HOW DO WE SECURE INFORMATION?

claude shannon
1916-2016

IEEE

many thanks to
Algorithmic Research in Network Information Flow (ARNI) Lab. Department of Electical Engineering University of California, Los Angeles (UCLA) USA Martina Cardone

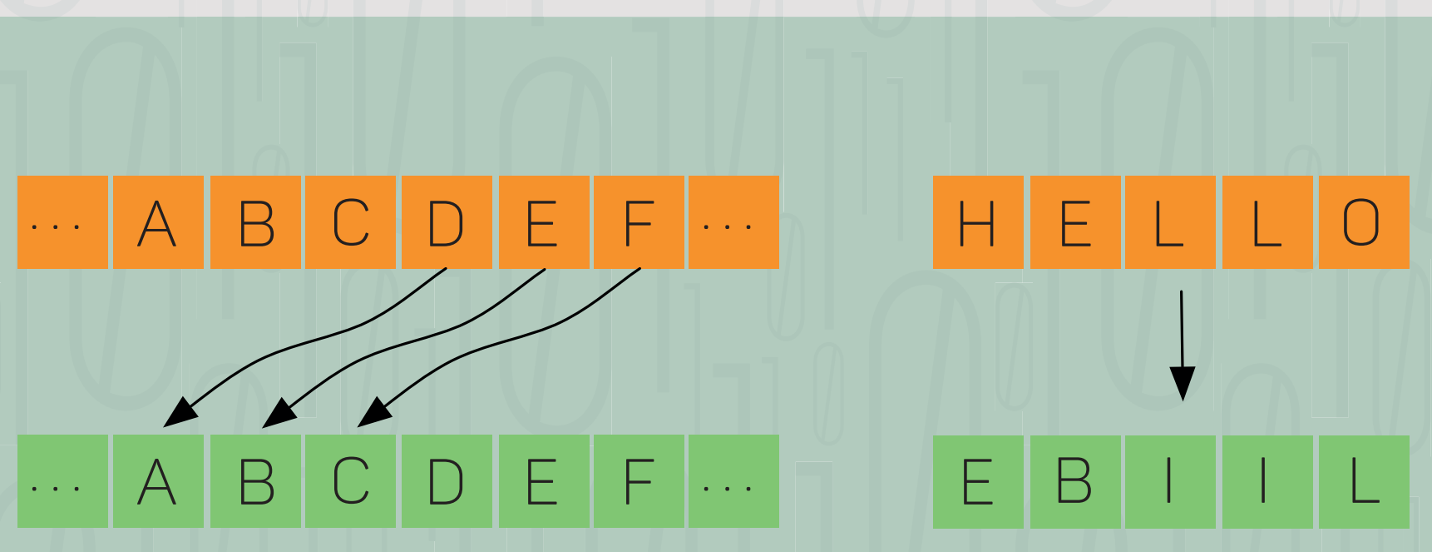
design
alesiom.ch

Transmitting private information (bank account, health information) through the internet, while protecting our privacy against fraudulent attacks, is of fundamental importance. This problem has always continuously posed new challenges, which led to the design of novel secure transmission techniques.

50 BC

ANCIENT CRYPTOGRAPHY

Caesar Cipher



- Introduced in 50 B.C. by Julius Caesar to protect messages of **military** significance; also used in 1915 by the **Russian army**
- Each letter in the plain text is replaced by a letter some **fixed** number of positions down the alphabet
- 🙂 Very **simple** to implement
- 🙁 **Easy to break**

1882

COMPUTER ERA

One-Time Pad

- Introduced in 1882 by F. Miller to secure the **transmission of telegraphs**; also used in **World War II**
- **Symmetric key encryption**: the encryption and decryption keys are the same

