NETWORK **SECURITY**

CPSC 441 - Tutorial 14

Winter 2018

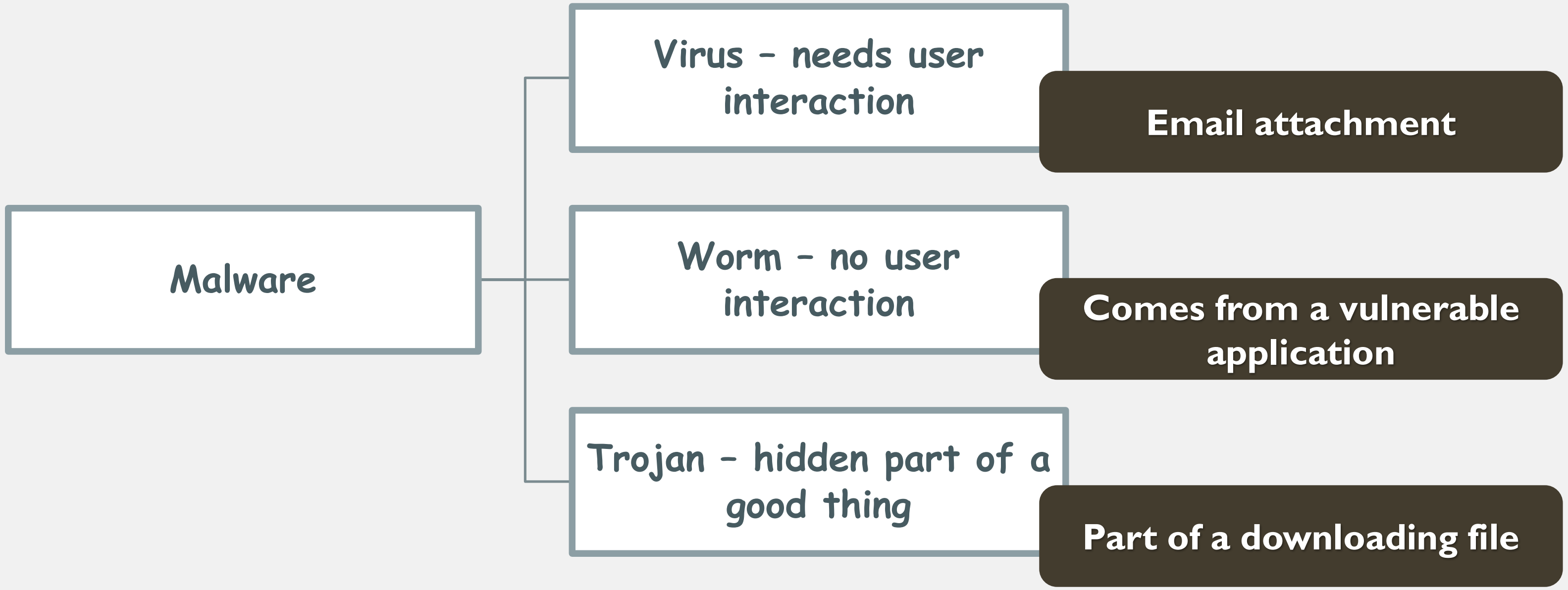
UNIVERSITY OF CALGARY

WHAT IS NETWORK SECURITY?

