Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques

June 24-28, 2024

Murtuza Jadliwala

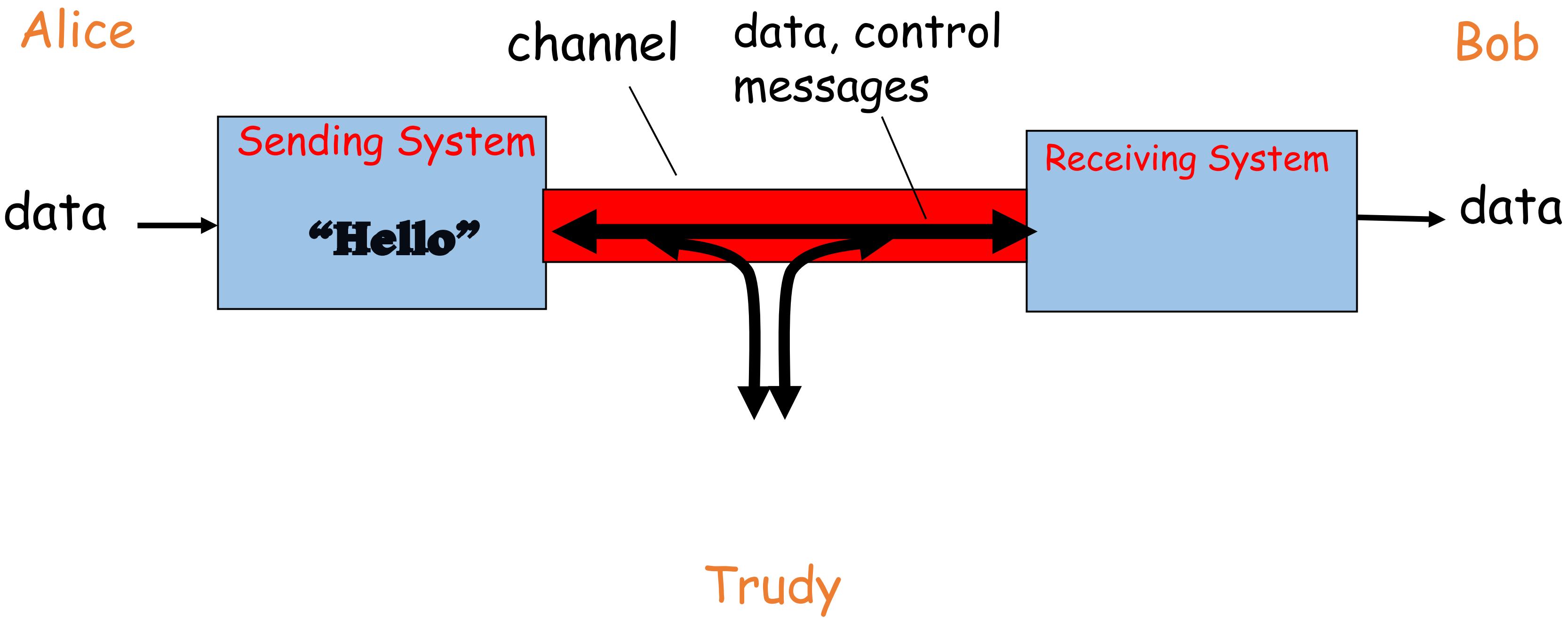
murtuza.jadliwala@utsa.edu

Information Security and Cryptography

Data/Information Security

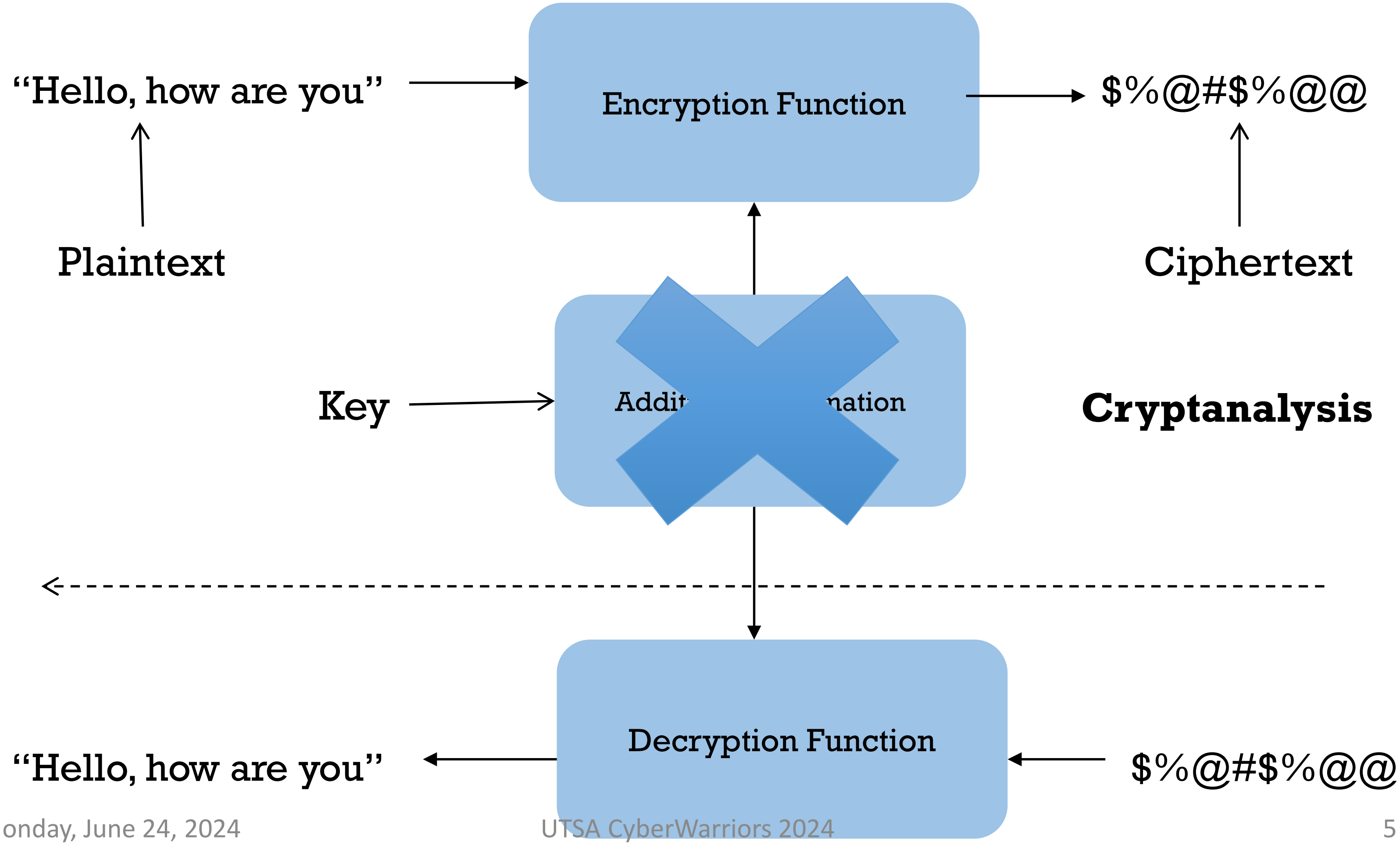
- Protection against security threats to data and information
- Required security properties:
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity
  - Accountability
  - Privacy

