Public Key Cryptography

- It is used two keys for encryption and for decryption.
  – a public-key, which may be known by anybody, and can be used to encrypt messages
  – a private-key, known only to the recipient, used to decrypt messages

- It has six ingredient

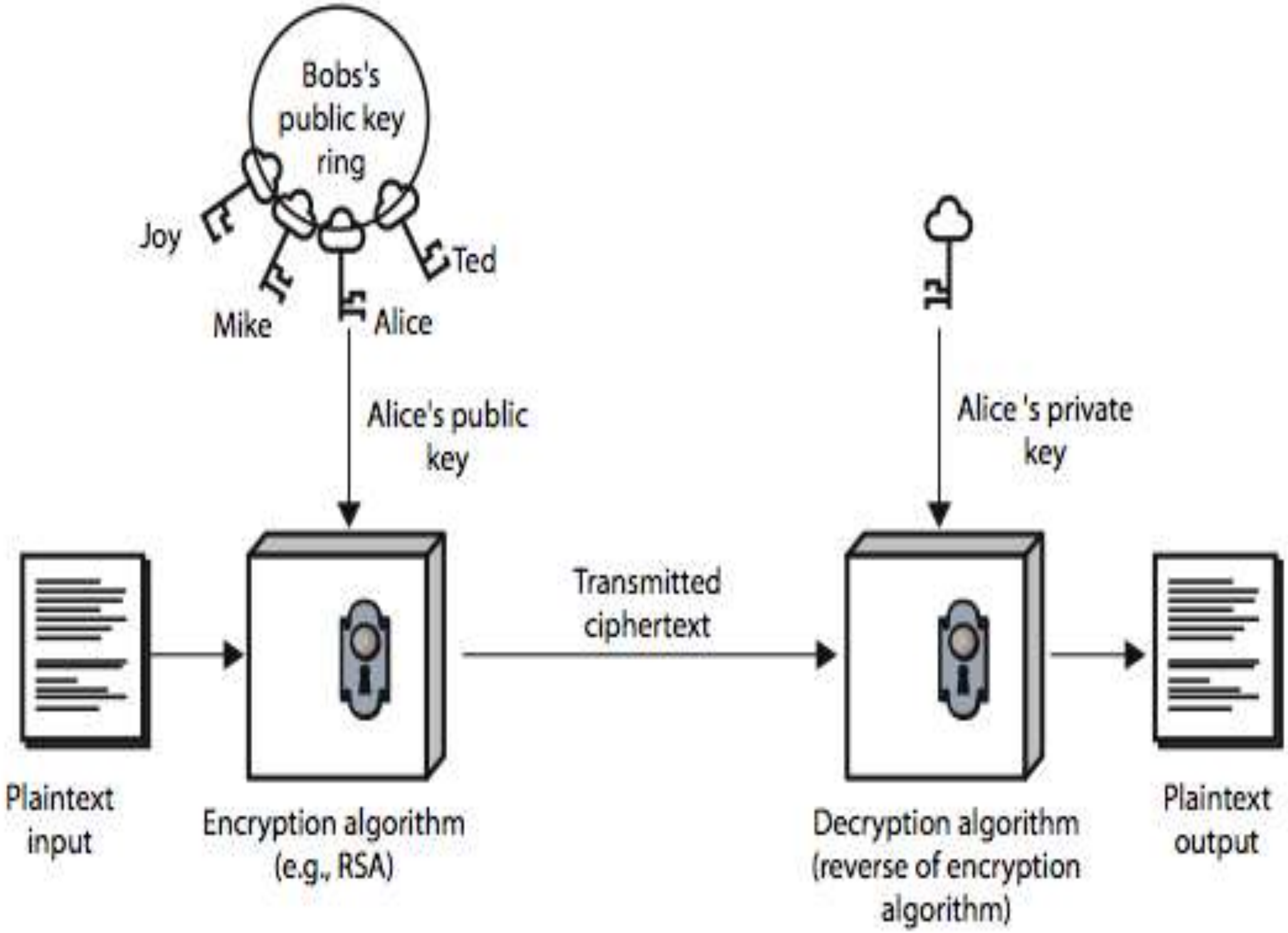
1 Plain text

2 Encryption algorithm

3 Public and private keys

4 Ciphertext

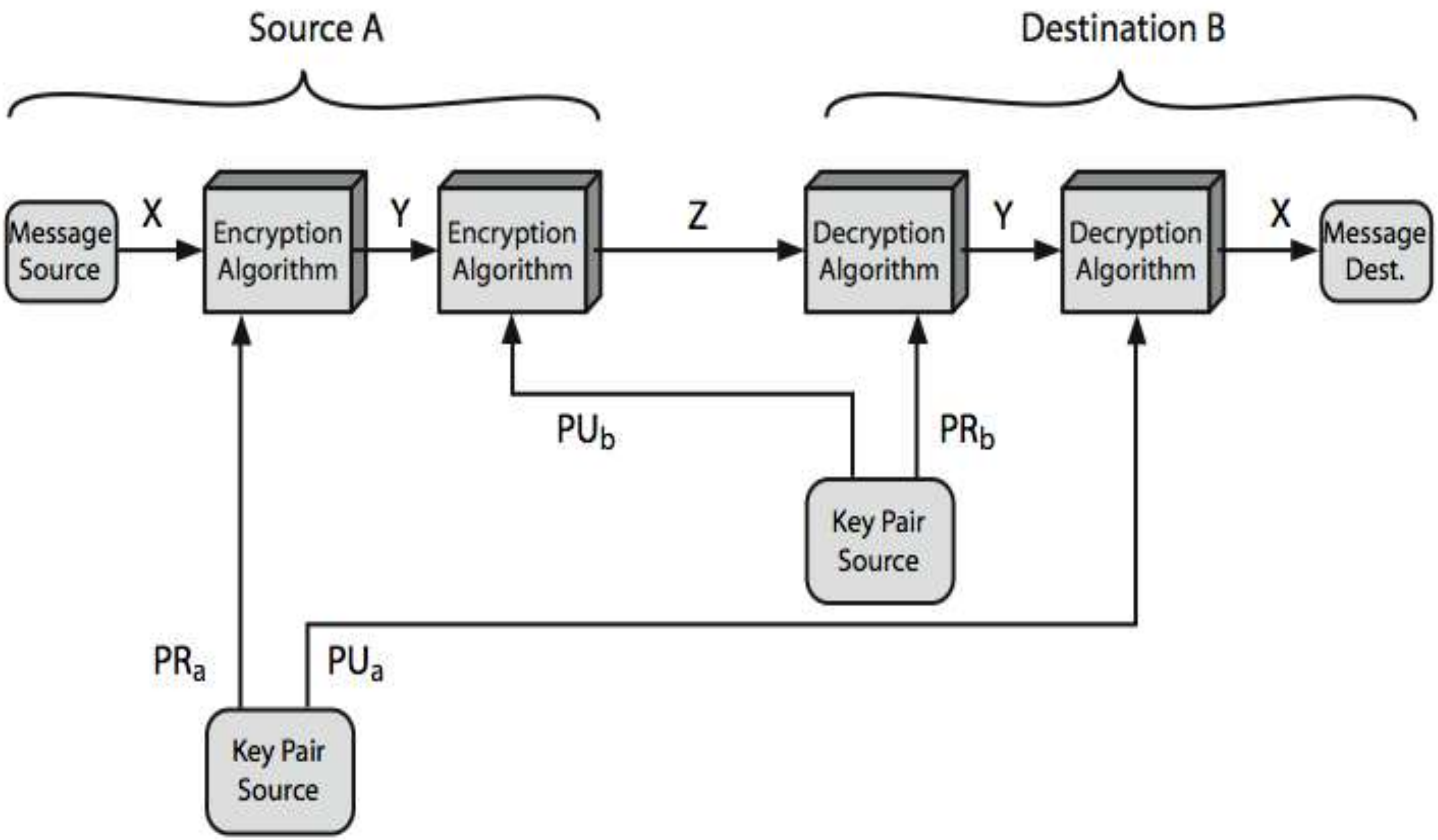
5 Decryption algorithm



(a) Encryption

Public-Key Characteristics

- Public-Key algorithms rely on two keys where:
  - it is computationally infeasible to find decryption key knowing only algorithm & encryption key
  - it is computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known
  - either of the two related keys can be used for encryption, with the other used for decryption (for some algorithms)



