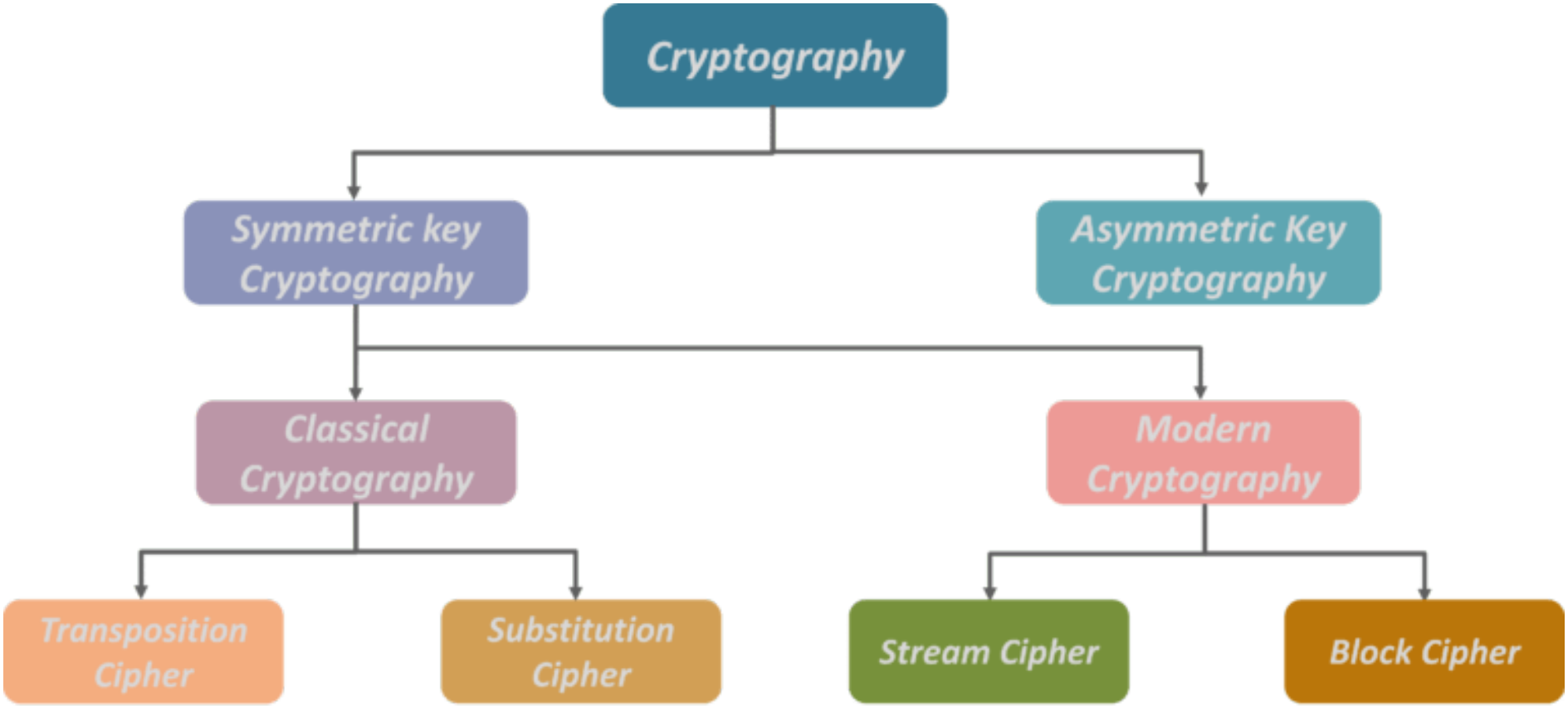
19CSE311 - COMPUTER SECURITY
UNIT-1
PART 2

January 18, 2022

Dr.Remya S/Mr. Sarath R
Assistant Professor
Department of Computer Science

AMRITA VISHWA VIDYAPEETHAM
DEEMED TO BE UNIVERSITY
School of Engineering

Public Key Cryptography



Why Public-Key Cryptography?