Confidentiality



How to Achieve Confidentiality?

Answer: Encryption or Encipherment!



"Hello, how are you"

Encryption Function

$%@#$%@@

Plaintext

Ciphertext

Key

Addit nation

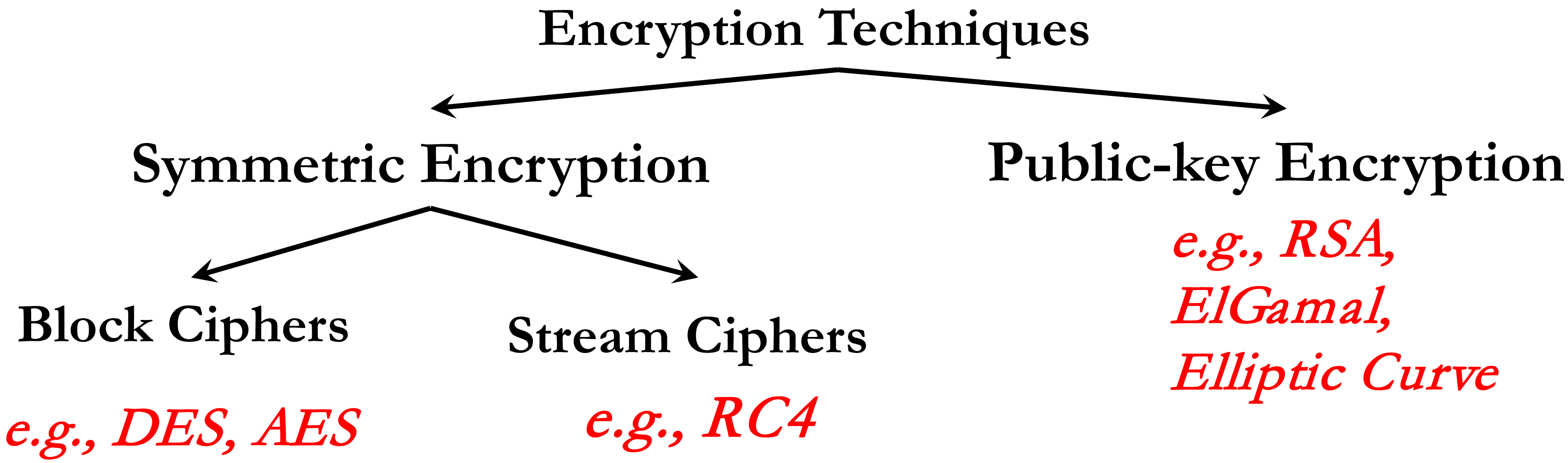
Cryptanalysis

Decryption Function

"Hello, how are you"