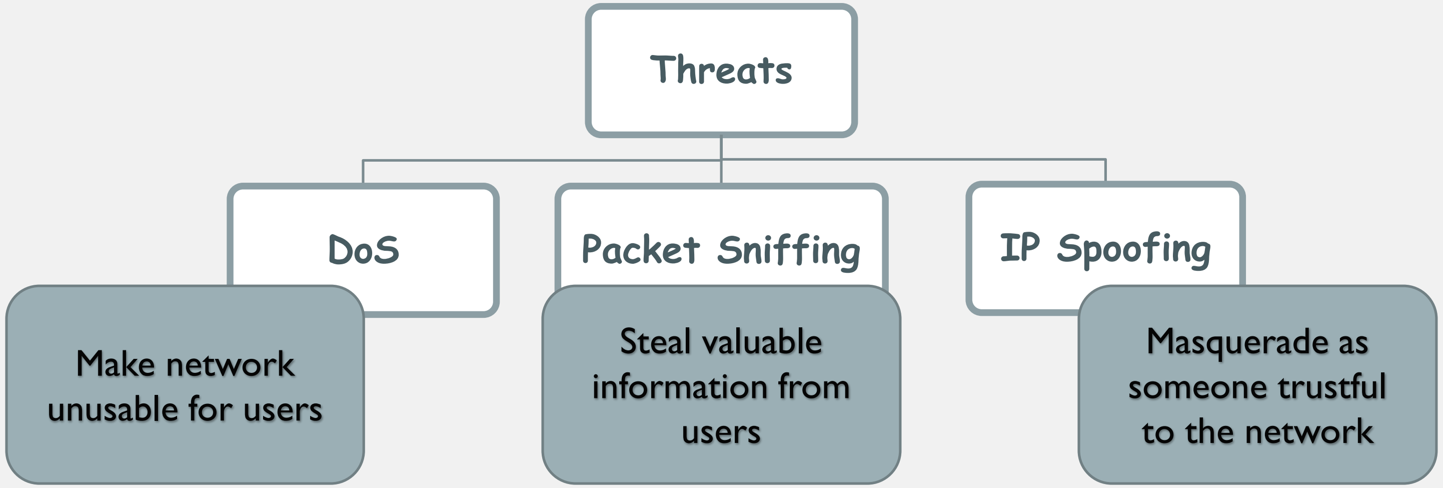
- Why internet is **not safe**?
  - Internet was originally invented for a group of "**good guys**" (mutually trusting users)
  - It **expanded** over time and many things have been added to it
  - Security vulnerabilities in all layers!
- Network security is about:
  - How "bad guys" can **attack** computer networks
  - How can we **detect** attacks and **defend** against them
  - How to design **architectures immune** to attacks

MALWARE

- **Self-replicating** malicious software that intend to damage the host computer


Malware
Virus – needs user interaction
Email attachment
Worm – no user interaction
Comes from a vulnerable application
Trojan – hidden part of a good thing
Part of a downloading file

SECURITY **THREATS**

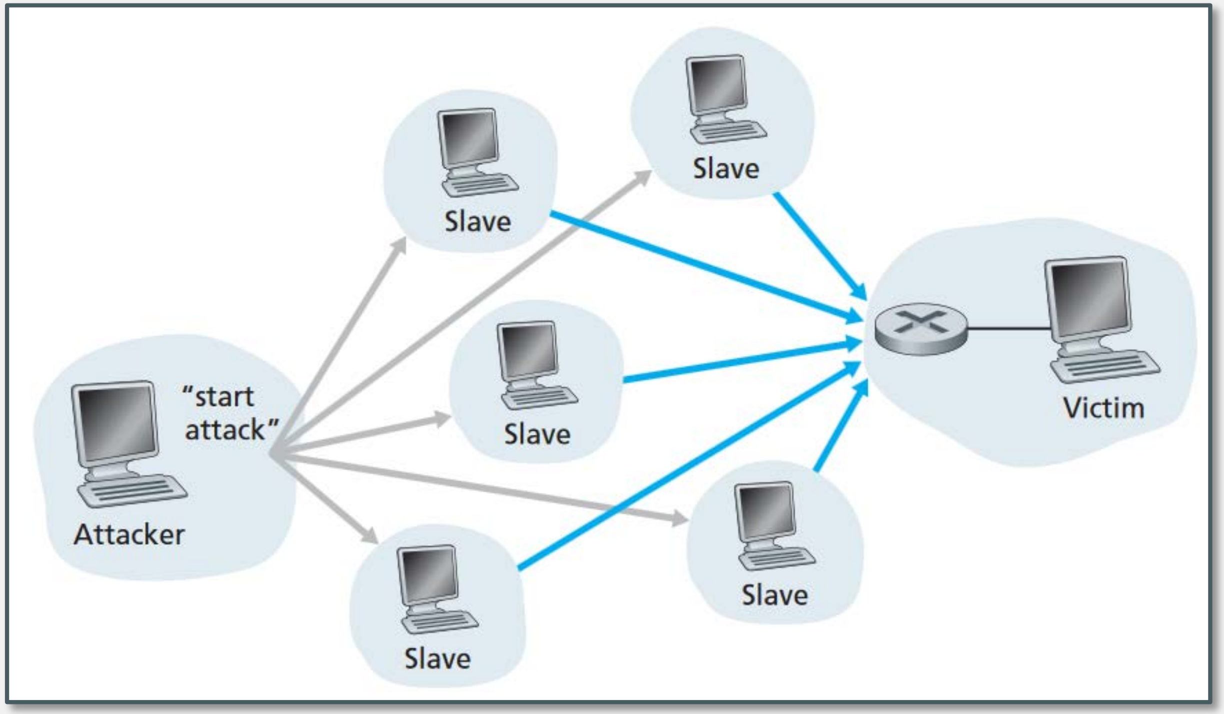

Threats
DoS
Packet Sniffing
IP Spoofing
Make network unusable for users
Steal valuable information from users
Masquerade as someone trustful to the network