1997

MODERN CRYPTOGRAPHY

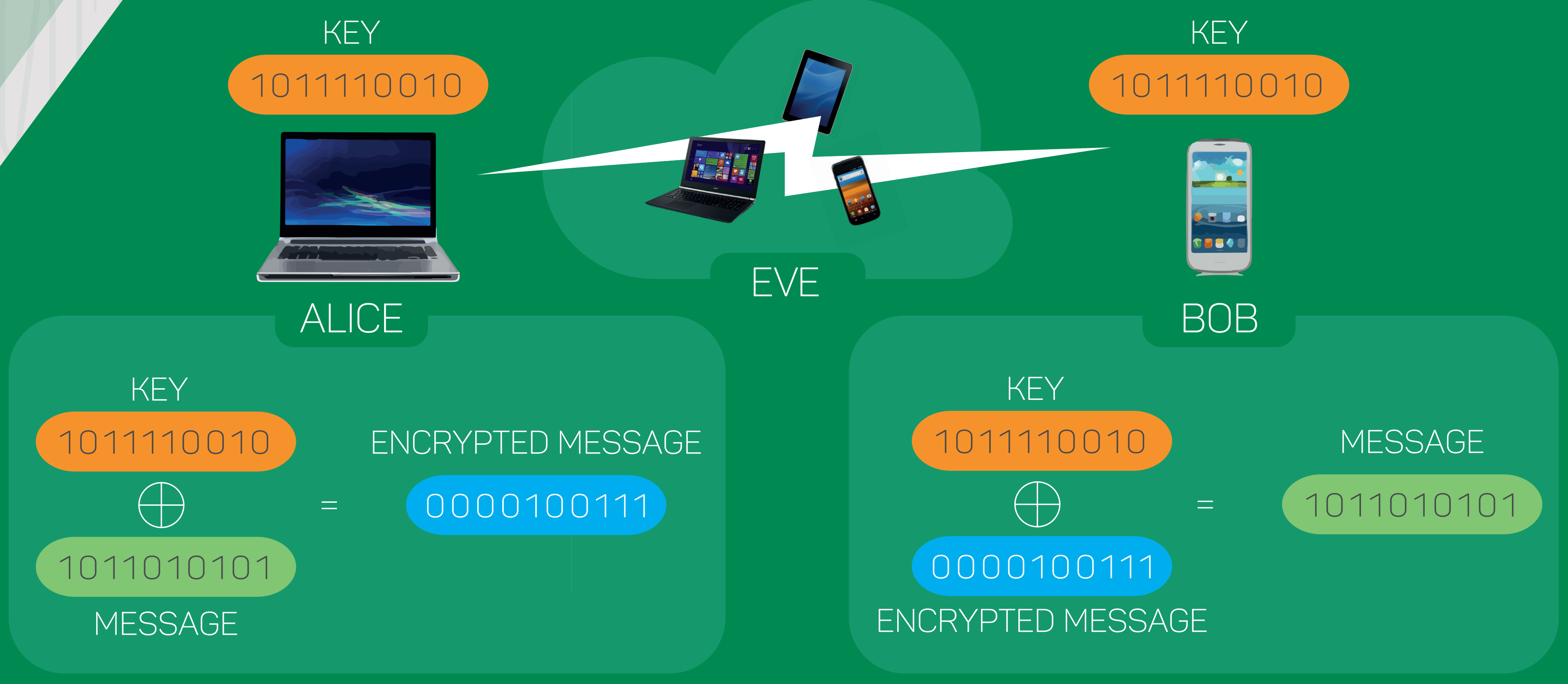
RSA (Rivest-Shamir-Adleman)

- Introduced in 1997 by Rivest-Shamir-Adleman for secure data transmission; widely employed nowadays
- **Public key encryption**: the encryption key is public to anyone, but only the receiving party has access to the decryption key
- 🙂 Uses **short keys**
- 🙁 **Not** proven to be unbreakable

ONE-TIME PAD

Although not widely used today because it is relatively difficult to work with, the one-time pad is still viewed as one of strongest ways to encrypt a communication.

JOHN MARKOFF in "Codebook Shows an Encryption Form Dates Back to Telegraphs"



XORING OPERATION

$0 \oplus 0 = 0$

$0 \oplus 1 = 1$

$1 \oplus 1 = 0$

SECRET KEY

- Shared only between Alice and Bob
- Randomly generated and **used only once**
- Same size as the message

MERITS AND DEMERITS

- 🙂 **Easy** to implement: can be computed by hand with only pen and paper
- 🙂 **Perfectly secure**: proved to be unbreakable (even by an alien!) by Shannon in 1949
- 🙁 Key length is **large** and keys are **not reusable**
- 🙁 **Perfect** and **secure** random key is difficult to generate

2016

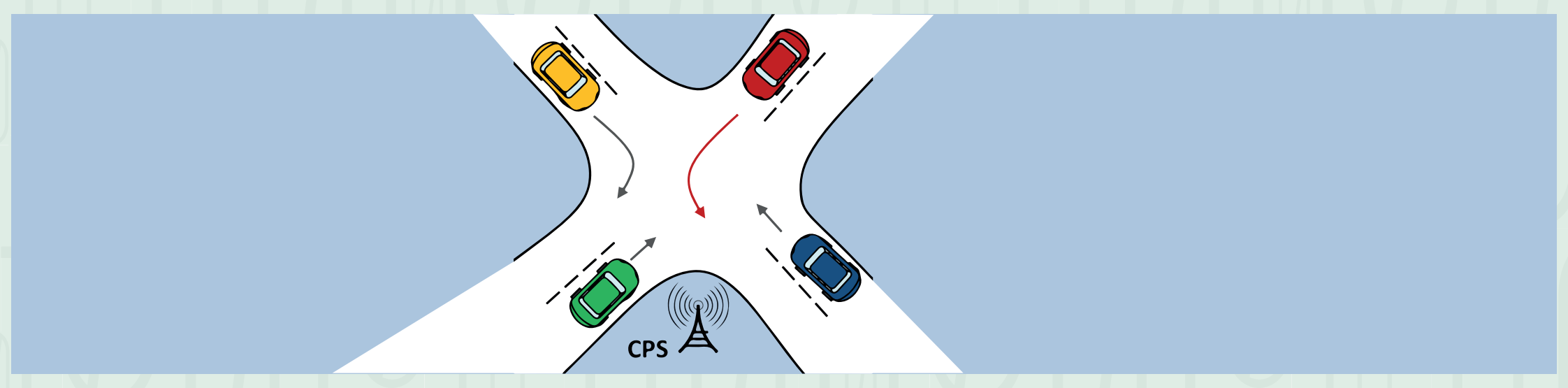
NEW OPPORTUNITIES ON THE HORIZON

Exploit **wireless medium properties** to generate secret keys

Opportunities:
- **Channel variability**: The legitimate receiver and eavesdropper receive different observations of the same transmission
- Presence of **multiple paths** and use of **feedback**

