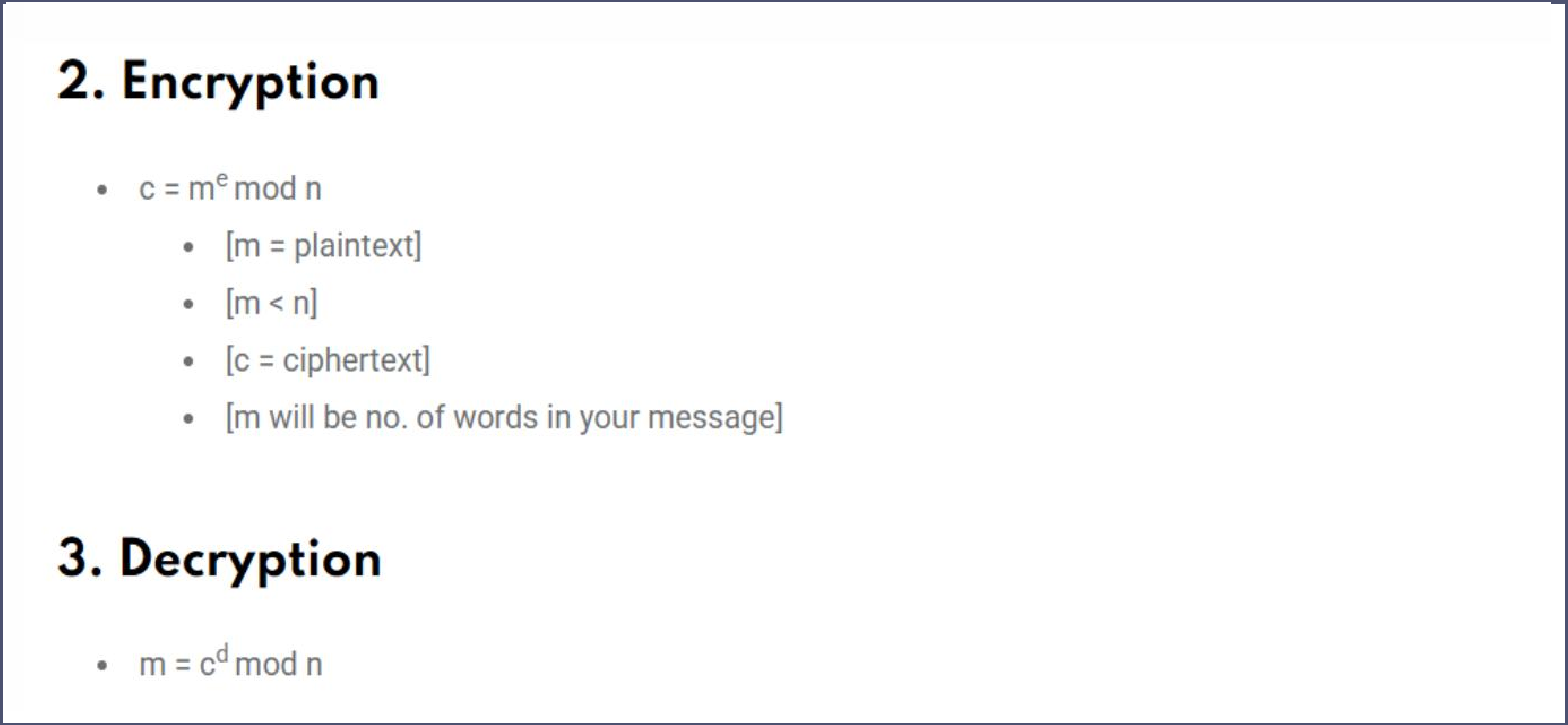
1. Key Generation

1. Select two prime numbers p and q respectively
2. Calculate n=p*q
3. calculate Φ(n)=(p-1)*(q-1)
   - Euler's Totient Function
4. Exponential GCD [Φ(n), e] = 1
   - Condition = 1<e<Φ(n)
   - GCD = Greatest Common Division
5. Calculate [de mod Φ(n) = 1]
6. Public key = [e, n]
7. Private key = [d, n]