$%@#$%@@

Types of Encryption Techniques



Encryption Techniques

Symmetric Encryption

Public-key Encryption

e.g., RSA, ElGamal, Elliptic Curve

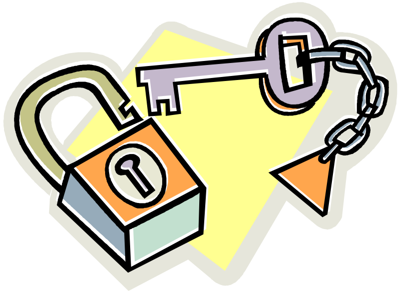
Block Ciphers

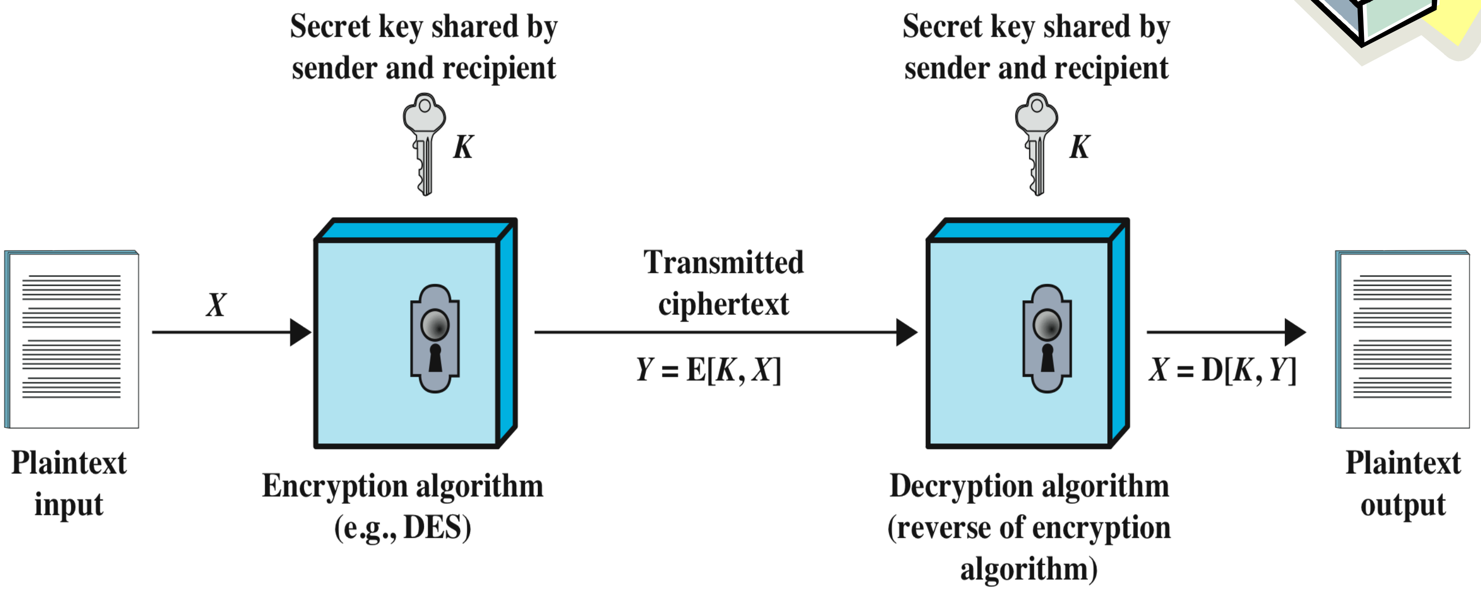
e.g., DES, AES

Stream Ciphers

e.g., RC4

Symmetric Encryption

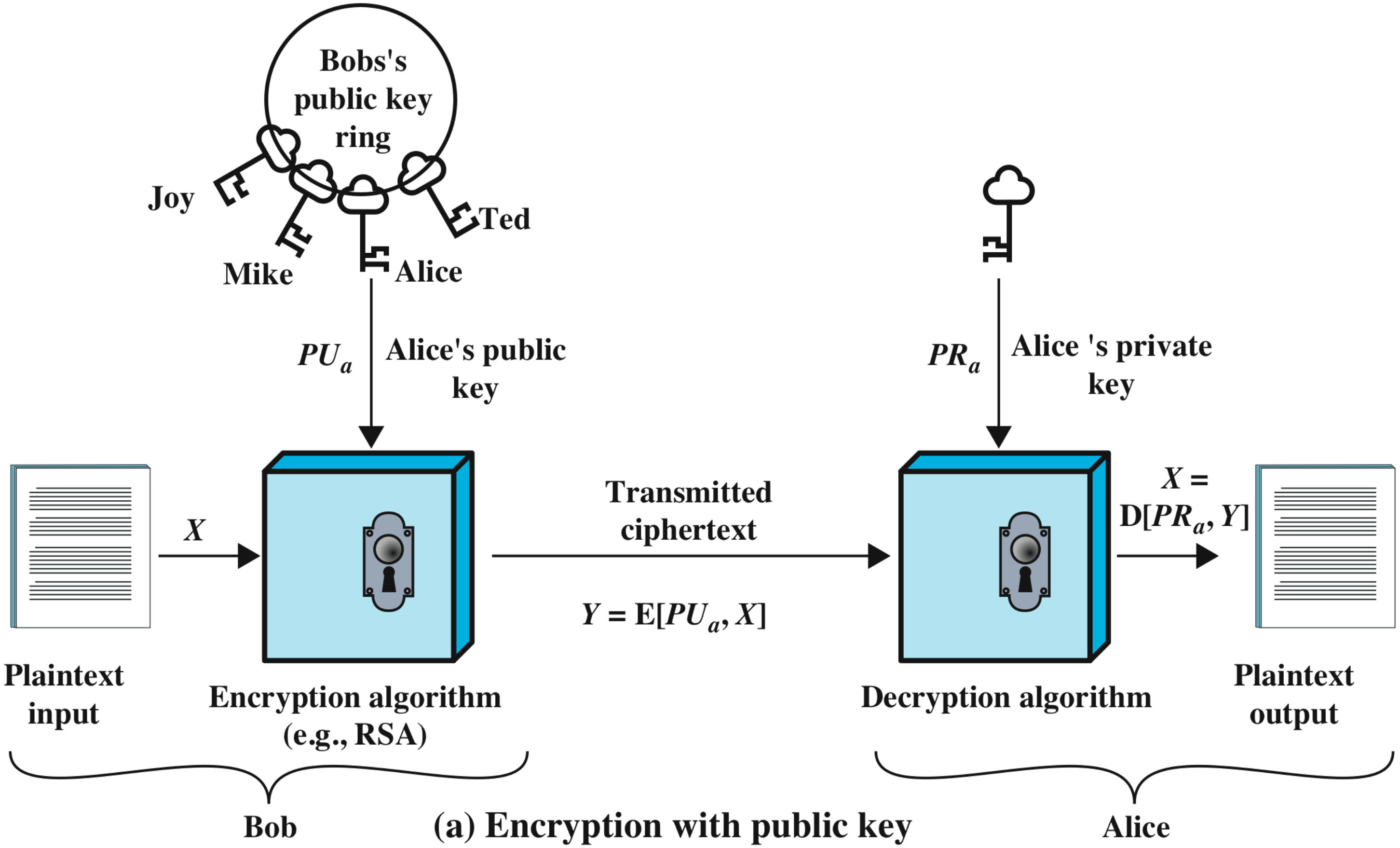




Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E[K, X]
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