Developed to address two key issues:

1. Key distribution – how to have secure communications in general without having to trust a KDC with your key
2. Digital signatures – how to verify a message comes intact from the claimed sender

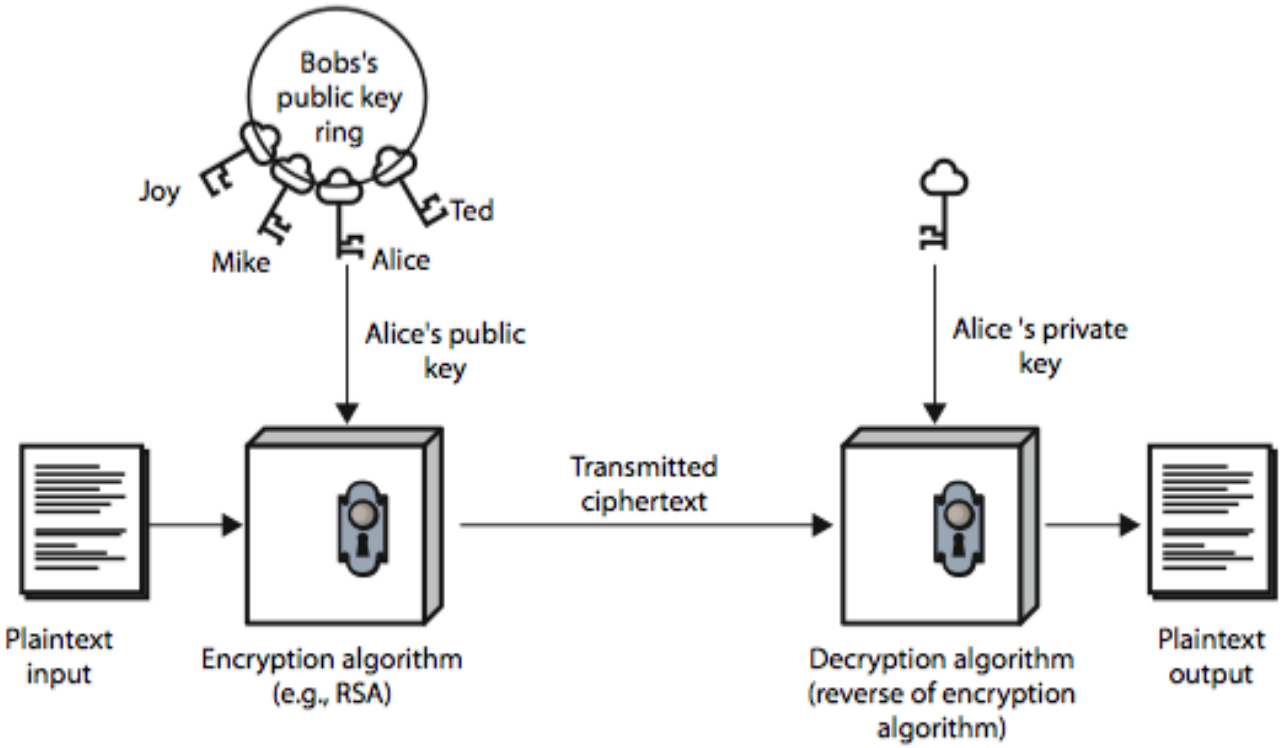
Asymmetric Key Cryptography

- Different keys are used for encryption and decryption
- Public key used for encryption, private key used for decryption and vice versa.
- It is also known as public key cryptography.
- Asymmetric cipher model consists of 6 elements
  1. Plain Text
  2. Encryption Algorithm
  3. Private Key
  4. Public Key
  5. Cipher Text
  6. Decryption Algorithm

- Plaintext is the original message or data that is fed into the algorithm as input
- Encryption algorithm performs various transformation on the plain text
- Public & Private Keys : Pair of keys that have been selected so that if one is used for encryption , the other is used for decryption
- Ciphertext is the unreadable message produces as output. It depends on the plain text and the key. Two different keys produced two different outputs
- Decryption Algorithm— takes the cipher text and the key and produces the original plaintext
- Public key is distributed to all users and private key is known to a particular user only
- There are 2 different scenario of encryption model:
  1. Public key used for encryption and private key used for decryption
  2. Private key used for encryption and public key used for decryption

Scenario 1

- If Bob wants to send message to Alice, Bob must have to use public key of Alice.Message to be transmitted after encryption of message using Alice's public key.
- Alice has received message and she can decrypt the message using only her private key's.



