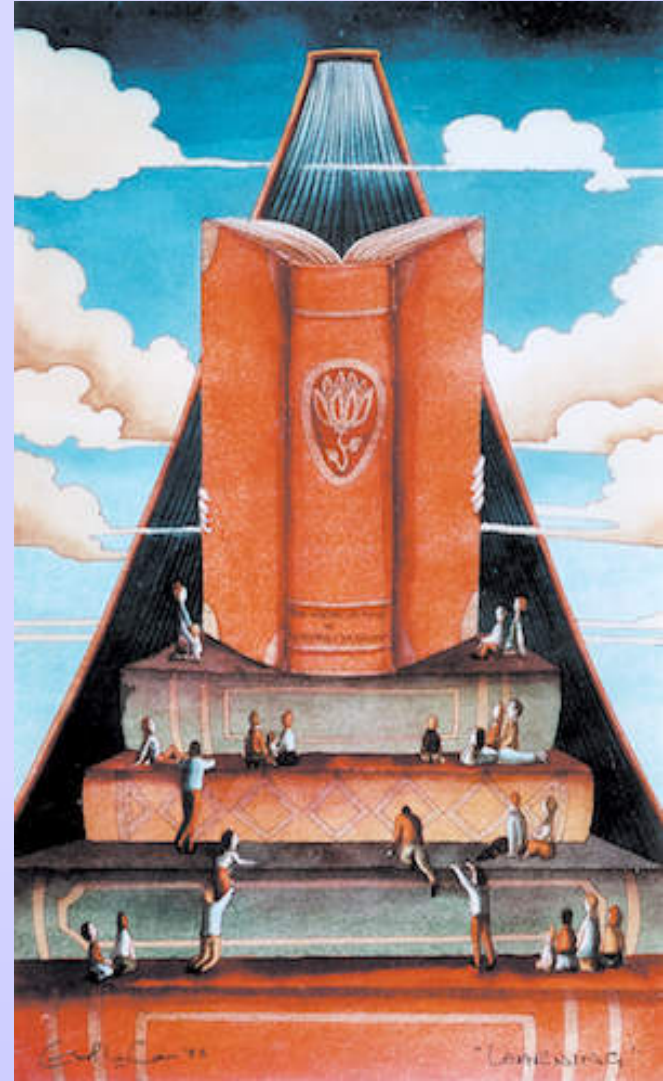



COMPUTER SECURITY (CSE 4105)