UNIVERSITY OF CALGARY

DOS ATTACK

- Denial of Service:
  - Attackers make resources (servers, links, routers, hosts) unavailable too legitimate traffic by overwhelming them with bogus traffic

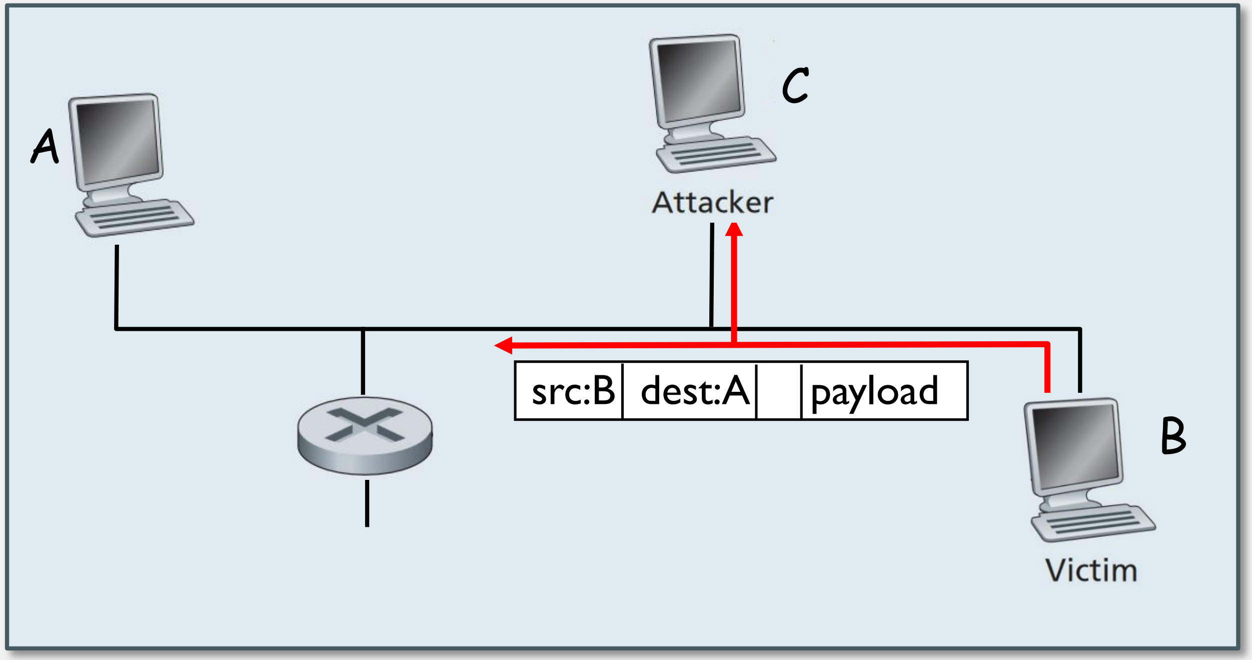
- Distributed Denial of Service (DDoS):
  - If the attacker uses only one host to inject his traffic to the network, an upstream router can detect the attack and block the traffic
  - The attacker can control multiple hosts (slaves) and each of them will generate the traffic



DDoS Attack

PACKET SNIFFING

- Happens in a **broadcast** media (shared **Ethernet** and **wireless**)
- Attacker reads the packet and its data (could be password!) without being detected
- Wireshark is a packet sniffer!