(a) Encryption

Mathematically, it is represented,

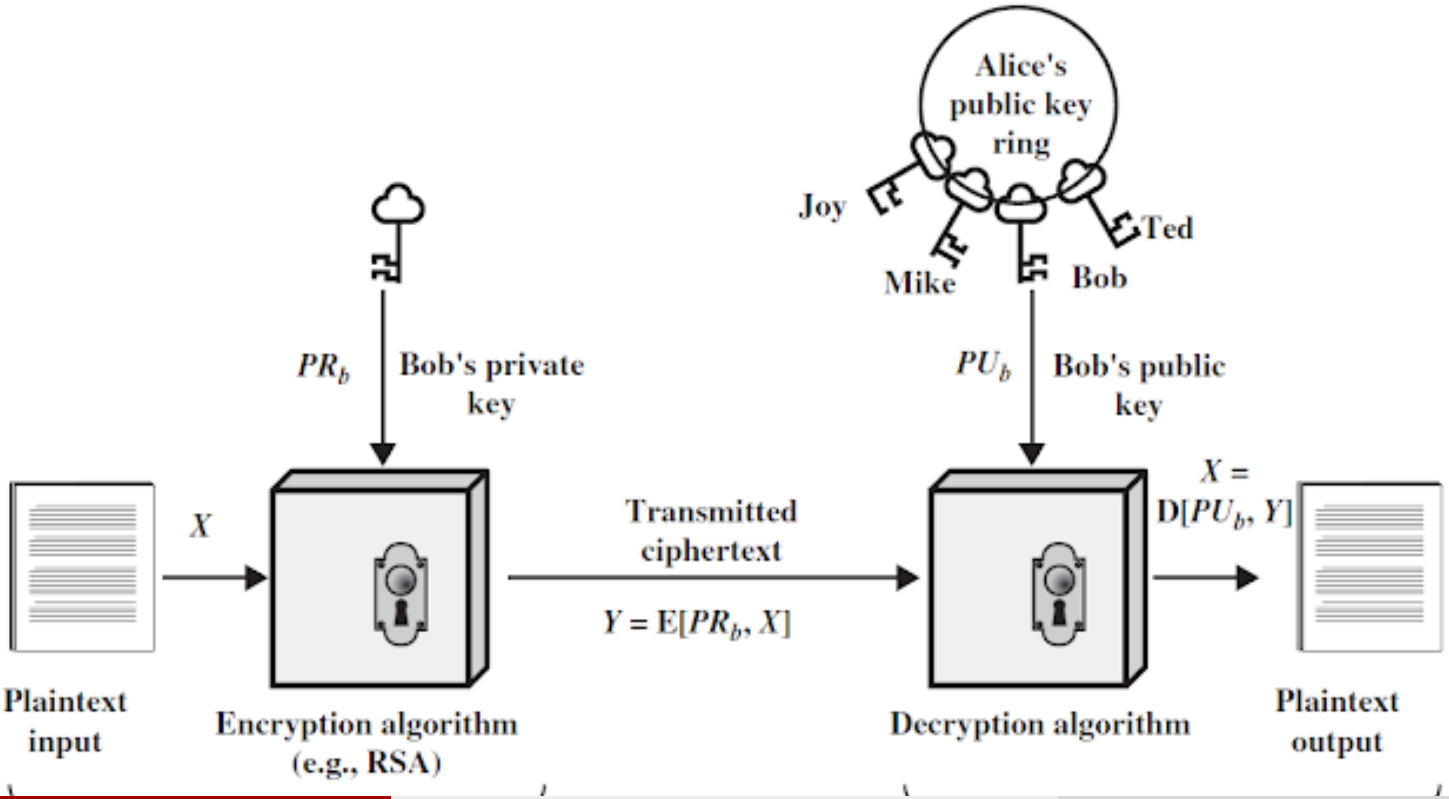
$Y = E(Pu(A), X)$

$X = D(Pr(A), Y)$.