RSA

Rivest, Shamir, Adleman

RSA Algorithm



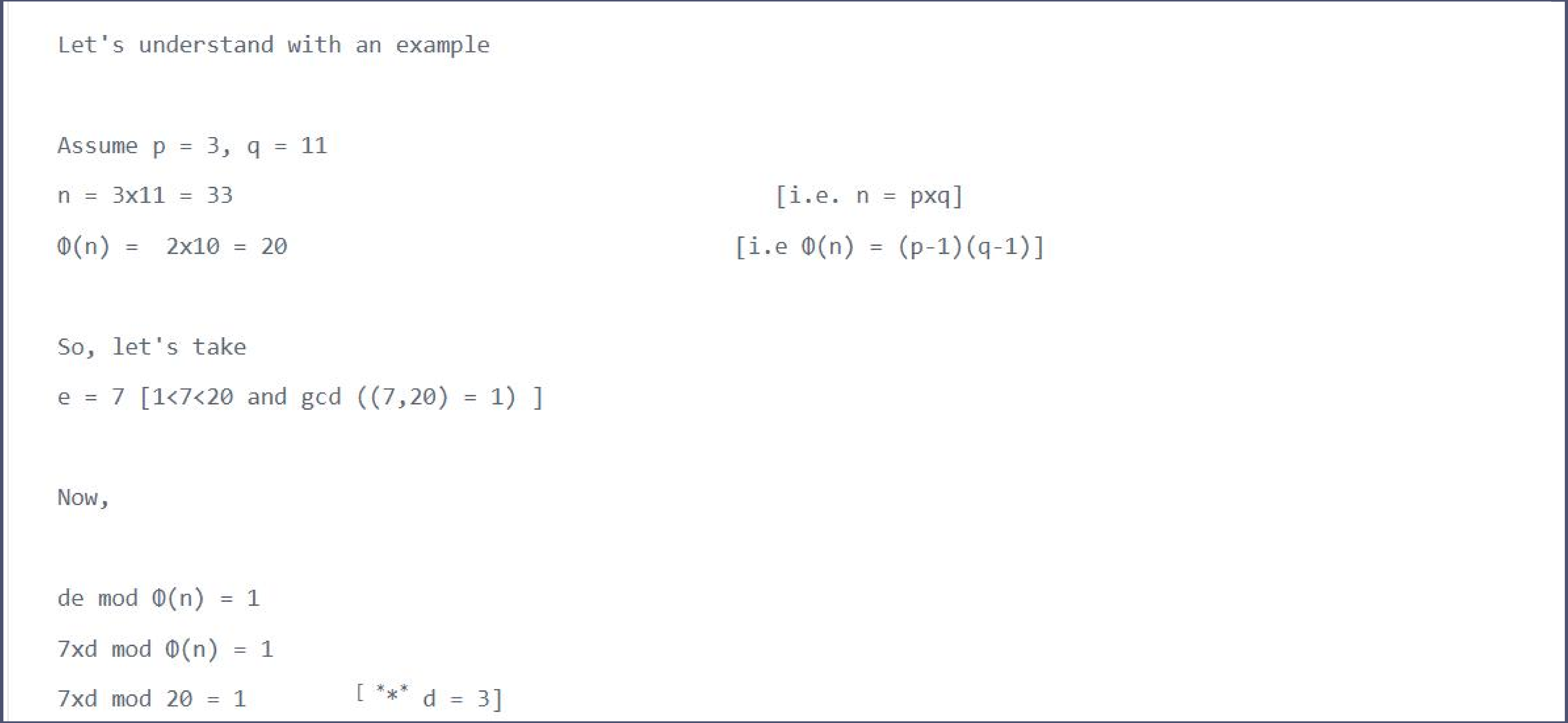
2. Encryption

- $c = m^e \bmod n$
  - [m = plaintext]
  - [m < n]
  - [c = ciphertext]
  - [m will be no. of words in your message]

