- **Decryption**
  - The Recipient B does following
    - Uses the private key *(d,n)* to compute $m=C^d \bmod n$
    - Extract the plaintext from the integer representative 'M'

- **Summary**
  - $n=pq$ where p and q are distinct primes
  - $m=(p-1)\,(q-1)$
  - Select 'e' such that $e<n$ such that $\gcd(e,m)=1$
  - $d=e^{-1} \bmod m$
  - $C=M^e \bmod n$, $1<n<m$
  - $M=C^d \bmod n$

- Key Length
  - Key length for RSA is typically 1024 bits
  - With faster computers available today time taken to encrypt and decrypt even with 4096 bits modulus really is not an issue any more.

- Security
  - The security of RSA cryptosystem is based on mathematical problems

1978 - Rivest RSA
- Shamir
- Adleman

$K_U = (e, n)$
$K_R = (d, n)$

1. p & q 10^{100}
2. $n = p \times q$
3. $z = (p-1) \times (q-1)$
4. $1 < e < z$
5. $(d \times e) \bmod z = 1$

Encrypt $C = m^e \bmod n$

Decrypt $c^d \bmod n = m$

1. $p = 3 \quad q = 11$
2. $n = 33$
3. $z = 2 \times 10 = 20$
4. $e = 7$
5. $(d \times e) \bmod 20 = 1$

$d = 3$

$K_U = (7, 33) \quad K_R = (3, 33)$

$m = 2$ Encrypt $2^7 \bmod 33 = 29$

Decryption $29^3 \bmod 33 = 2$

Key Management

- Key Distribution
  - There are two aspects of public key cryptography are:-

    -The distribution of public keys, and

    - The use of public key encryption to distribute secret keys .
  - The public key can be distributed by any one of the following approaches :

Public announcement

Publically available directory

Public key Authority

Public key certificates

Key Management Contin…

- **Public Announcement**
  - The owner of public key broadcasts his key to the community.
  - Drawback:
    - Any one can forge such key and may misuse it for encryption or decryption of the data because there is no control on the accessing of the key .

Management Contin…

- **Publically Available directory**
  - Provides more security by maintaining a publically available directory of public keys
  - Every user should keep the keys in the directory associated and a trusted party is responsible for distribution of public keys to different users.
  - The directory maintains the database of the keys such as name of the person/party with his public keys.
  - Each user has to register his public keys to the database.

  - **Weakness**
    - If the opponent is able to capture the password of the directory, he will be able to access all public keys

Management Contin…

- **Public key Authority**
  - Provides tight control over the distribution of public keys from the directory
  - The authority is responsible for the distribution of the public key.
  - The directory will maintain the public keys of all persons and each person should know the public keys of authority.

Management Contin…

- **Public key Certificates**
  - Is an alternative to public key authority where it uses certificates.
  - This approach was suggested by Kohnfelder.
  - The certificates can be used by the user to exchange the keys without contacting authority.
  - Each certificate contains public key and other meta information such as time, network address of the user who made a request. The time used to differentiate among the user request.