Where, $Pu(A)$ = Alice public key and $Pr(A)$ = Alice private key.

Scenario 2

- If Bob wants to send message to Alice, Bob must have to use his own private key. Message to be transmitted after encryption of message using Bob's public key.
- Alice has received message and she can decrypt the message using Bob's public key.



Mathematically, it is represented,

$Y = E(Pr(B), X)$

$X = D(Pu(B), Y)$.

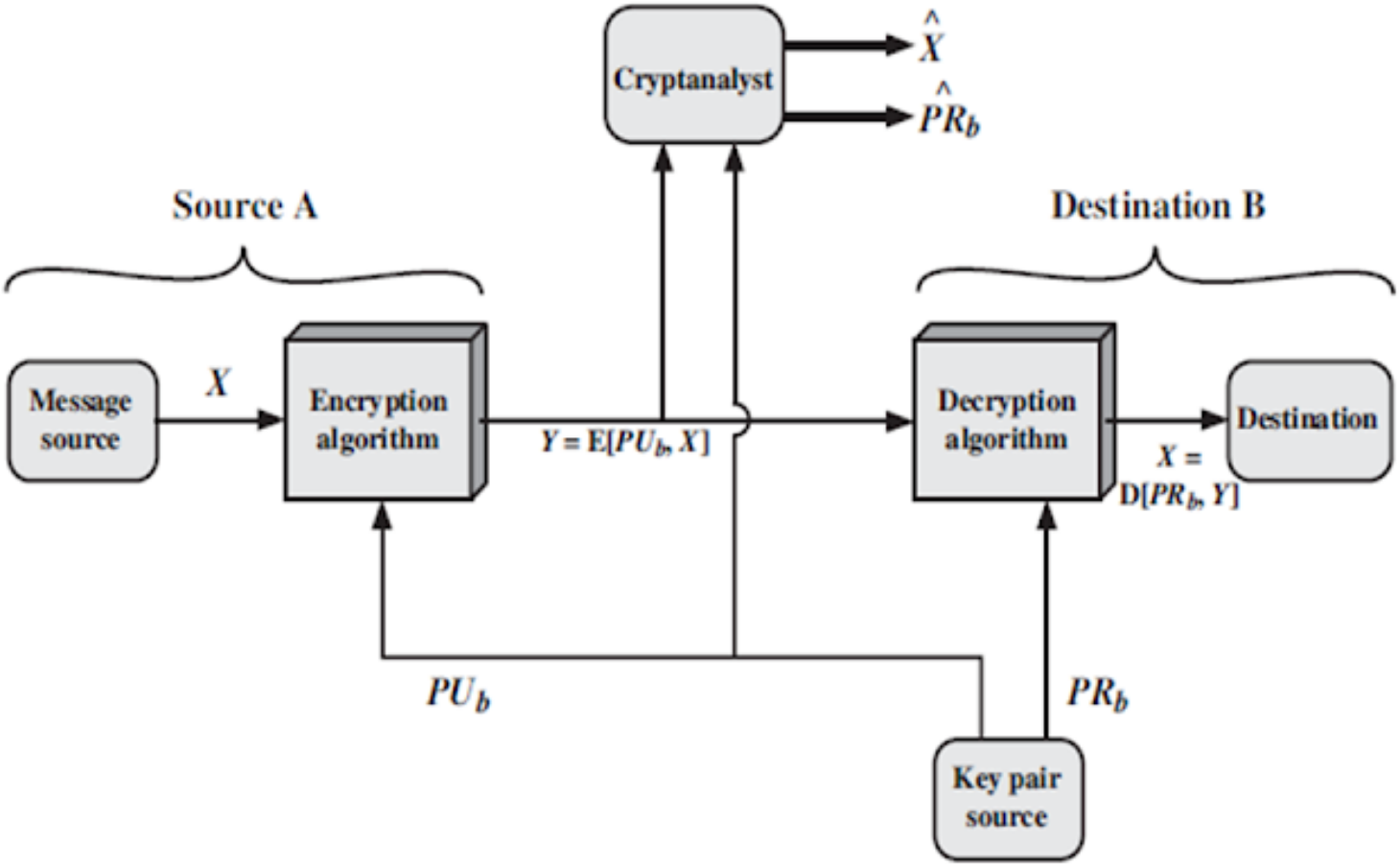
Where, $Pr(B)$ = Bob's private key, $Pu(B)$ = Bob's public key.