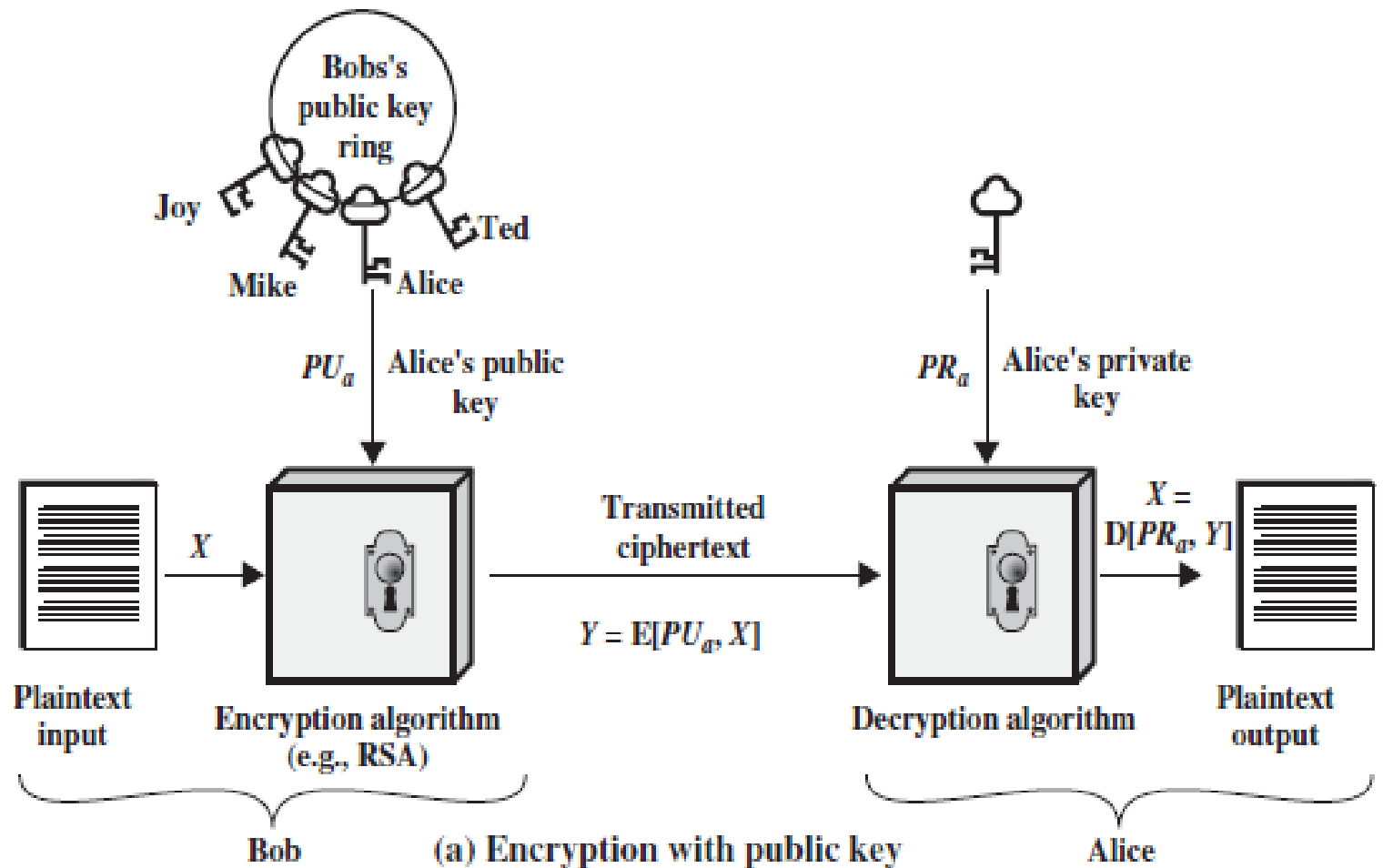
Public Key Cryptosystem and RSA



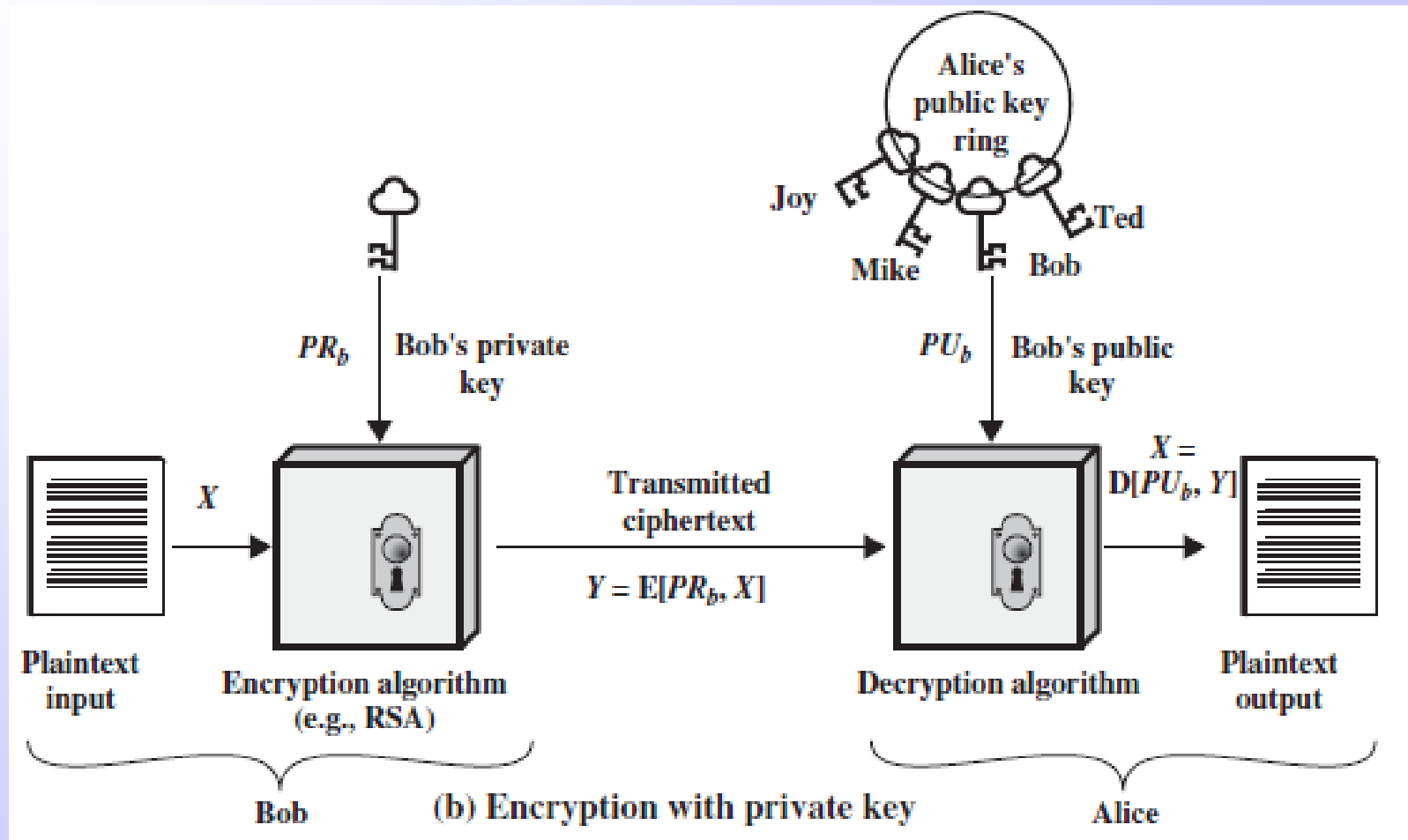
Public Key Cryptosystem

- 
- ➡ When encryption and decryption are performed using the different keys- one a public key and one a private key, is known as public key cryptosystem.
 - ➡ These algorithms have the following important characteristic:
 - It is **computationally infeasible** to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key.
 - In addition, some algorithms, such as RSA, also exhibit the following characteristic:
 - ✓ Either of the two related keys can be used for encryption, with the other used for decryption.


Public Key Cryptosystem




Public Key Cryptosystem




Public Key Cryptosystem

- 
- ☞ A public key encryption scheme has six ingredients:
- **Plaintext**: This is the readable message or data that is fed into the algorithm as input
 - **Encryption algorithm**: The encryption algorithm performs various transformations on the plaintext.
 - **Public and private keys**: This is the pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.
 - **Ciphertext**: This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.
 - **Decryption algorithm**: This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

Essential steps of Public key cryptography

- 
- Each user generates a pair of keys to be used for the encryption and decryption of messages
 - Each user places one of the two keys in a public register or other accessible file. This is public key. The companion key is kept private.
 - If Bob wishes to send a message to Alice, Bob encrypts the message using Alice's public key
 - When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message as only Alice knows Alice's private key