Public key Cryptosystem : Authentication and secrecy

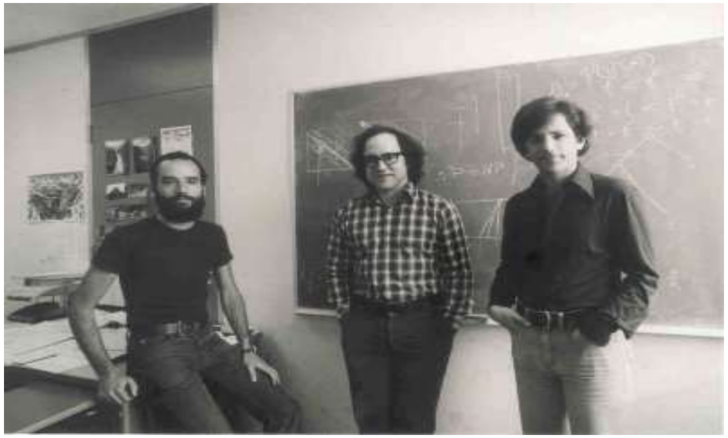
Requirement of Public key Cryptography

1. It is easy for party **B** to generate a pair of keys (public key PU_b , Private key PR_b).
2. It is easy for a sender **A** , knowing the public key and message to be encrypt. $C=E(PU_b, M)$
3. It is easy for receiver **B** to decrypt the resulting ciphertext using the private key . $M=D(PR_b,C)=D[PR_b,E(PU_b,M)]$
4. It is infeasible for an any person , to know the public key PU_b to determine the private key PR_b.
5. It is infeasible for any person to know the public key **PUb** and a ciphertext **C** to recover the original message **M.**
6. Two keys can be applied in either order

$$M=DP[PU_b, E(PR_b,M)] = D[PR_b,E(PU_b, M)]$$

Exercise

- Explain the difference between conventional and public key encryption.
- What are the different requirements for public key cryptography .



RSA

- Invented by **R**ivest, **S**hamir & **A**dleman of MIT in 1977
- It is a best known & widely used public-key scheme.
- It is a **block cipher algorithm** in which palintext and ciphertext integers between 0 to n-1 for some ***n.***
- A typical size for ***n*** is 1024 bits or 309 decimal digits.

RSA Algorithm

Key Generation

Select p, q	p, q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

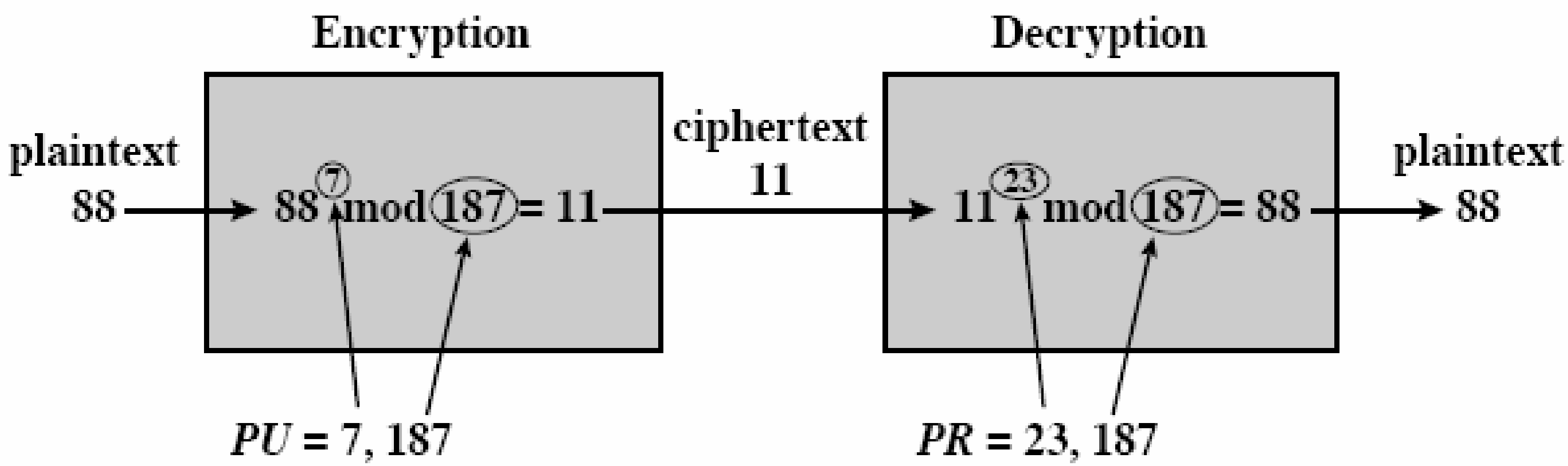
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod{n}$