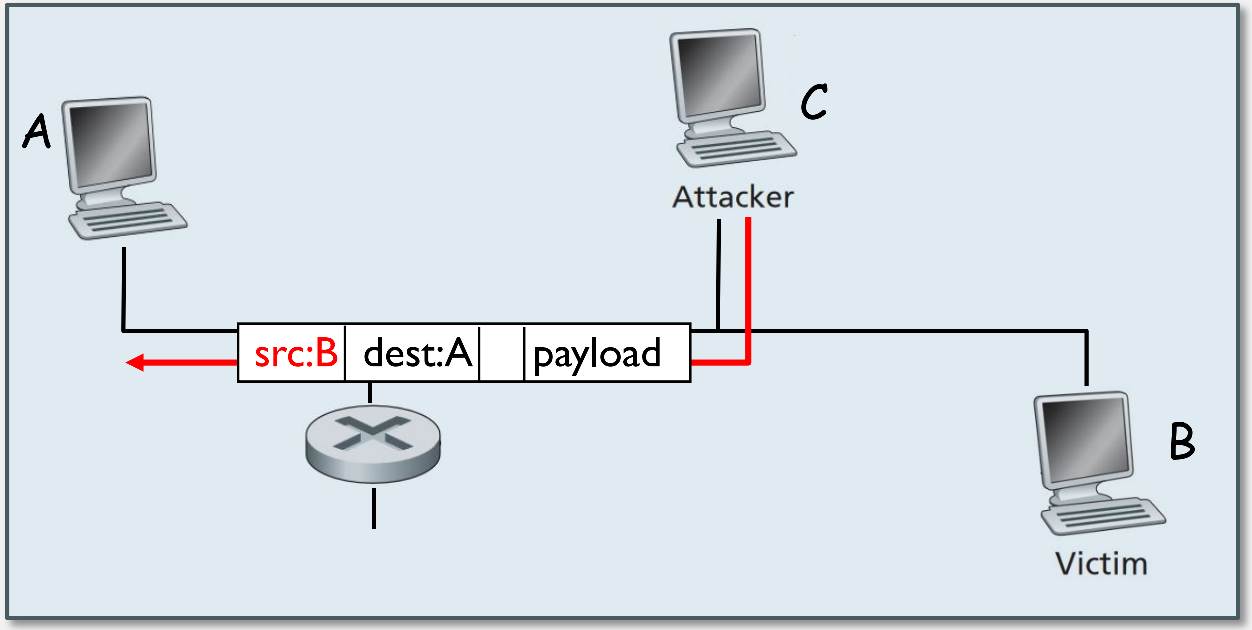


Packet Sniffing Attack

IP SPOOFING

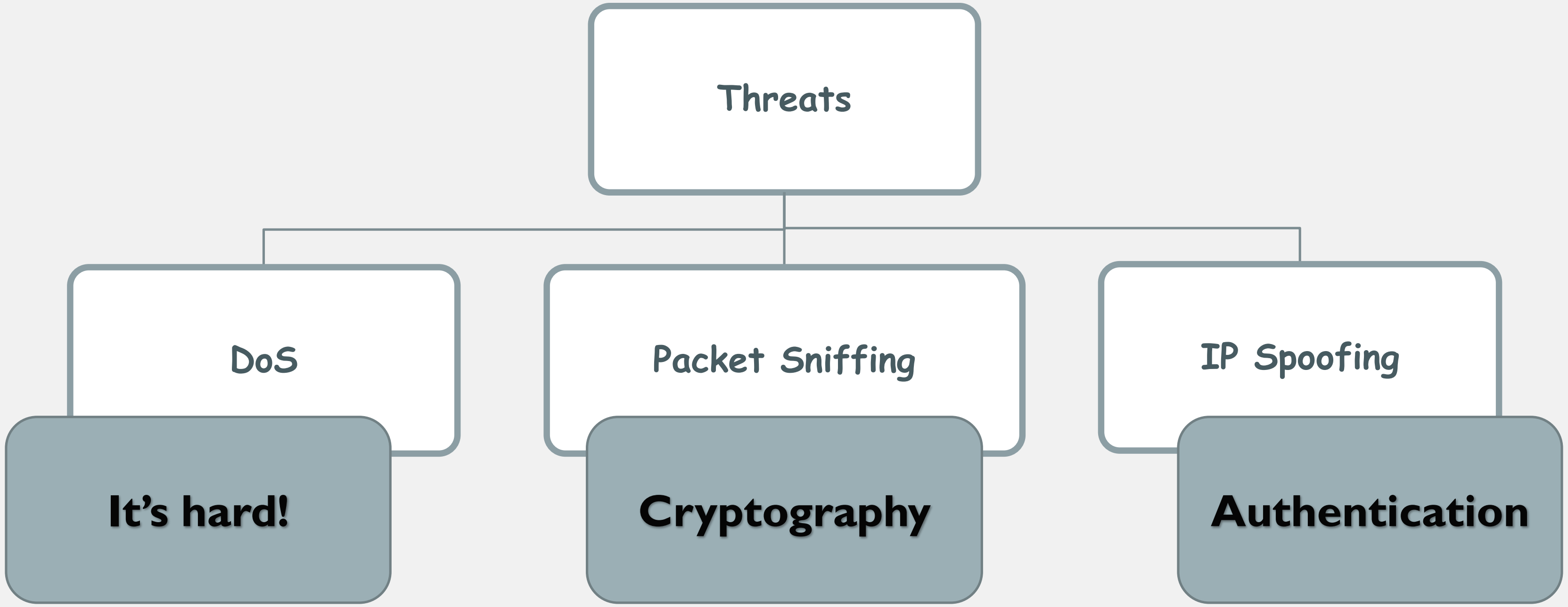
- Attacker sends packets with the IP address of a trusty host to manipulate the receiver
    - Sending a request to a server
    - Changing routing tables of a router with some command embedded in the packet's content

- End-to-End Authentication can solve the problem



IP Spoofing Attack

HOW TO **DEFEND**?