Applications of Public key cryptosystem

- 
- ☞ We can classify the use of public-key cryptosystems into three categories:
 - **Encryption /decryption:** The sender encrypts a message with the recipient's public key.
 - **Digital signature:** The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.
 - **Key exchange:** Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

Requirements for Public-Key Cryptography

☞ **Diffie and Hellman** laid out the conditions:

- 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 .



Requirements for Public-Key Cryptography

- It is computationally infeasible for an adversary, knowing the public key, PU_b , and a ciphertext, C , to recover the original message, M .
- The two keys can be applied in either order [not for all public key cryptosystem]:

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



RSA Cryptosystem

- ➡ Introduced by Ron Rivest, Adi Shamir and Len Adleman
- ➡ Developed in 1977 at MIT and published in 1978.
- ➡ RSA scheme is the most widely accepted and implemented general-purpose approach to public-key encryption



Ronald Linn Rivest
Prof @ MIT



Adi Shamir
Prof @ Tel Aviv University



Len Adleman
Prof @ University of
Southern California.

RSA Cryptosystem

👉 Key Generation:

- Choose randomly two large prime number p, q
- Compute $n=pq$ and $\phi(n)=(p-1)(q-1)$
- Randomly choose e such that
$$\gcd(e, \phi(n)) = 1$$
- Compute $d=e^{-1} \bmod \phi(n)$
- Keep (d, n) as private key and publish (e, n) as public key



Continue...



➡ Encryption:

- Compute $C = m^e \bmod n$
- Send C

➡ Decryption:

- Compute $m = C^d \bmod n$

Thanks for your Attention

