

## Network Security (I)

---

### Security

- Security is a broad problem. In this course, we will look at [securing communication protocols](#).
  - Objectives
    - **encryption**
      - for the [confidentiality](#)
      - the [content](#) of the transmitted message should [only be understood by the sender and receiver](#)
      - an intercepted message cannot be understood by any interceptor/eavesdroppers
    - **authentication**
      - [confirm the other party](#) involved in the communication [is indeed who or what they claim to be](#)
      - no simple if we cannot communicate with the other party face-to-face
    - **message integrity**
      - make sure the [content](#) of the communication [is not altered](#)
      - checksumming techniques can be used to provide message integrity
    - **non-repudiation**
      - Non-repudiation is the concept of [ensuring that a party in a dispute cannot repudiate](#), or [refute the validity](#) of a statement or contact
- 

### Cryptography

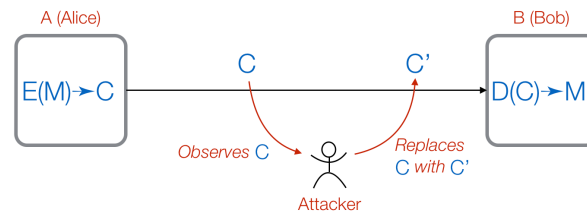
- Cryptographic techniques are relevant to all four objectives we described above.
  - Long history since at least Julius Caesar
  - Modern cryptographic techniques, including many of those used in the Internet, are based on the advances made in the past 30 years
  - We only touch the essential aspects of cryptography, particular as they are practiced on the Internet.
- 

### Encryption



- **Alice** **disguises** the [message/plaintext \(M\)](#) by using an [encryption algorithm \(E\)](#).
- The encrypted message/[ciphertext \(C\)](#) looks unintelligible to any intruder.
- **Bob** receives the ciphertext and **decrypted** it by some [decryption algorithm \(D\)](#).

## Encryption - Attacks



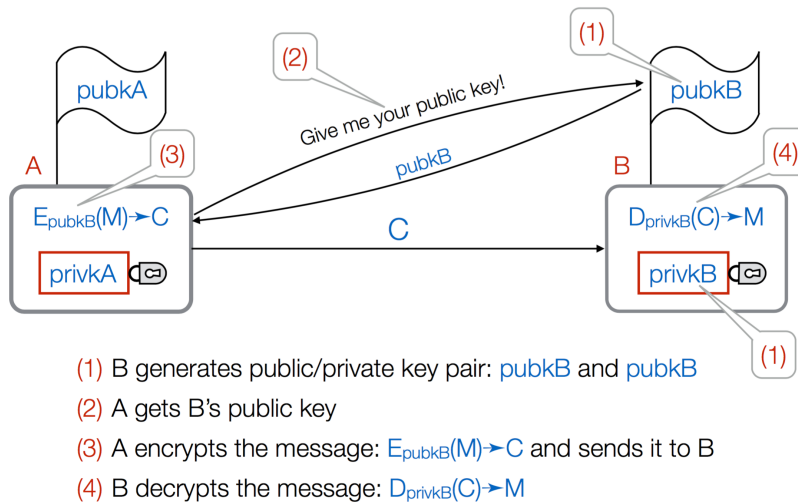
- ▶ **Passive attack:** message observed
- ▶ **Active attack:** message replaced or modified

- Generally speaking, the attacks can be categorized into two groups:
  - **Passive attack:** intruders passively observe the cipher text, decrypt the cipher text, and then know the transmitted messages.
  - **Active attack:** intruders intercept the cipher text and replace with another message or modify the intercepted message and then send it to B.

## Encryption Categories

- **Secret method:**  $E()$  and  $D()$ 
  - Encrypt message using a secret method known by Alice and Bob only
  - Not quite feasible in Internet, as the **encryption technique is available to everyone**.
    - These methods are published and standardized. E.g. MD5/RFC1321, Public-Key Cryptography Standards/RFC3447, PPP Triple-DES Encryption Protocol/RFC2420.
  - So, there must be some secret information that prevents an intruder from decrypting. Therefore, the secret key is introduced.
- **Public method, secret key:**  $E_k()$  and  $D_k()$ 
  - **Encryption algorithm** is **public**, but the **key** is **private**, which are known by Alice and Bob only.
  - So, even if intruders sniff the message, they cannot interpret it without the secret key.
  - Since the sender and receiver use the same private key to encrypt messages, this type of methods are called Symmetric Key Protocols:
    - **DES** - Data Encryption Standard
      - 1977, symmetric key, 56-bit key, 64-bit data
    - **AES** - Advanced Encryption Standard
      - 1998, symmetric key, 128, 192, and 256-bit keys, 128-bit data blocks
  - However, this requires that Alice and Bob have an **agreement on the private key**.
    - They can first meet and agree on the key in person.
    - But, **in Internet this is infeasible**. Agreement on the key must be made over another secure communication. This secure communication faces the same problem.

- **Public method, public and private keys:**  $E_{\text{pubk}}()$  and  $D_{\text{privk}}()$ 
  - To address the issue of the agreement on the private, each person has two keys: a **public** key and a **private** key
  - Public key is accessible to everyone, including intruders. Private key is accessible to the receiver only. The public key and private key are carefully selected and are paired.
  - Alice **uses** the Bob's **public key** along **with a standard encryption algorithm** to **send a message** to Bob
  - After Bob receives the message, he **uses** his **private key** to **decrypt** the ciphertext.



## RSA - Rivest, Shamir, and Adleman

- 1978, **public/private key algorithm**, 1,024 to 4,096-bit keys (typically)
- Requirements:
  - need  $K_B^+(\cdot)$  and  $K_B^-(\cdot)$  such that  $K_B^-(K_B^+(m)) = m$
  - given public key  $K_B^+$ , it should be impossible to compute (which is why key is 1024 to 4096 bits) private key  $K_B^-$
- RSA: getting ready
  - message: just a bit pattern
  - bit pattern can be uniquely represented by an integer number
  - thus, encrypting a message is equivalent to encrypting a number
  - Example:
    - $m = 1001\ 0001$ . This message is uniquely represented by the decimal number 145.
    - to encrypt  $m$ , we encrypt the corresponding number, which gives a new number (the ciphertext).

*Disclaimer: Notes adapted from the textbook and online resources.*