ELL365: Embedded Systems

Lecture on Introduction to Cyber Security

Vireshwar Kumar
CSE@IITD

February 8, 2024

Semester II
2023-2024

Agenda

- Need for Security
- Symmetric Key Cryptography
- Asymmetric Key Cryptography

Modern Embedded Systems

Smart City

Smart Home

Smart Transportation

Smart Robot

Cyber Attacks

Ukraine power cut 'was cyber-attack'[1]

Mirai botnet: How CCTV cameras almost brought down the internet[2]

Hackers remotely kill a Jeep on the highway[3]

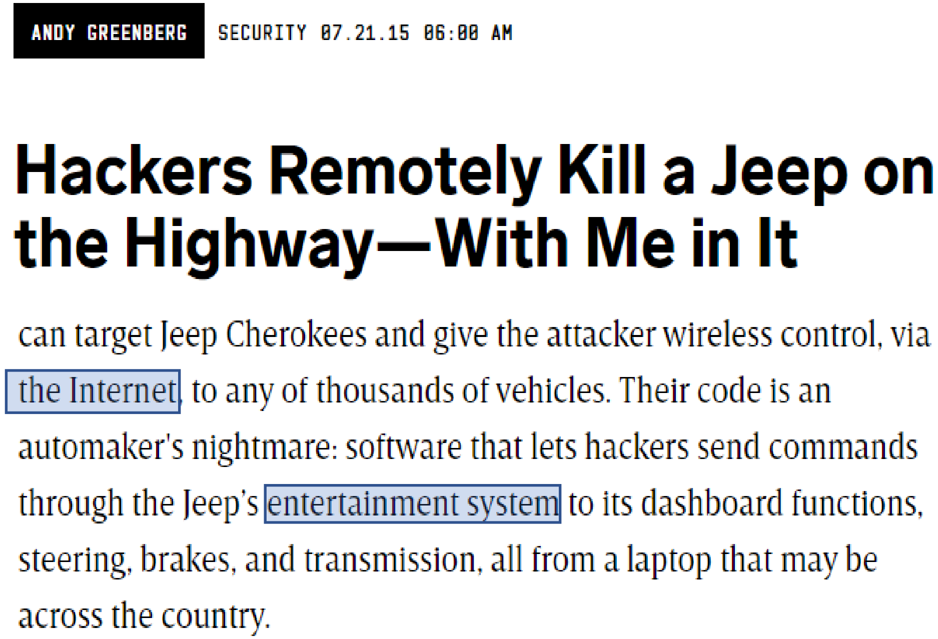
'I'm in your baby's room': A hacker took over a baby monitor[4]

Discover and mitigate security and privacy vulnerabilities

A Notorious Example

Video Link

In 2015, Jeep recalled
1.4 million cars[2]