Threats

DoS

It’s hard!

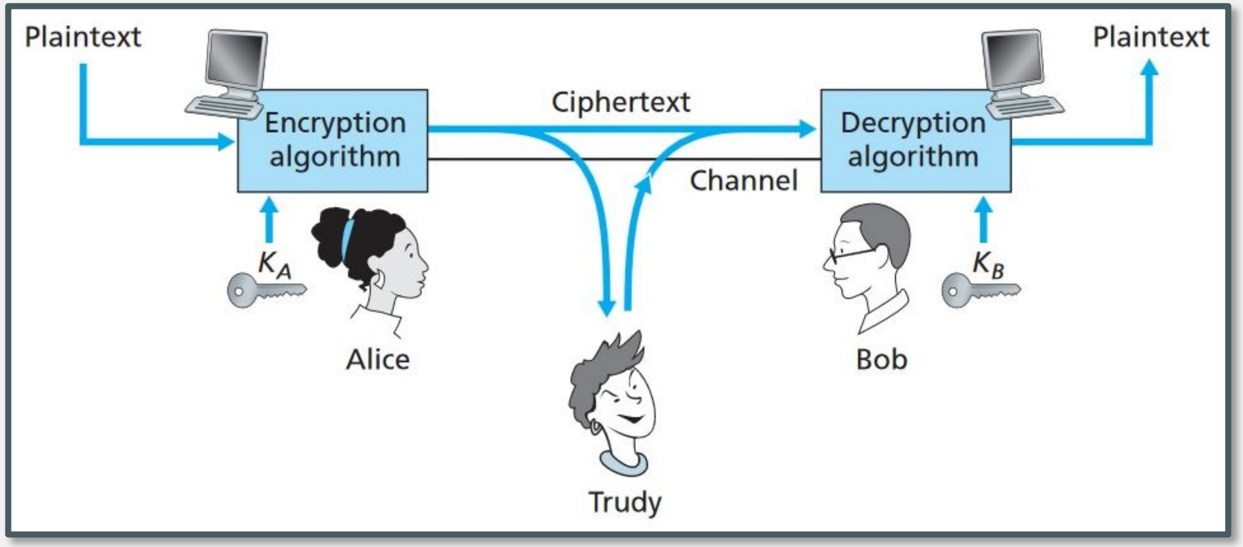
Packet Sniffing

Cryptography

IP Spoofing

Authentication

CRYPTOGRAPHY

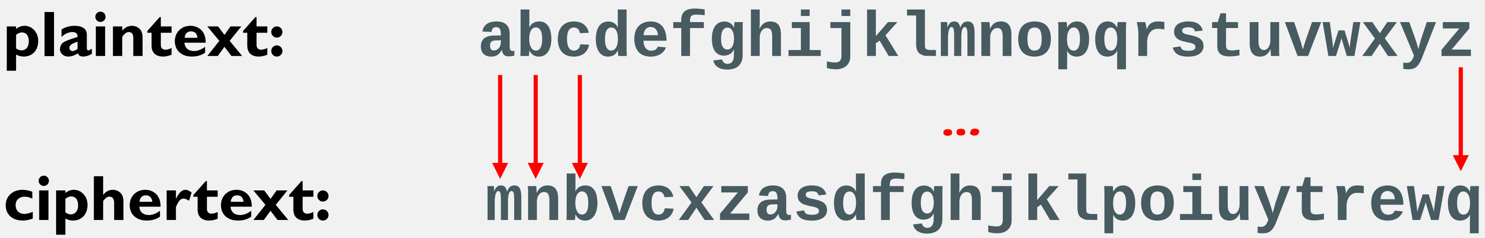


Cryptography Process

CRYPTOGRAPHY **EXAMPLE**

- Substitution Cipher:

Key is the mapping from the set of 26 letters to the set of 26 letters



plaintext: `abcdefghijklmnopqrstuvwxyz`

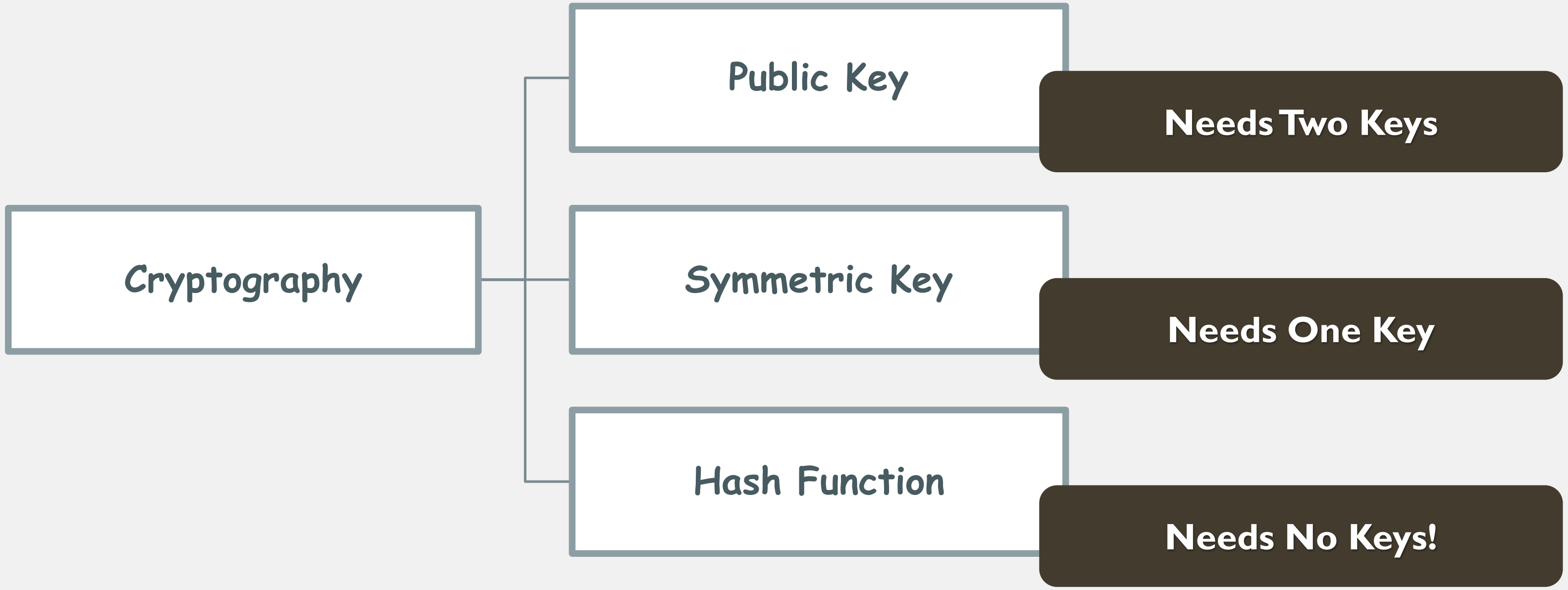
...