3. Decryption

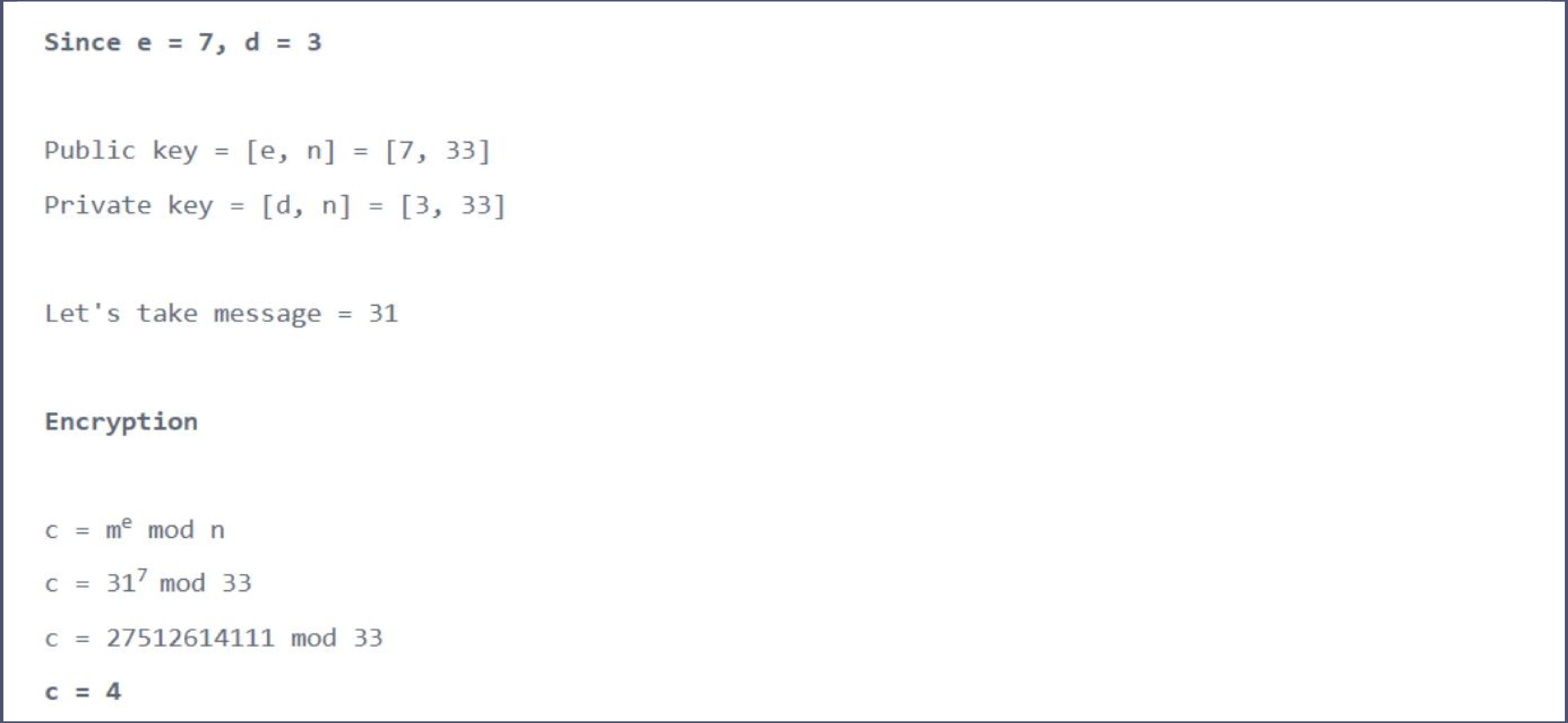
- $m = c^d \bmod n$

Example RSA Algorithm



```
Let's understand with an example


Assume p = 3, q = 11

n = 3x11 = 33                                          [i.e. n = pxq]

Φ(n) =  2x10 = 20                                   [i.e Φ(n) = (p-1)(q-1)]


So, let's take

e = 7 [1<7<20 and gcd ((7,20) = 1) ]


Now,


de mod Φ(n) = 1

7xd mod Φ(n) = 1

7xd mod 20 = 1       [ *** d = 3]
```