ANDY GREENBERG SECURITY 07.21.15 06:00 AM

Hackers Remotely Kill a Jeep on the Highway—With Me in It

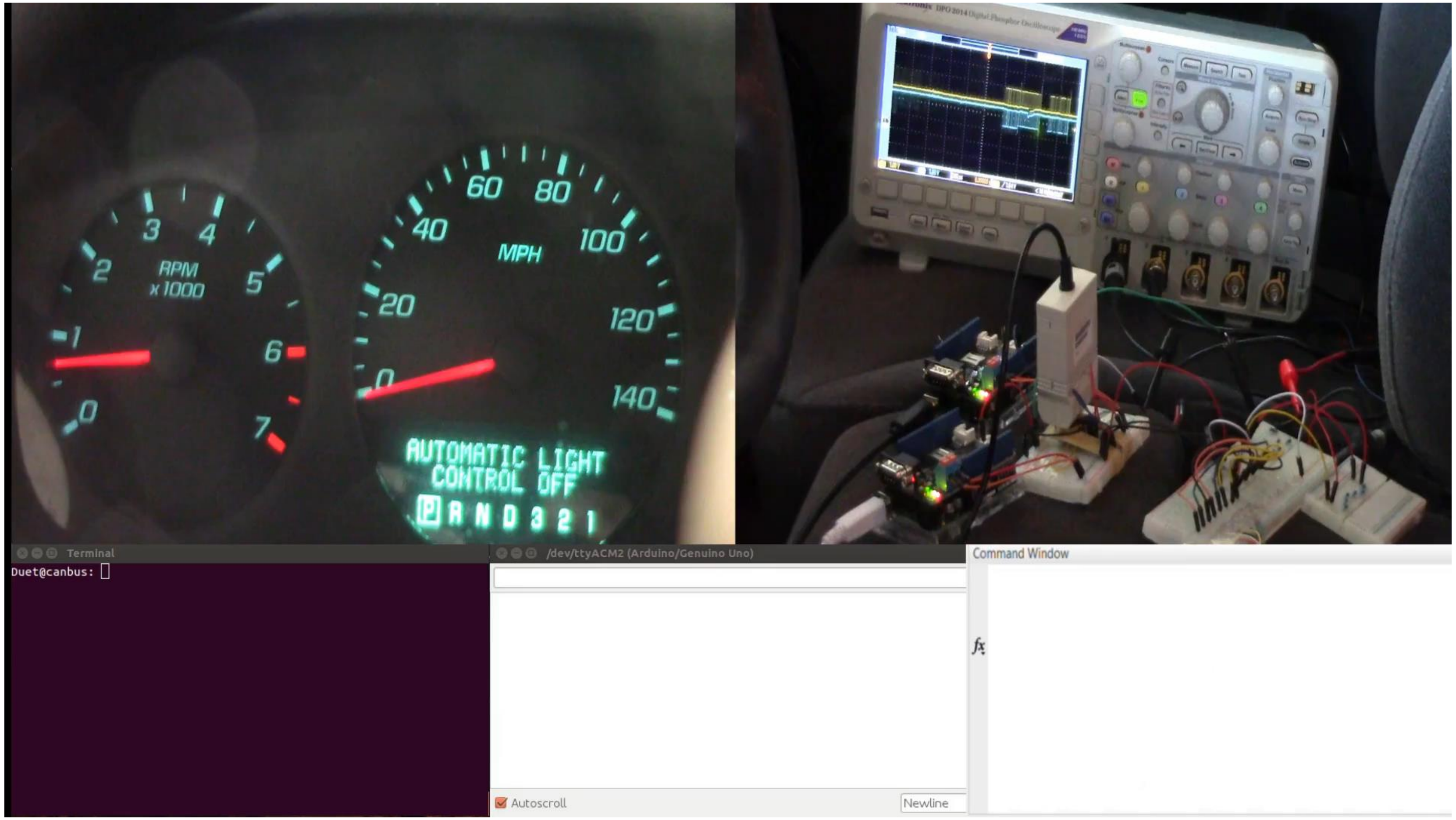
can target Jeep Cherokees and give the attacker wireless control, via the Internet, to any of thousands of vehicles. Their code is an automaker's nightmare: software that lets hackers send commands through the Jeep's entertainment system to its dashboard functions, steering, brakes, and transmission, all from a laptop that may be across the country.

Maintenance is 100X
costlier than design[3]

[2] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[3] https://www.ibm.com/downloads/cas/D8LEB3AQ

Demo: Compromising RPM Meter



```
Duet@canbus: 
```

Required Tools

Real Car (2010 Impala)
Custom Connectors
Arduino Boards
Oscilloscope

Required Skills

Reverse-Engineering
Application-Layer Protocol
MAC-Layer Protocol
Physical-Layer Protocol
Machine Learning

[Video Link]

Demo: Spoofing Information from Oura Ring

Video Link

Fundamental Security Objectives

- Confidentiality
  - Preserving restrictions on information access and disclosure
  - Procedure: Encryption

- Integrity
  - Guarding against improper information modification and sender’s authenticity
  - Procedure: Authentication

Cat-and-Mouse Game

- Defender (enable secure information flow between a sender and receiver)
  - Consider the threat model
  - Consider all potential vulnerabilities