ciphertext: `mnbvcxzasdfghjklpoiuytrewq`

plaintext: `bob. i love you. alice`

ciphertext: `nkn. s gktc wky. mgsbc`

TYPES OF CRYPTOGRAPHY



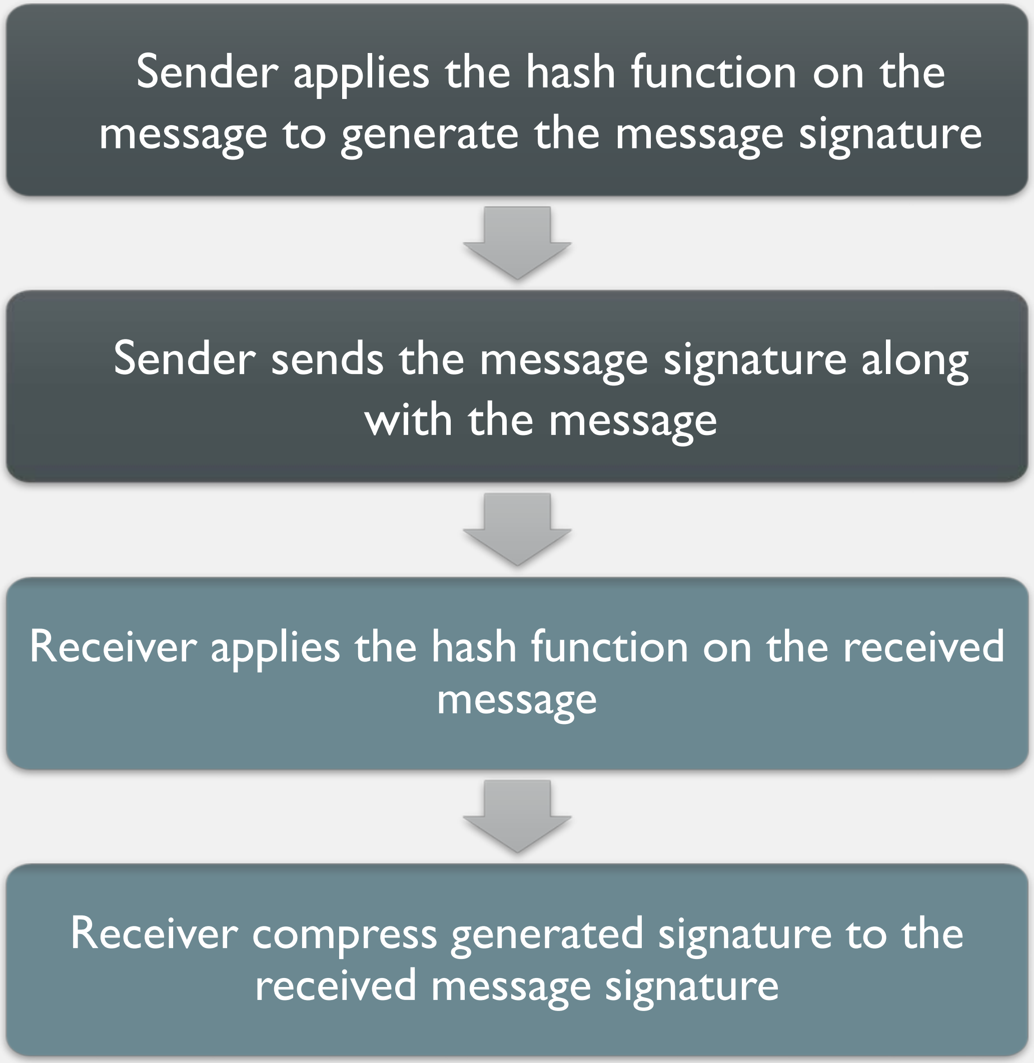
Cryptography

- Public Key
  - Needs Two Keys
- Symmetric Key
  - Needs One Key
- Hash Function
  - Needs No Keys!

HASH FUNCTION

- Hash function **H( )** takes an **arbitrary-length** message as input and outputs a **fixed-length** string called **message signature**
- Useful for checking **Message Integrity**

- Hash function properties:
  - Easy to calculate
  - Irreversibility: m cannot be determined from $H(m)$
  - Collision resistant: it is computationally difficult to produce m and m' such that $H(m) = H(m')$
  - Seemingly random output



Sender applies the hash function on the message to generate the message signature

Sender sends the message signature along with the message

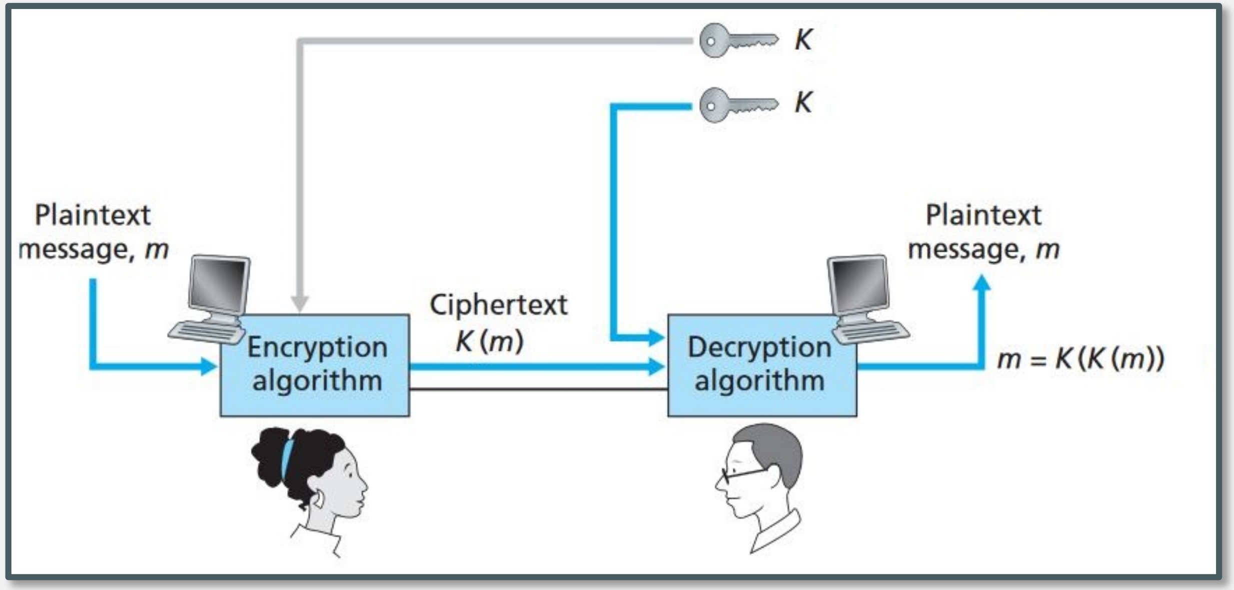
Receiver applies the hash function on the received message