Key Details	Bob Should Know	Alice Should Know
Bob's Private Key Pr(B)	Bob must know	Alice not known
Bob's Public Key Pu(B)	Bob must know	It is known to Alice also
Alice's Private Key Pr(A)	Bob not known	Alice must know
Alice's Public Key Pu(A)	It is known to Bob	Alice must know

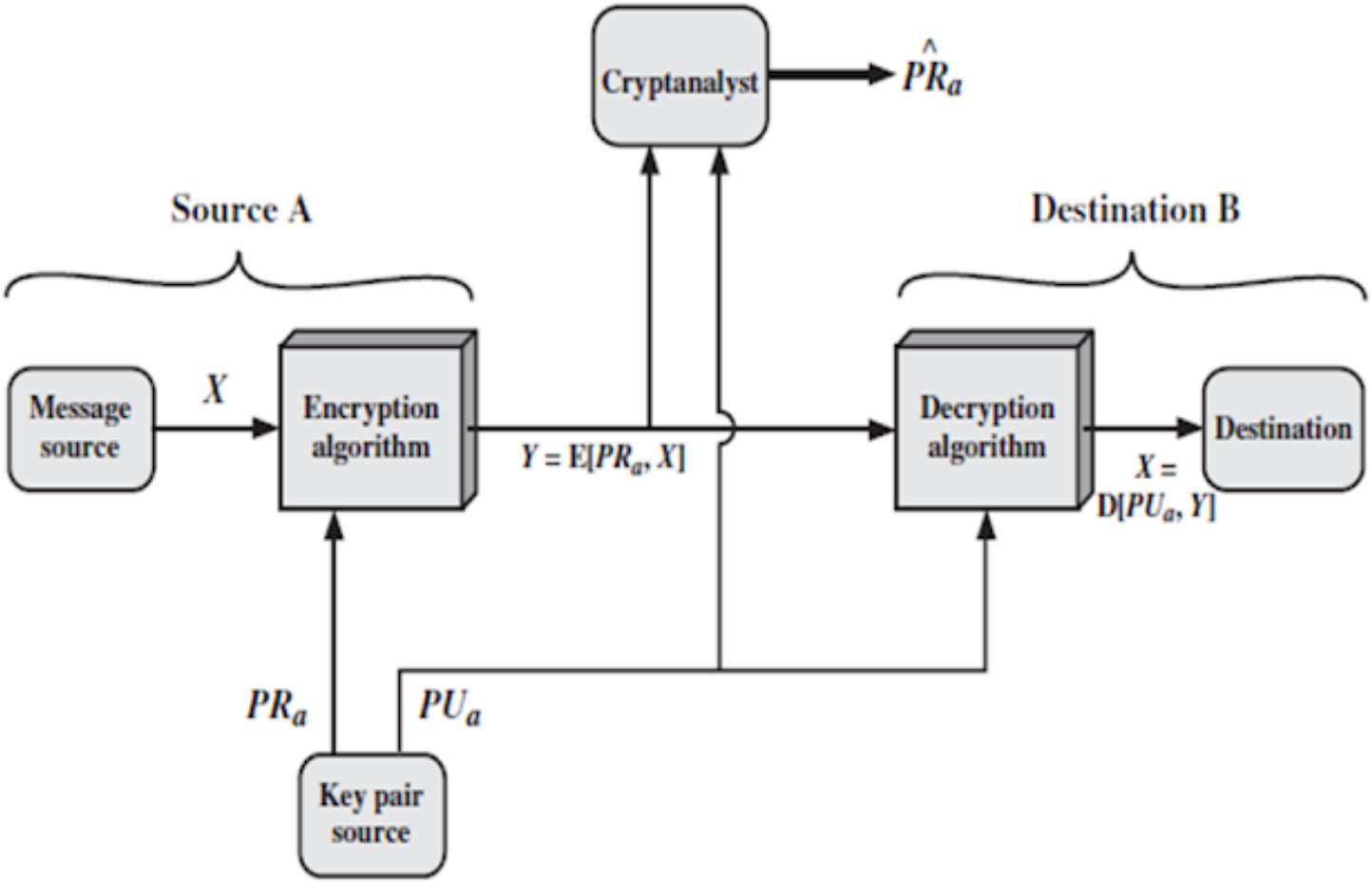
Eg: RSA Algorithm, Deffie Hellman Key Exchange Algorithm