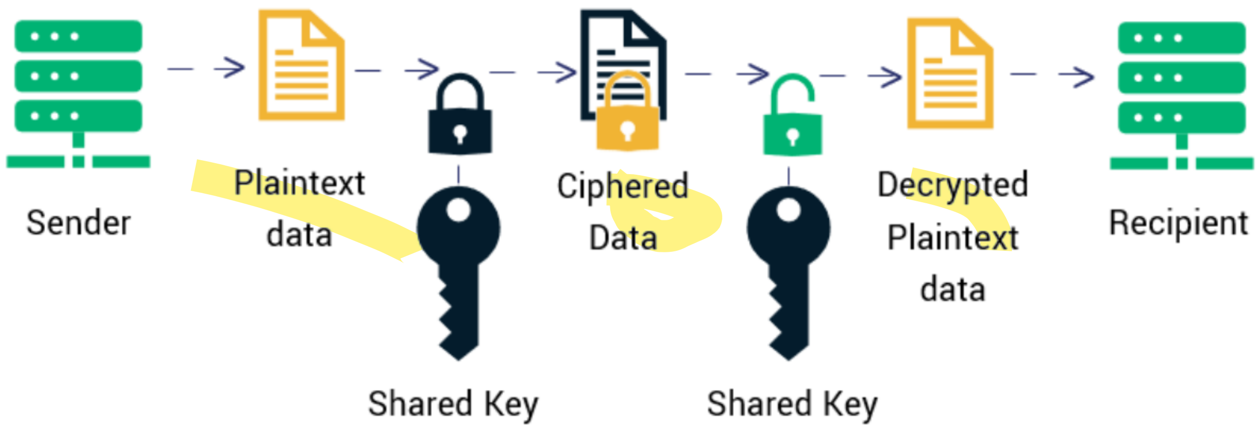
- Attacker (eavesdrop, intercept and/or forge messages)
  - Has full information about the defense mechanism
  - No knowledge of an information stored by the sender and/or receiver
  - Aims to find one vulnerability in the defense mechanism

Security Procedures

- Symmetric Key Cryptography
  - One key shared between the sender and receiver

- Asymmetric Key Cryptography
  - Two keys at the sender and two keys at the receiver

Symmetric Encryption



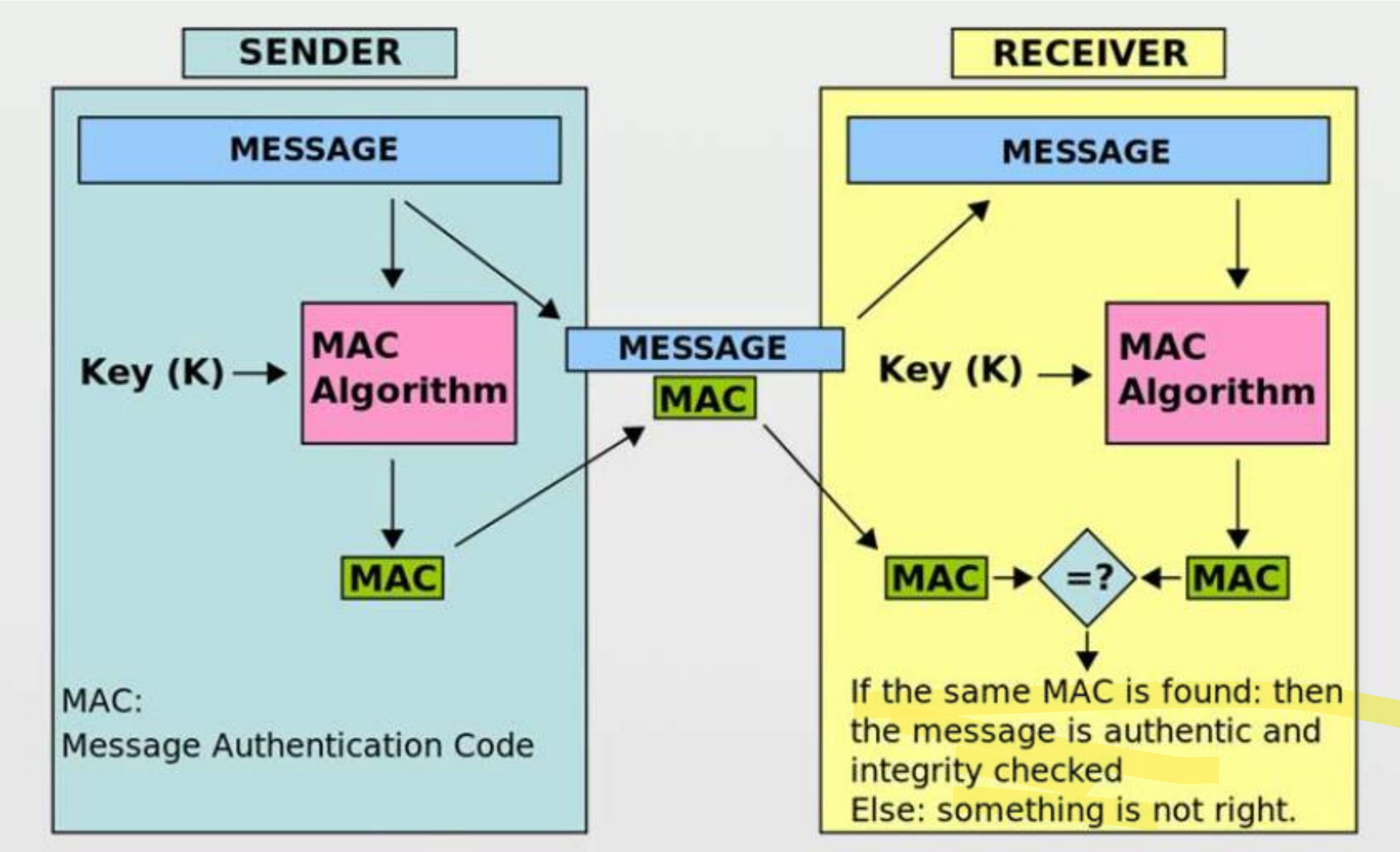
Advanced Encryption Standard (AES)