Receiver compress generated signature to the received message signature

SYMMETRIC KEY

- **Bob** and **Alice** share the same (symmetric) key K

- Bob and Alice must know the shared secret key
  - How do they agree on it if they've never met each other?
  - How they can **share** the secret key?

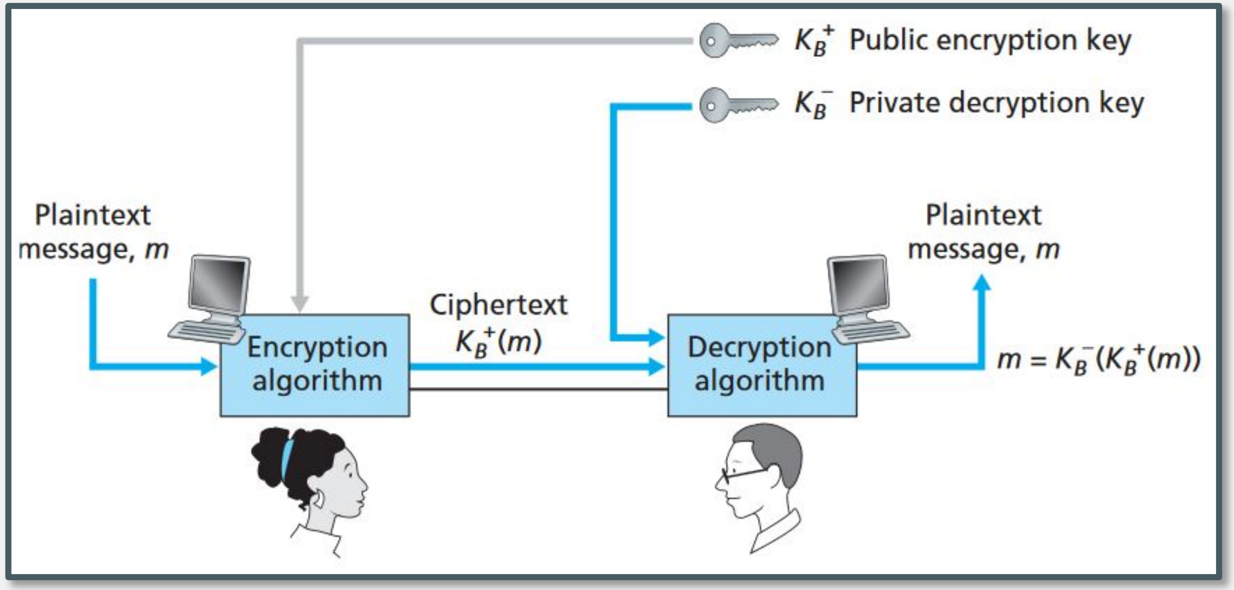


Symmetric Key Encryption

UNIVERSITY OF CALGARY

PUBLIC KEY

- Bob broadcasts his public key K_B^+ in the network
- Alice uses the public key K_B^+ to encrypt the message she wants to send to Bob
- Bob Uses a private key K_B^- to decrypt the received message from Alice
  - private encryption key is known only to Bob



Public Key Encryption

UNIVERSITY OF CALGARY

AUTHENTICATION

- Digital Signature
  - Used against IP Spoofing
  - Provides non-repudiation
  - Public key encryption scheme:
    - Sender digitally signs document, using his private key
    - Recipient decrypts the signature with sender's public key for verification
  - The signature is verifiable and non-forgeable
    - Recipient can prove to someone that the sender, and no one else, must have signed the document

CPSC 526

- There's a course for the field:

  Network Systems Security (CPSC 526)

- Course Description:

  "Attacks on networked systems, tools and techniques for detection and protection against attacks including firewalls and intrusion detection and protection systems, authentication and identification in distributed systems, cryptographic protocols for IP networks, security protocols for emerging networks and technologies, privacy enhancing communication. Legal and ethical issues will be introduced."

REFERENCES

- Computer Networks: A Top Down Approach
  - Chapter 1 – section 1.6
  - Chapter 8