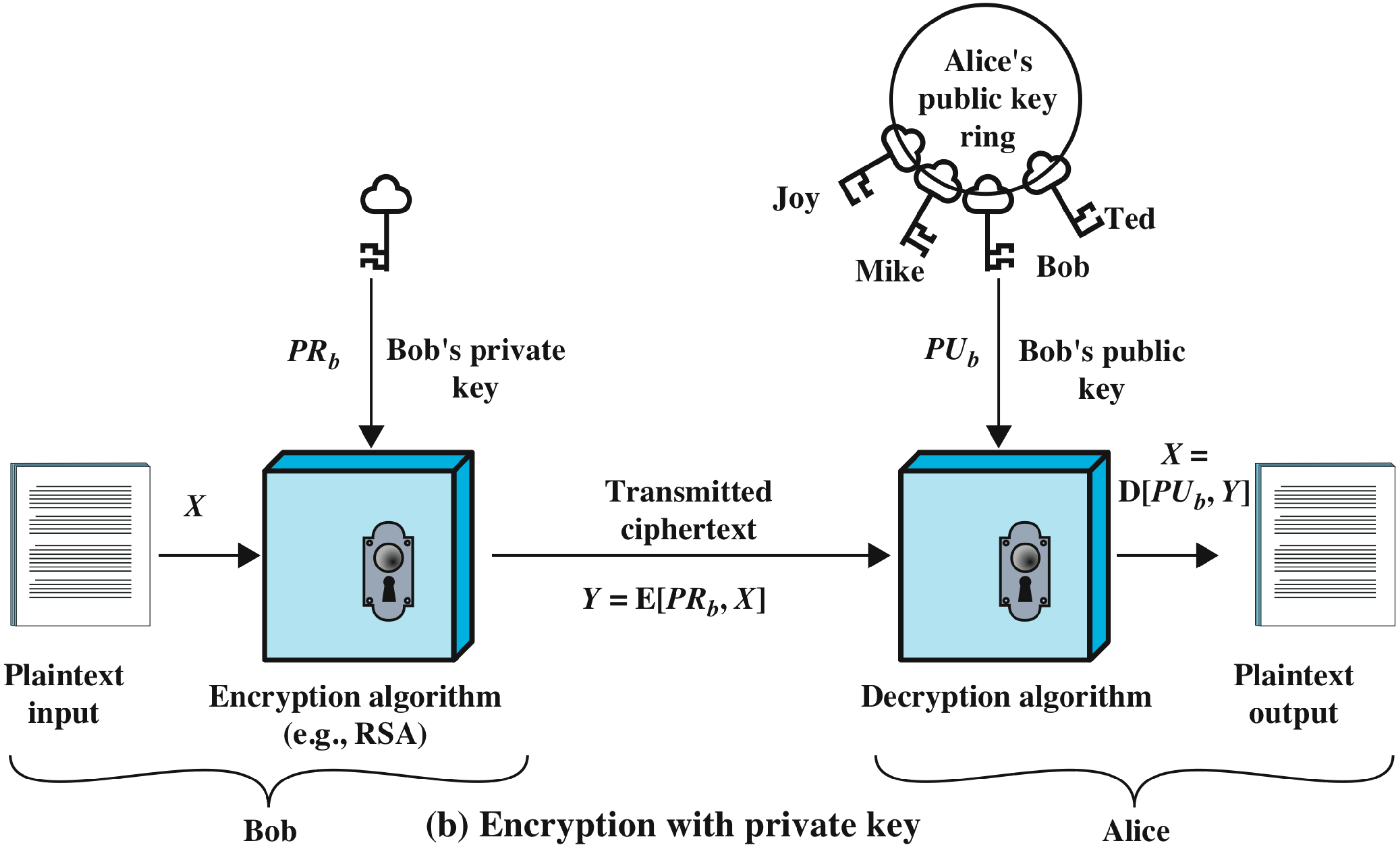
Most symmetric encryption algorithms employ a sequence of permutations and substitution operations (dependent on the symmetric key)