- State-of-the-art block cipher

- Key sizes – 128 bits and 256 bits

- Demonstration and Discussion
    - https://www.youtube.com/watch?v=evjFwDRTmV0

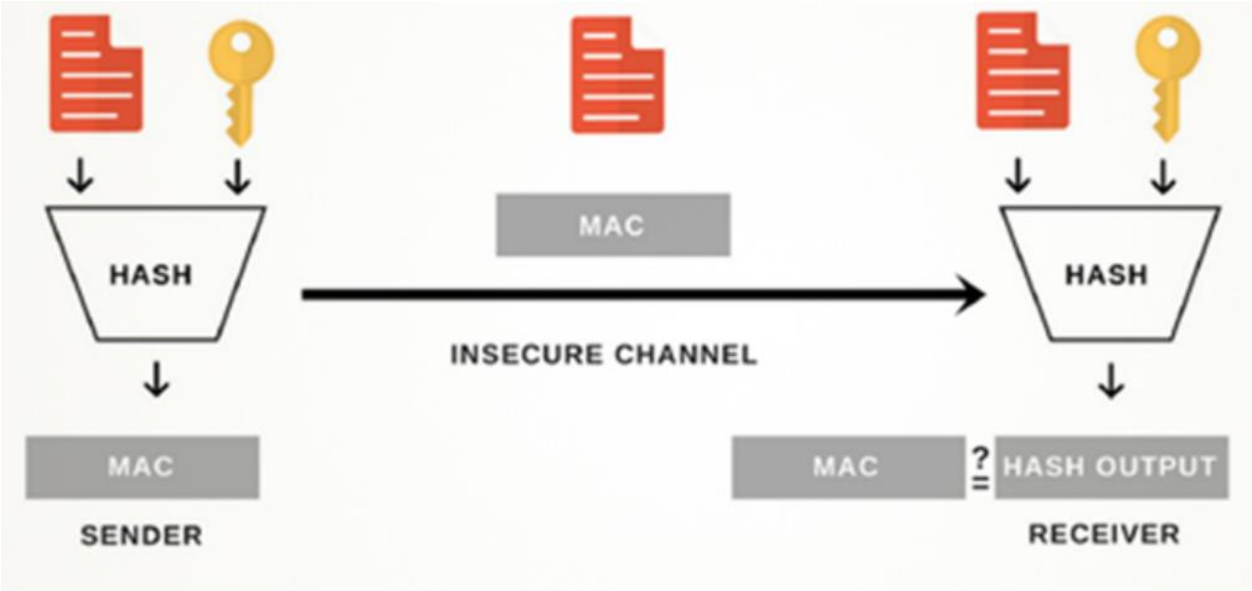
Message Authentication Code (MAC)



MAC:
Message Authentication Code

If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.