Example RSA Algorithm



Since e = 7, d = 3

Public key = [e, n] = [7, 33]

Private key = [d, n] = [3, 33]

Let's take message = 31

Encryption

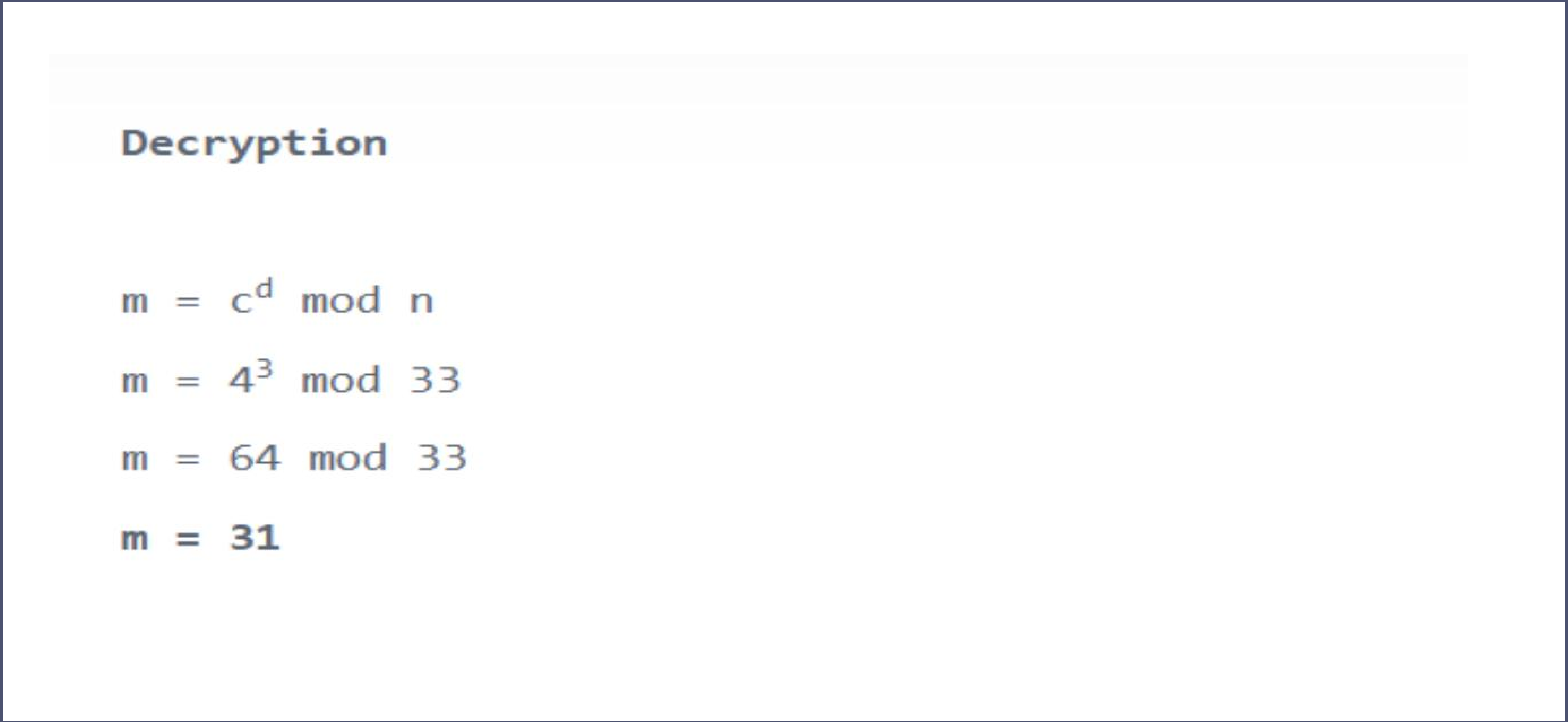
c = m^e mod n

c = 31^7 mod 33

c = 27512614111 mod 33

c = 4

Example RSA Algorithm



Decryption

$m = c^d \bmod n$

$m = 4^3 \bmod 33$

$m = 64 \bmod 33$

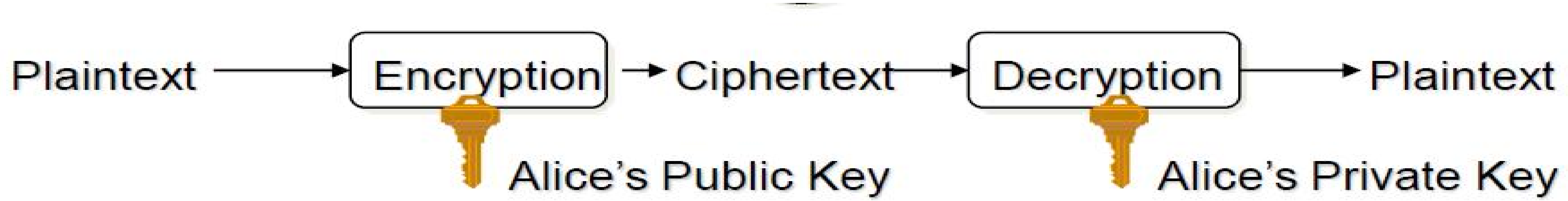
$\mathbf{m = 31}$

Public Key Cryptography

Public Key Cryptography, also called asymmetric cryptography, is a system where each user has a pair of mathematically linked keys: a "public key" that can be freely shared with anyone, and a "private key" kept secret.
Allowing anyone to encrypt messages using the recipient's public key, but only the recipient can decrypt them using their private key, enabling secure communication, digital signatures, and user authentication.

Key Points about Public Key Cryptography
Two Keys:

Public Key – Can be freely distributed.
Private Key – Must be kept secret.



Need for Public Key Cryptography

- Symmetric encryption requires secure key exchange, which is challenging.
- Public Key Cryptography enables secure communication over untrusted networks.
- Ensures Confidentiality, Integrity, Authentication, and Non-Repudiation

Public Key Cryptography

Applications:

- **Secure Communication** – Used in internet security (SSL/TLS).
- **Email Encryption** – Protects email privacy (PGP, S/MIME).
- **Website Authentication** – Enables **HTTPS** for secure browsing.
- **Code Signing** – Ensures software integrity and authenticity.

Key Management Techniques

- **Public Key Infrastructure (PKI) – A framework to manage key pairs securely.**

- **Certificate Authorities (CAs) – Trusted entities that issue and verify digital certificates.**

- **Key Revocation & Expiry – Managing outdated or compromised keys.**

Key Distribution

- **Public announcement**
- **Public key directory**
- **Public key Authority**
- **Certificate Authorities**