Public-Key or Asymmetric Encryption



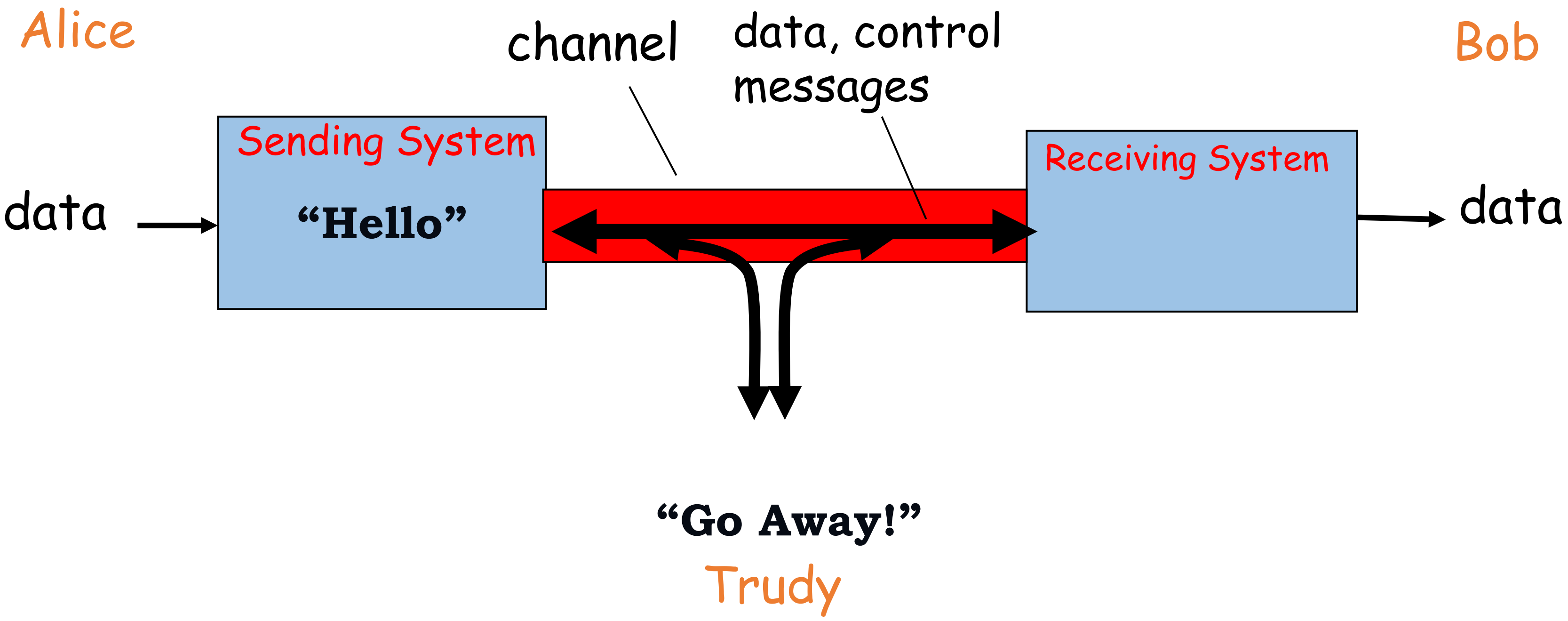
(a) Encryption with public key

Public-Key or Asymmetric Encryption



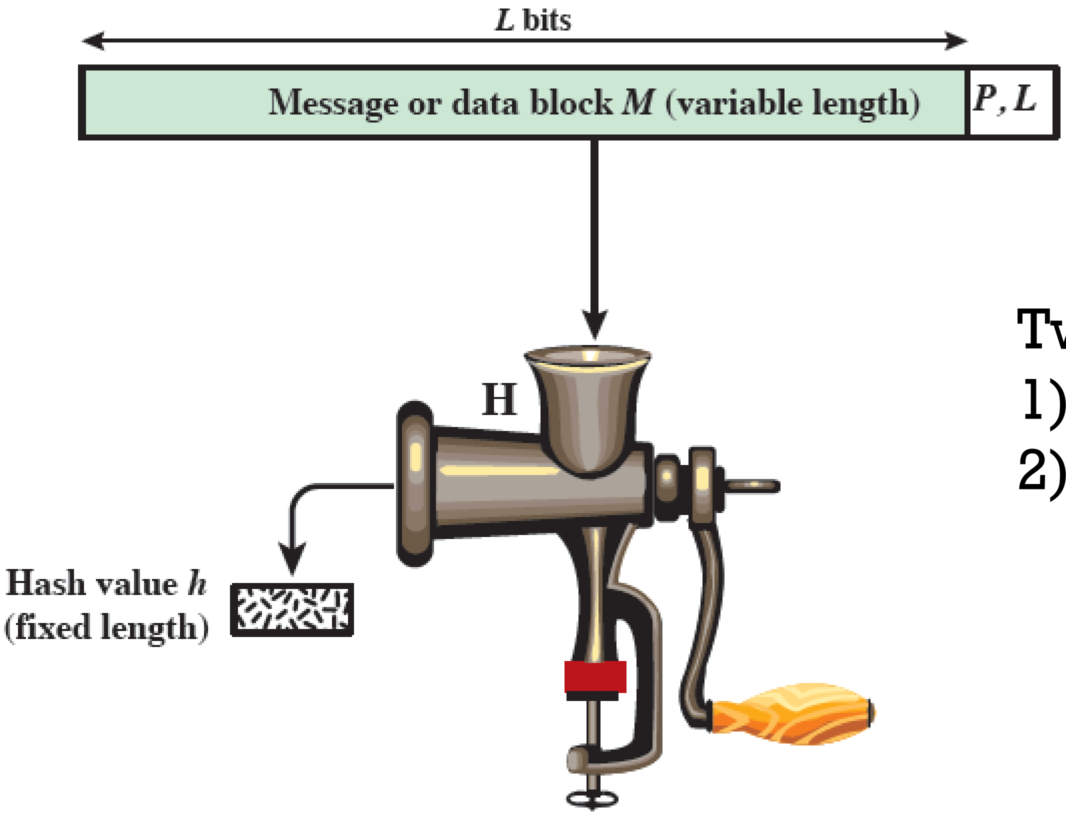
(b) Encryption with private key

Integrity


Alice
channel
data, control messages
Bob
Sending System
"Hello"
Receiving System
data
data
"Go Away!"
Trudy

How to Achieve Integrity?

Answer: Hash Functions



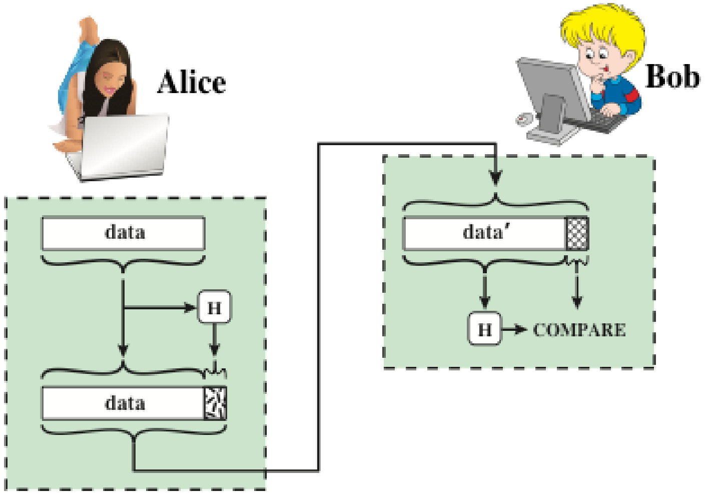
P, *L* = padding plus length field

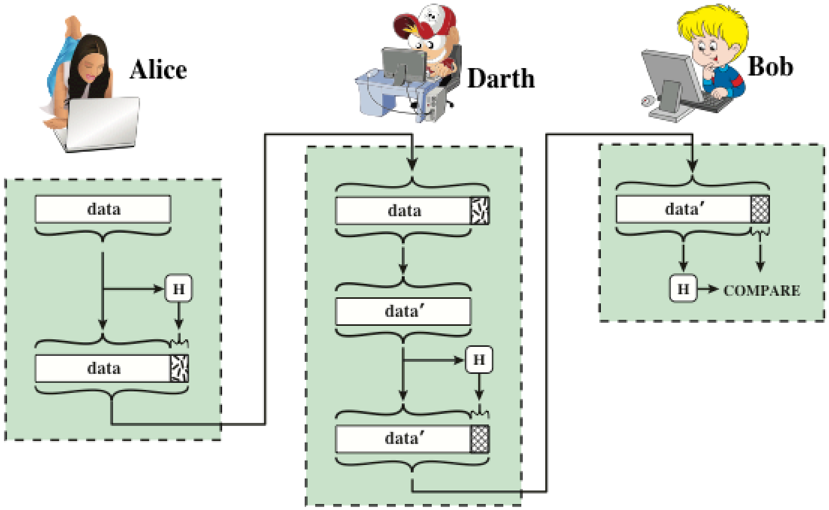
Two Important Properties:

1) One-way
2) Collision Resistance

How to Achieve Integrity?