Hash-based MAC



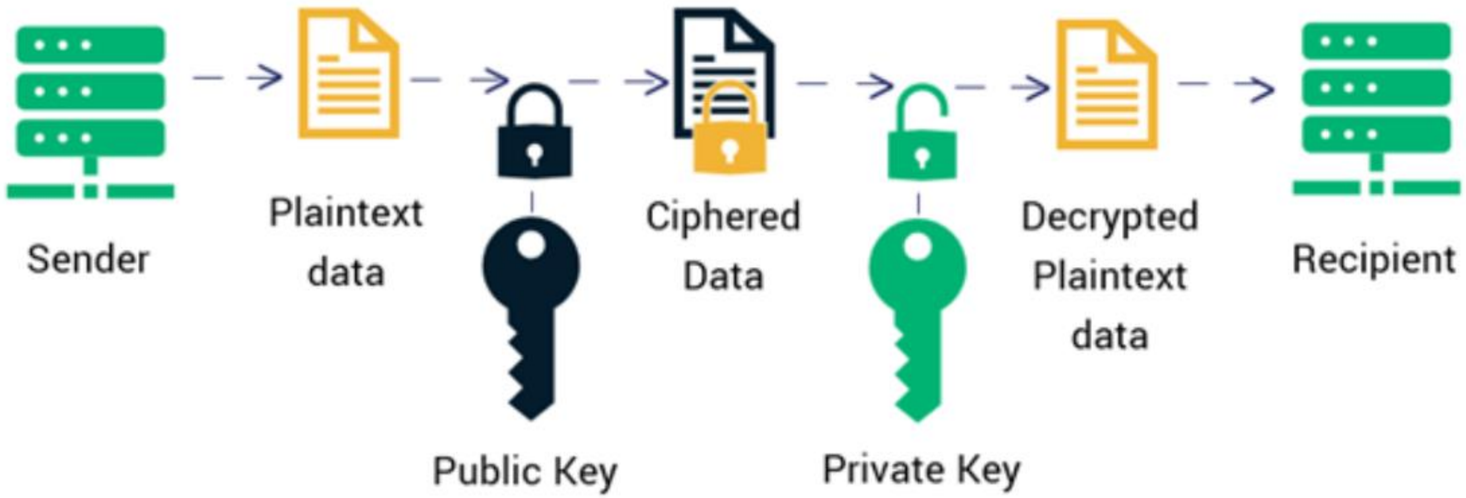
Asymmetric-Key Cryptography

- At the start, how to share the secret/symmetric key?

- How to encrypt if there is no shared key?

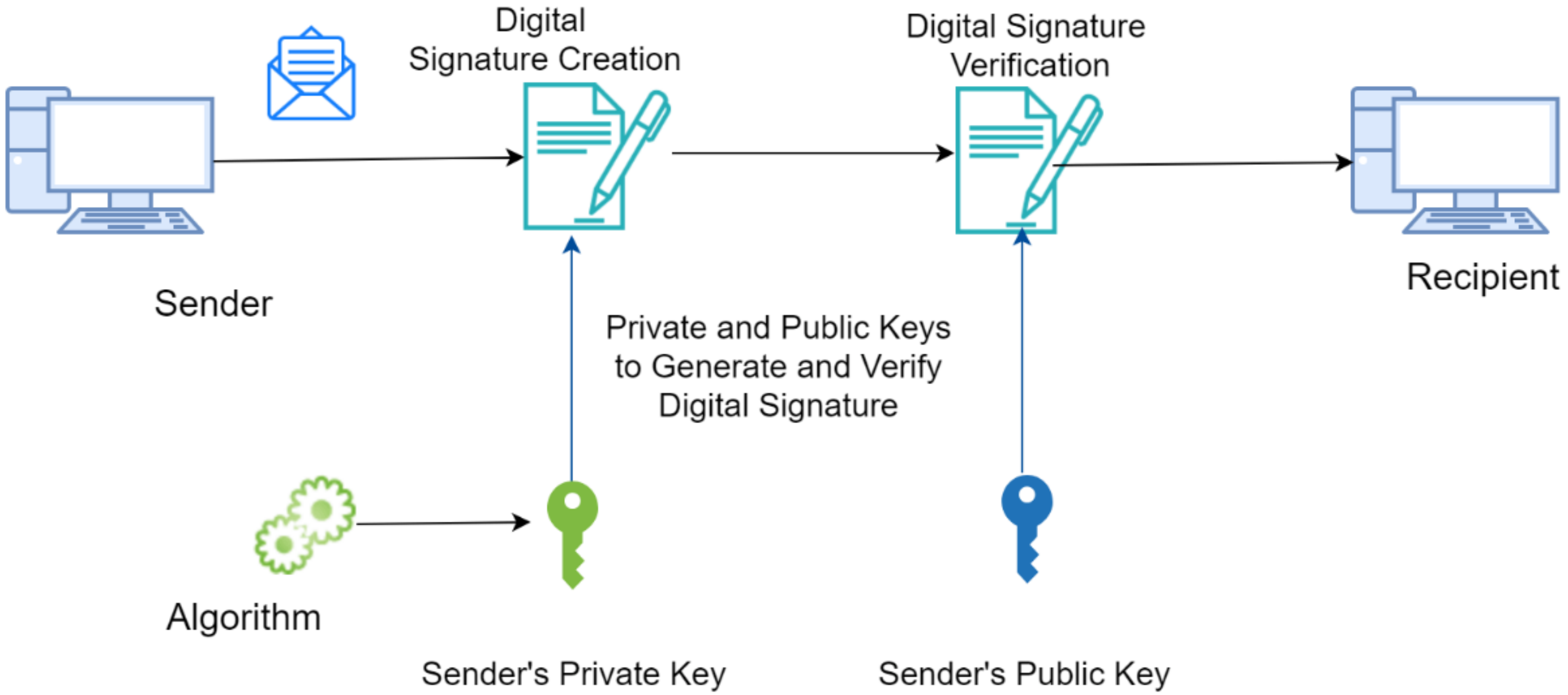
- How to authenticate if there is no shared key?