- Advantages
  1. If data is transmitting on insecure channel, but key cannot distributing among sender and receiver
  2. Separate key is used for encryption and decryption, even if encrypted message is stolen by attacker he/she cannot decrypt the message
- Disadvantages
  1. Asymmetric key use more resources as compared to symmetric key cryptography
  2. More mathematical calculations required
  3. Slower as compared to symmetric cryptography

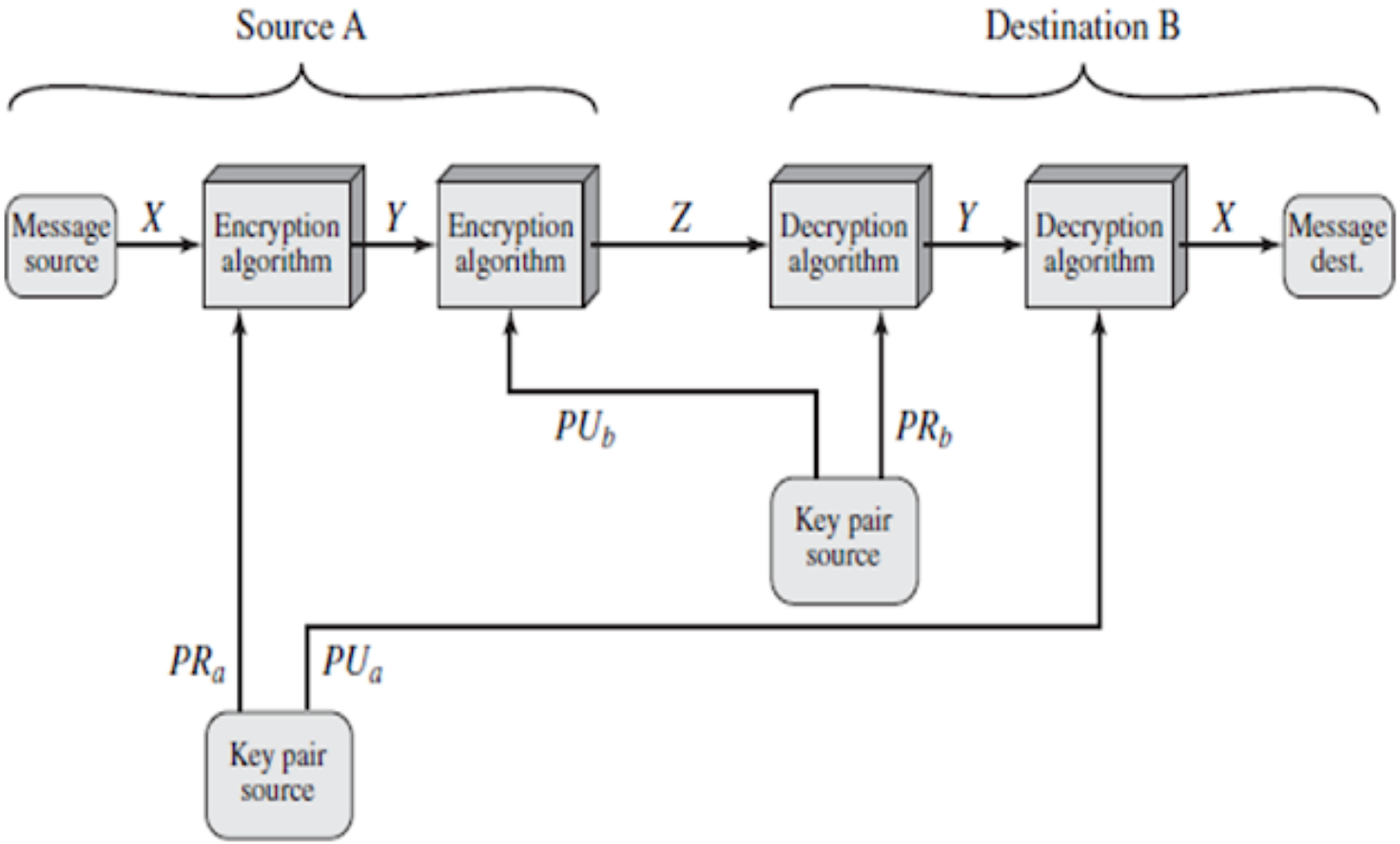
How to achieve Confidentiality using public key cryptography?