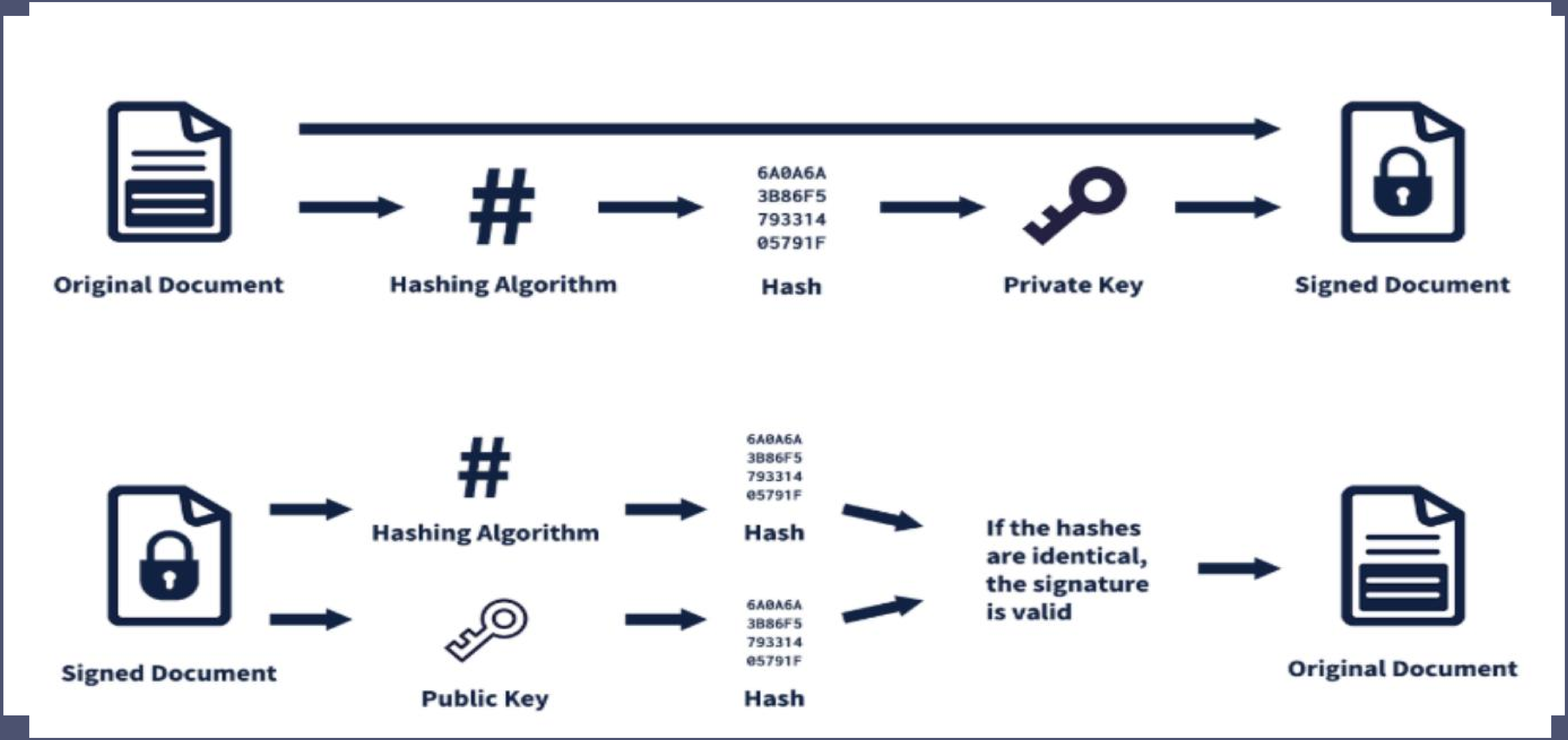
Key Distribution Problem

- Ensuring a public key is authentic and belongs to the claimed entity.
- Risk of Man-in-the-Middle (MITM) attacks if an attacker replaces the public key
- Solutions: Certificate Authorities (CAs) & Web of Trust.

Digital Signature

- A digital signature is a method of authenticating a message or document
- A digital signature confirms that a message or document originated with a specific signer, and that it has not been altered since it was signed.
- They are often used with PDF documents, email messages, and word-processing documents to authenticate the signer and recipient.

Digital Signature


Original Document
Hashing Algorithm
6A0A6A
3B86F5
793314
05791F
Hash
Private Key
Signed Document
Signed Document
Hashing Algorithm
6A0A6A
3B86F5
793314
05791F
Hash
Public Key
6A0A6A
3B86F5
793314
05791F
Hash
If the hashes are identical, the signature is valid
Original Document