RSA Algorithm: Example

- Select two large primes: p, q, p ? q
  $p = 17$, $q = 11$
- $n = p \times q = 17 \times 11 = 187$
- Calculate $\Phi = (p-1)(q-1) = 16x10 = 160$
- Select e, such that lcd(Φ, e) = 1; $0 < e < \Phi$
  say, $e = 7$
- Calculate d such that de mod $\Phi = 1$
  - $160k+1 = 161, 321, 481, 641$
  - Check which of these is divisible by 7
  - 161 is divisible by 7 giving $d = 161/7 = 23$
- Key 1 = {7, 187}, Key 2 = {23, 187}



Example of RSA Algorithm

An Example

- Let p= 3 and q=5,
- n= 3 X 5 =15
- Q(n)= (3-1) * (5-1) = 2 x 4= 8
- Select e such that **gcd**(Q(n), e) =1 where, 1<e<Q(n)
- Say e=3 (any prime number)
- Calculate d , such that d e mod Q(n)=1
- 8k+1= 9, 17,25, 33, 41……..where k=1,2,3,4….
- Now check which number is divisible by 3.
- 33 is divisible by 3 .So, d=33/3=11. //9 is also divisible by 3.
- Now k1=(3,15) and K2=(11,15)
- Take plan text M =**13 , where (M<n)**
- Encryption C= 13^3 mod 15 =7
- Decryption D= 7^{11} mod 15 =**13**

Exercise

- Perform encryption and decryption using the RSA algorithm for the following

1. p=3, q=11, e=7, M=5
2. P=5,q=11, e=3 , M=9

- Explain various Asymmetric Encryption Algorithms .
- Draw an algorithm, flowchart for implementing the RSA Algo.

Diffie –Hellman Key Exchange

in 1976

- It is used by two users to **securely exchange a key** that can be used for subsequent encryption of messages.

a public-key distribution scheme
- cannot be used to exchange an arbitrary message
- rather it can establish a common key
- known only to the two participants

value of key depends on the participants (and their private and public key information)

based on mathematical principles

security relies on the difficulty of computing discrete logarithms (similar to factoring) – hard

Diffe-Hellman Key Exchange Algorithm

Global Public Elements

q = prime number(300 decimal, i.e. 1024 bits)