Public Key Encryption

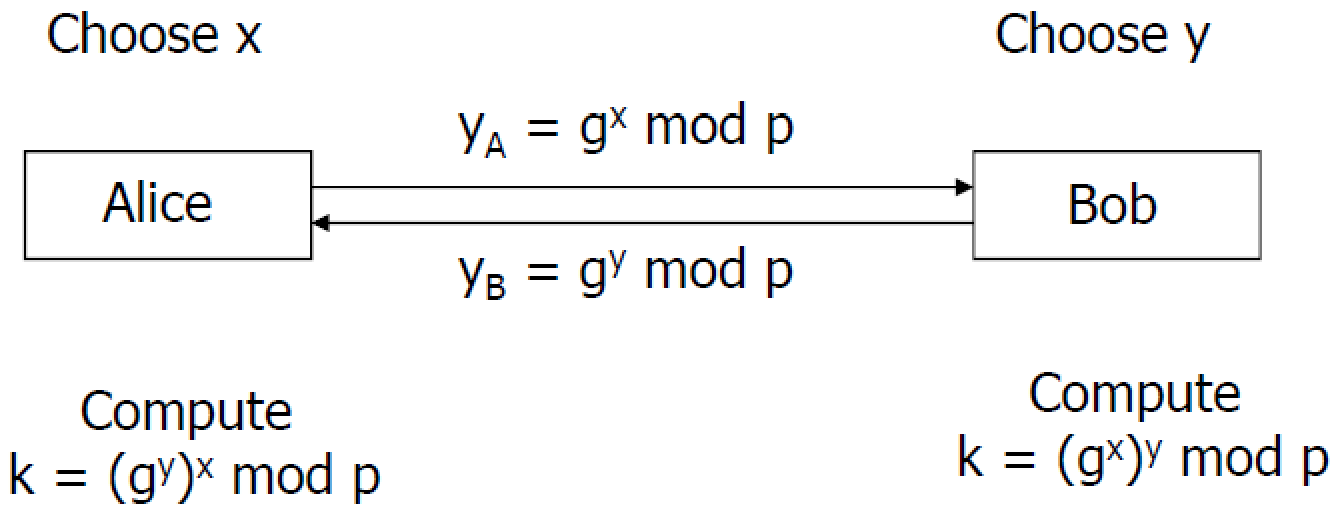


- RSA
    - Ron Rivest
    - Adi Shamir
    - Leonard Adleman

Digital Signature



Diffie-Hellman Key Exchange



Choose x

Choose y

$y_A = g^x \bmod p$

Alice

Bob

$y_B = g^y \bmod p$

Compute
$k = (g^y)^x \bmod p$

Compute
$k = (g^x)^y \bmod p$

Cryptography Overview

	Symmetric Key Setting	Asymmetric Key Setting
Secrecy / Confidentiality	Block Cipher	Public Key Encryption
Authenticity / Integrity	Hash-Based Message Authentication Code	Digital Signature

What’s Next?

- Next Lecture
  - February 12 (Monday), 5:00 pm – 6:30 pm
  - Lecture on Embedded System Security