Challenges:
- Attractive targets to hackers

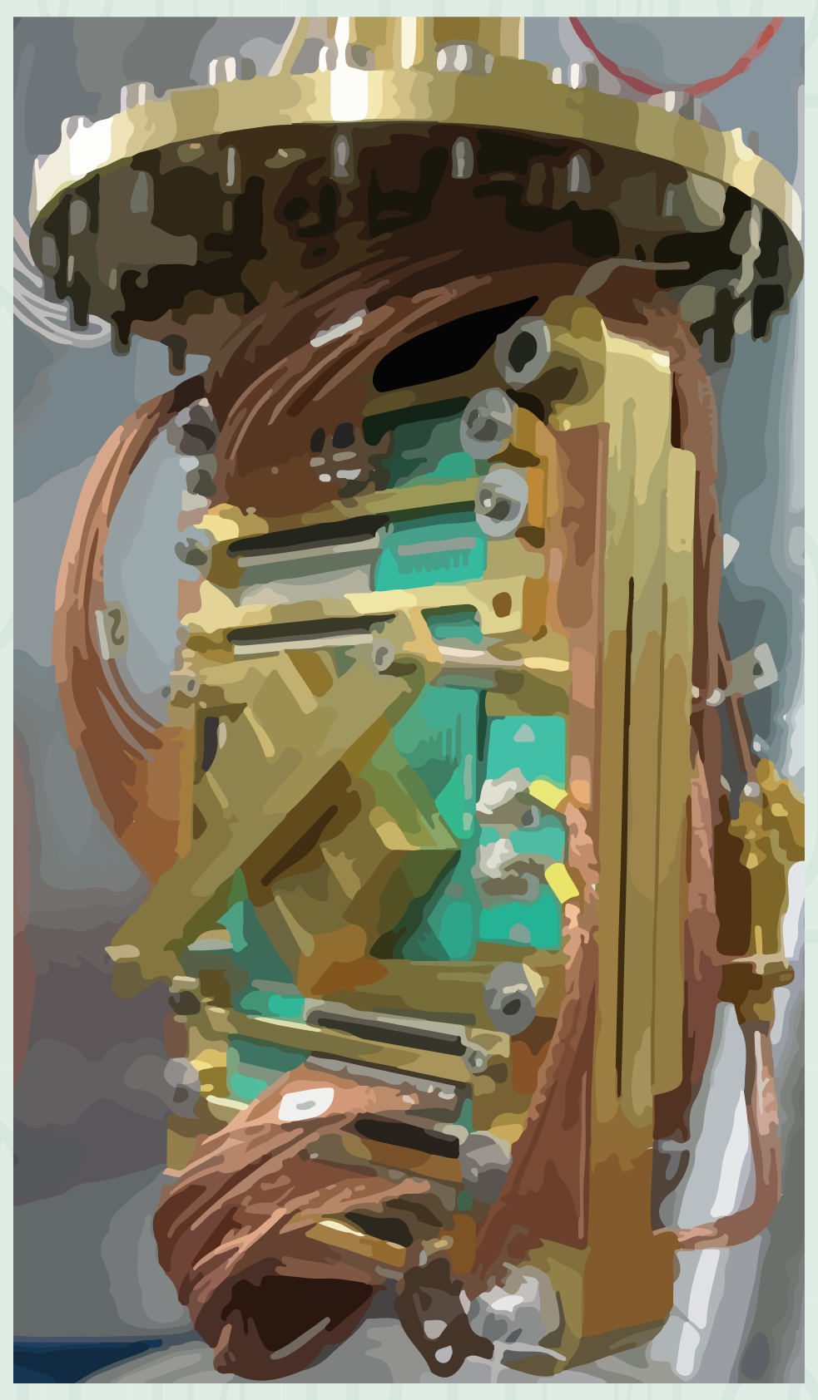
Exploit **properties of physical systems** to design secure protocols for cyber-physical systems



Opportunities:
- Benefits many areas, such as personalized health care, emergency response and traffic flow management

Challenges:
- Interoperation among heterogeneous applications

Exploit **quantum mechanical properties** to generate secret keys



Opportunities:
- Current exchange key techniques (RSA) are vulnerable to **quantum** computers
- **Perfectly Secure**: Heisenberg's uncertainty principle

Challenges:
- Transmission distance and encryption rate limitations