How to achieve authenticity using public key cryptography?



How to achieve Confidentiality & authenticity using public key cryptography?



Applications of public key cryptography

- Encryption/Decryption: During this process the sender encrypts the message with the receiver's public key.
- Digital Signature: During this process the sender "signs" a message with his private key.
- Key exchange: Both sender & receiver cooperate to exchange a session key, typically for conventional encryption.

Requirements for Public-Key Cryptography

- It is computationally easy for a party B to generate a pair (public key PU_b, private key PR_b).
- It is computationally easy for a sender A, knowing the public key and the message to be encrypted,M, to generate the corresponding ciphertext: $C = E(PU_b,M)$
- It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message: $M = D(PR_b, C) = D[PR_b, E(PU_b,M)]$
- It is computationally infeasible for an adversary, knowing the public key, PU_b, to determine the private key,PR_b.
- It is computationally infeasible for an adversary, knowing the public key,PU_b, and a ciphertext, C, to recover the original message,M. We can add a sixth requirement that, although useful, is not necessary for all public-key applications:
- The two keys can be applied in either order: $PR_bM = D[PU_b, E(PR_b,M)] = D[PR_b, E(PU_b,M)]$

Symmetric Vs Asymmetric

Table 9.2 Conventional and Public-Key Encryption

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

RSA Algorithm

- Developed by Rivest, Shamir Adleman of MIT in 1977
- Best known widely used public-key scheme(Asymmetric encryption)
- The algorithm works as follows
  - Step-1: Select two prime numbers p and q where $p \neq q$
  - Step-2: Calculate $n = p * q$.
  - Step-3: Calculate $\Phi(n) = (p-1) * (q-1)$.
  - Step-4: Select e such that, e is relatively prime to $\Phi(n)$, i.e. $(e, \Phi(n)) = 1$ and $1 < e < \Phi(n)$
  - Step-5: Calculate $d = e^{-1} mod \Phi(n)$ or $ed = 1 \bmod \Phi(n)$
  - Step-6: Public key = $\{e, n\}$, private key =$\{d, n\}$.
  - Step-7: Find out cipher text using the formula,
    $C = P^e modn$ where, $P < n$
    where C = Cipher text, P = Plain text, e = Encryption key and n=block size.
  - Step-8: $P = C^d modn$.
    Plain text P can be obtained using the given formula. where, d = decryption key