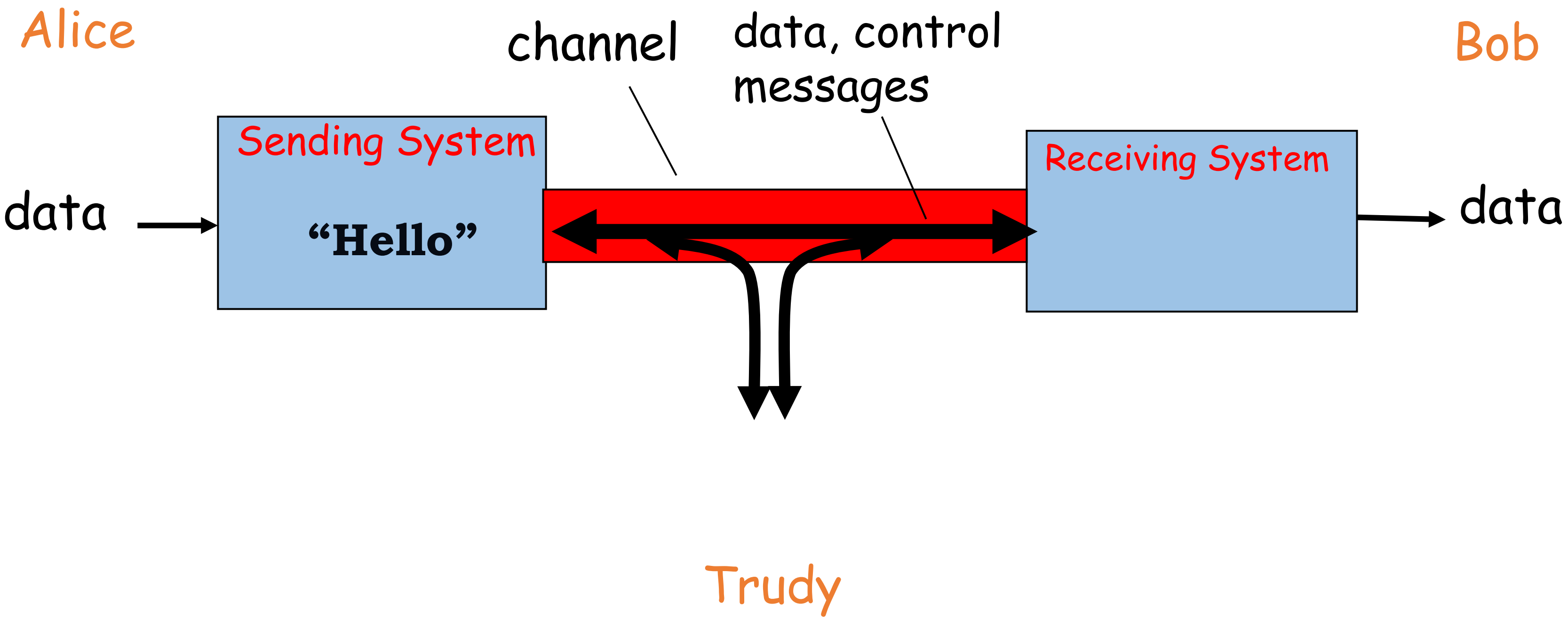
How to Achieve Message Integrity using Hash Functions?





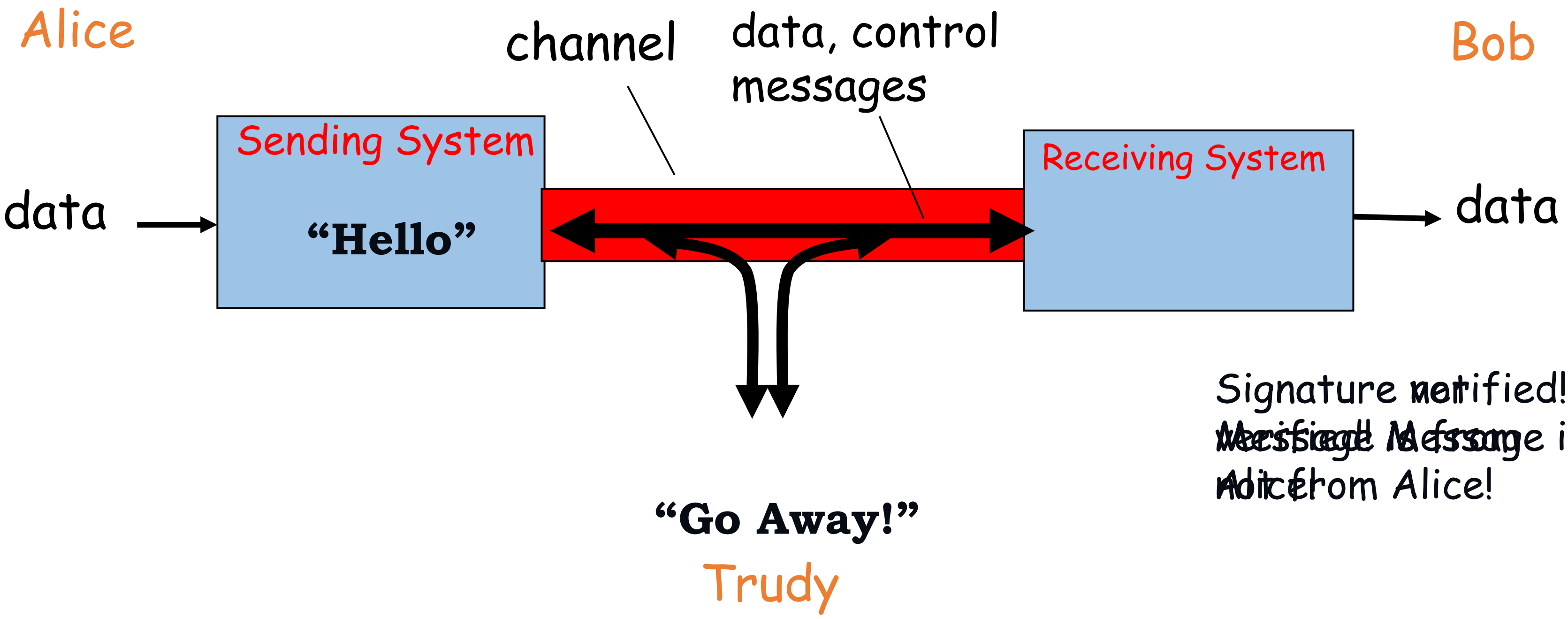
Hash functions are used to construct complex integrity checking functions called **Keyed Hash Functions** or **Message Authentication Codes (MAC)**

Availability



- Attacks on Availability are also called **Denial of Service (DoS)** Attacks.
- One protection strategy is to detect DoS attacks (and attackers) and isolate the attacker (and source of the attack).