α = Integer

User A key Generation

Select private Xa , Xa < q

Calculate public Ya , Ya= α^{Xa} mod q

User B Key Generation

Select private Xb , Xb < q

Calculate public Yb , Yb= α^{Xb} mod q

Diffe-Hellman Key Exchange Algorithm

Generation of secret key by user A

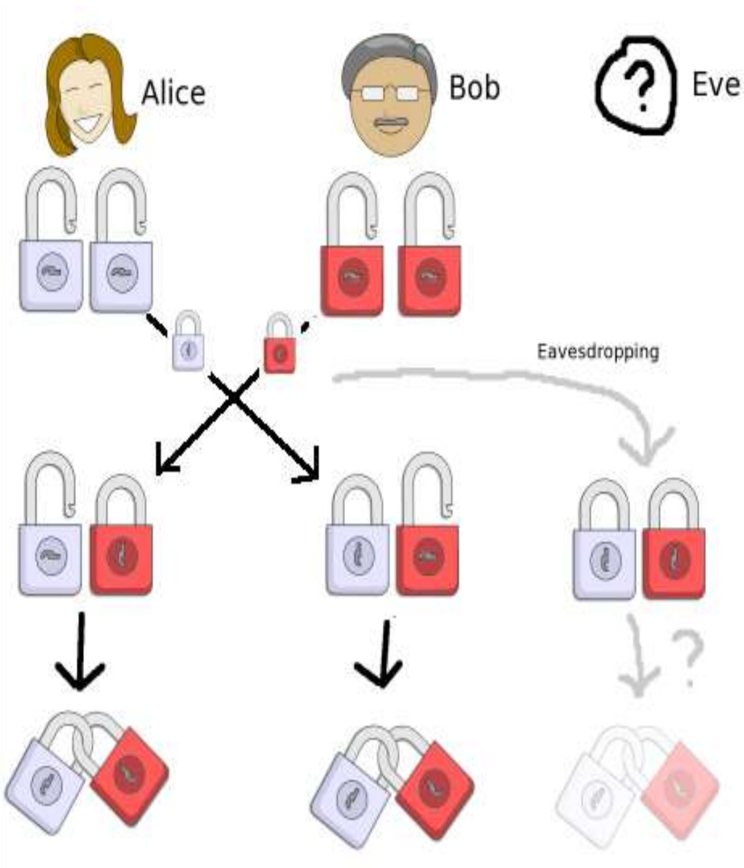
$$K=(Y_b)^{X_a} \bmod q$$

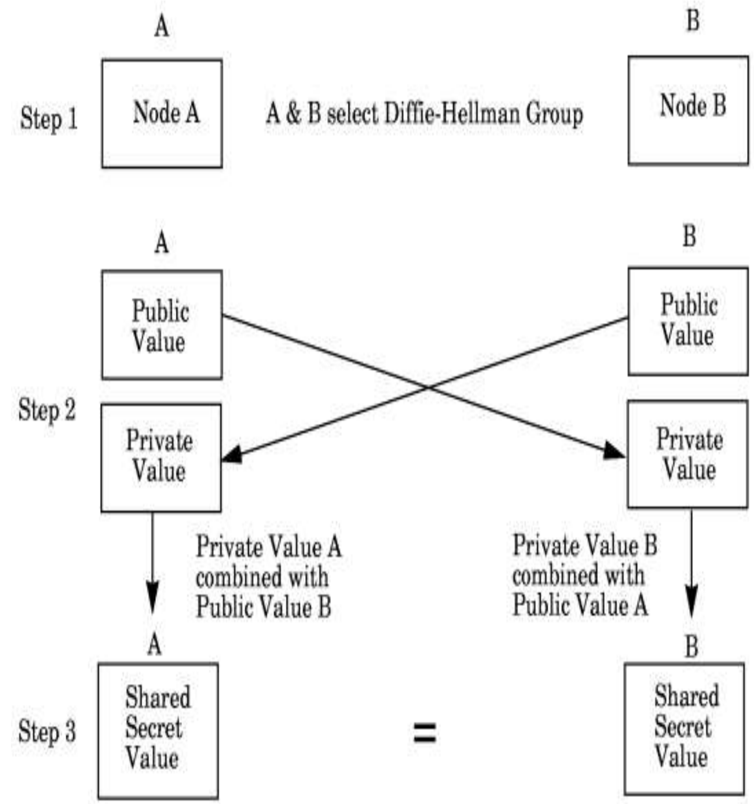
Generation of secret key by user B

$$K=(Y_a)^{X_b} \bmod q$$

- users Alice & Bob who wish to swap keys:
- agree on prime $q=\mathbf{353}$ and $\alpha=\mathbf{3}$
- select random secret keys:
  - A chooses $x_A=\mathbf{97}$, B chooses $x_B=\mathbf{233}$
- compute respective public keys:
  - $y_A=\mathbf{3}^{97}$ mod $\mathbf{353}$ = $\mathbf{40}$ (Alice)
  - $y_B=\mathbf{3}^{233}$ mod $\mathbf{353}$ = $\mathbf{248}$ (Bob)
- compute shared session key as:
  - $K_{AB}= y_B^{xA}$ mod $\mathbf{353}$ = $\mathbf{248}^{97}$ = 160 (Alice)
  - $K_{AB}= y_A^{xB}$ mod $\mathbf{353}$ = $\mathbf{40}^{233}$ = 160 (Bob)

Diffie –Hellman Key Exchange





Exercise

users Alice & Bob who wish to swap keys:
agree on prime q=5 and α=7
select random secret keys:

- A chooses x_A= 8, B chooses x_B= 13

Exercise

Using diffie- hellman key exchange techniques ,Find A’s public key Y_A and B’s public key Y_B .
If, q=71 and α= 7 , X_A =5 and X_B = 12

Draw an algorithm, flowchart and write C++ program to implement Diffe-Hellman Key Exchange Algorithm