RSA algorithm explanation with example step by step

Step – 1: Select two prime numbers p and q where p q.
Example, Two prime numbers p = 13, q = 11.
Step – 2: Calculate n = p * q.
Example, n = p * q = 13 * 11 = 143.
Step – 3: Calculate $\Phi(n)$ = (p-1) * (q-1).
Example, $\Phi(n)$ = (13 – 1) * (11 – 1) = 12 * 10 = 120.
Step – 4: Select e such that, e is relatively prime to (n), i.e. (e, $\Phi(n)$) = 1 and 1 < e < $\Phi(n)$.
Example, Select e = 13, gcd (13, 120) = 1.
Step – 5: Calculate d = e -1 mod $\Phi(n)$ or e * d = 1 mod $\Phi(n)$
Example, Finding d: e * d mod $\Phi(n)$ = 1

13 * d mod 120 = 1
(How to find: d *e = 1 mod $\Phi(n)$
d = (($\Phi(n)$ * i) + 1) / e
d = (120 + 1) / 13 = 9.30 (i = 1)
d = (240 + 1) / 13 = 18.53 (i = 2)
d = (360 + 1) / 13 = 27.76 (i = 3)
d = (480 + 1) / 13 = 37 (i = 4))
Step – 6: Public key = {e, n}, private key = {d, n}.
Example, Public key = {13, 143} and private key = {37, 143}.
Step – 7: Find out cipher text using the formula, $C = P^e modn$ where, P < n.
Example, Plain text P = 13. (Where, P<S n)
$C = P^e modn = 13^{13} mod 143 = 52.$
Step – 8: P = Cd mod n. Plain text P can be obtain using the given formula.
Example, Cipher text C = 52
P = Cd mod n = 52^{37} mod 143 = 13.

Example 1

Exercise - 1

Question: P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 6, then what will be cipher text value according to RSA algorithm? Again calculate plain text value from cipher text.

Solution:

1. Two prime numbers P=7, Q=17
2. $n = P * Q = 17 * 7 = 119$ **n = 119**
3. $\Phi(n) = (P-1) * (Q-1) = (17-1) * (7-1) = 16 * 6 = 96$ **Φ(n) = 96**
4. Public key $E = 5$. **E= 5**
5. Calculate $d = 77$. $d = ((\Phi(n) * i) + 1) / e$ **d= 77**

   $d = ((96*1)+1) / 5 = 19.4$

   $d = ((96*2)+1) / 5 = 38.6$

   $d = ((96*3)+1) / 5 = 57.8$

   $d = ((96*4)+1) / 5 = 77$ (Stop finding d because getting integer value)
6. Public key = {e, n} = {5, 119}, private key = {d, n} = {77, 119}.
7. Plain text PT = 6, $CT = PT^E \bmod n = 6^5 \bmod 119 = 41$. **Cipher Text = 41**
8. Cipher text CT = 41, $PT = CT^d \bmod n = 41^{77} \bmod 119 = 6$. **Plain Text = 6**

Example 2

Exercise - 2

Question: In a public key cryptosystem using RSA algorithm, user uses two prime numbers 5 and 7. He chooses 11 as Encryption key, find out decryption key. What will be the cipher text, if the plaintext is 2? Decrypt the cipher text, what will be the value of plain text?

Solution:

1. Two prime numbers p = 5, q = 7
2. n = p * q = 5 * 7 = 35 **n = 35**
3. $\Phi(n) = (p-1) * (q-1) = (5-1) * (7-1) = 4 * 6 = 24$ **$\Phi(n) = 24$**
4. Public key e = 11. **e= 11**
5. Calculate d = 11. d = $((\Phi(n) * i) + 1) / e$ **d= 11**
6. Public key = {e, n} = {11, 35}, private key = {d, n} = {11, 35}.
7. Plain text P = 2, $C = P^e \bmod n = 2^{11} \bmod 35 = 18$. **Cipher Text = 18**
8. Cipher text C = 18, $P = C^d \bmod n = 18^{11} \bmod 35 = 2$. **Plain Text = 2**