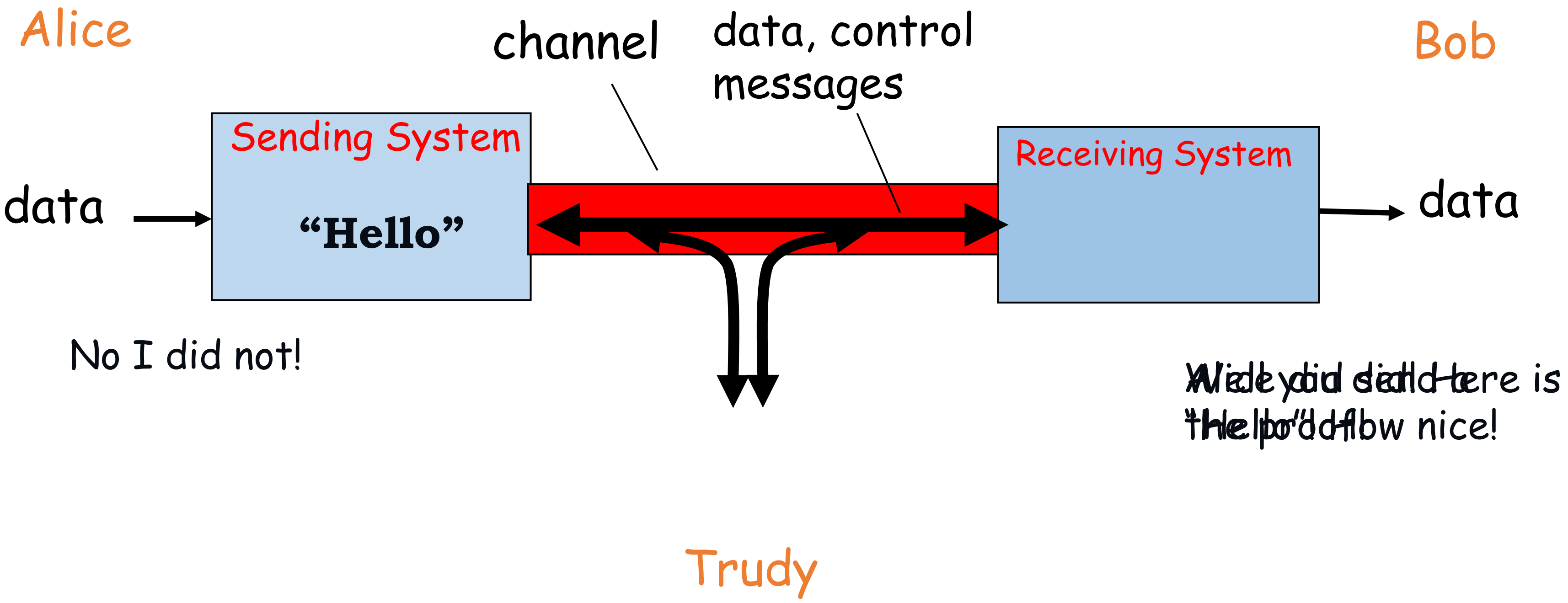
Authenticity



Signature not verified! Message is not from Alice!

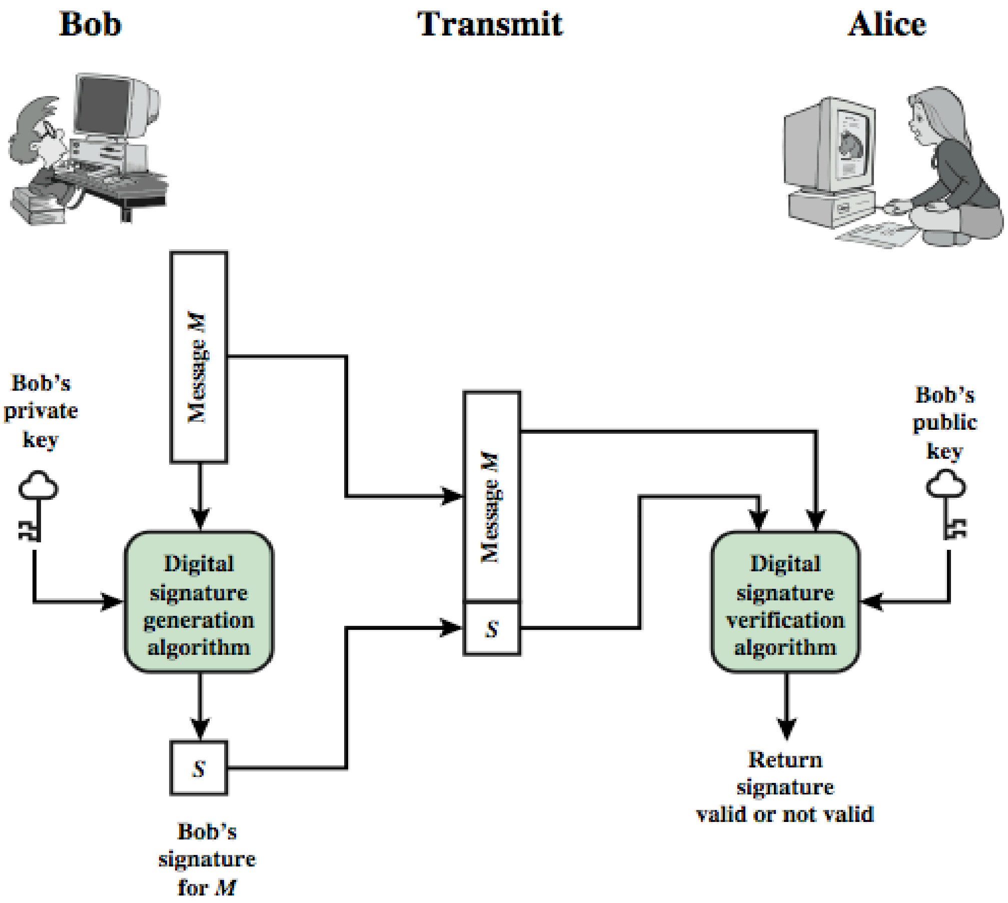
Signature verified! Message from Alice!

Accountability

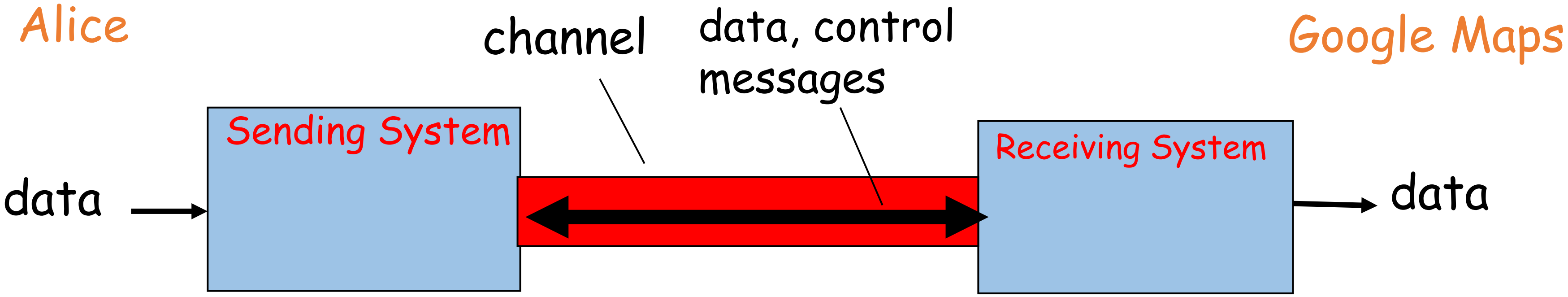


How to Achieve Authentication and Accountability?

Answer: Digital Signatures!


Bob
Transmit
Alice
Message M
Bob's private key
Digital signature generation algorithm
S
Bob's signature for M
Message M
S
Bob's public key
Digital signature verification algorithm
Return signature valid or not valid

Privacy



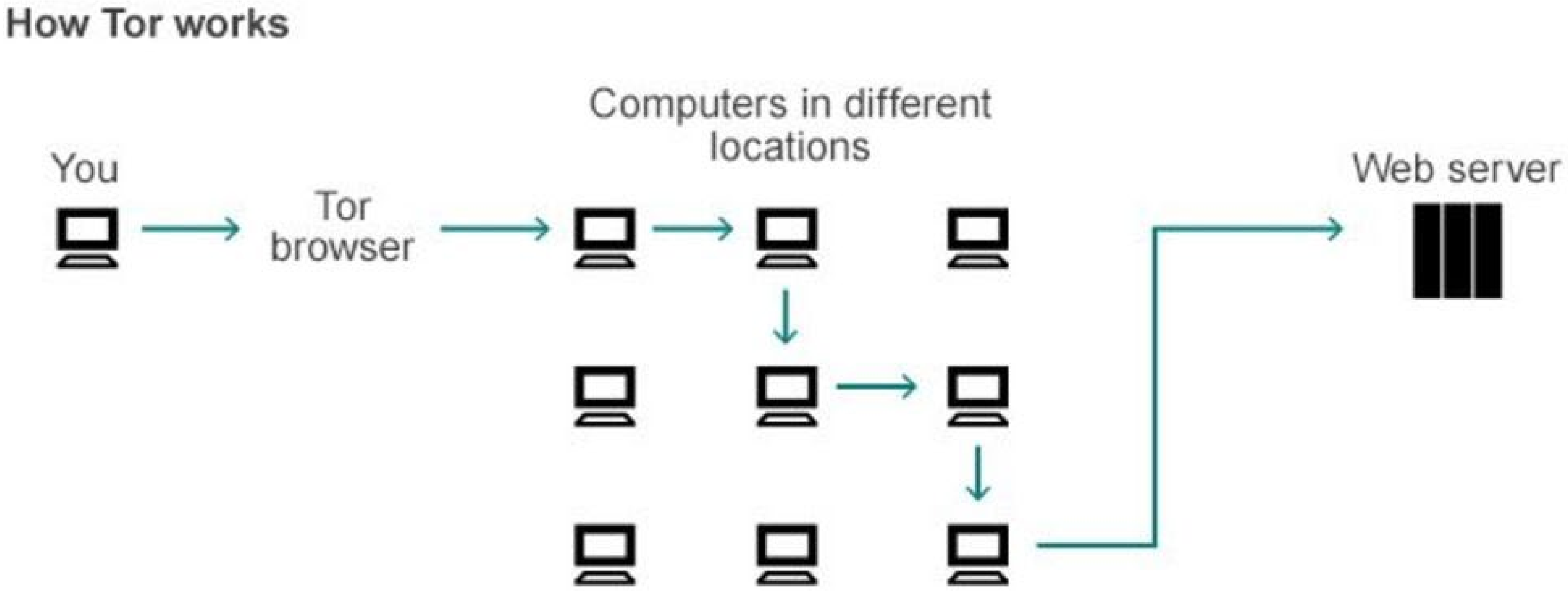
“What are the Pizza joints near Timesquare?”

Papa Johns & Dominos

Hmmm…Alice is in NewYork City!

How to Achieve Privacy?

Answer: Anonymization Services (e.g., The Onion Router or ToR)!



Questions