IN410
Cryptography and Secure Communications

Ahmad Fadlallah

General Information

- 50-H course
- Mondays-Tuesdays-Wednesdays*: 8:00 – 9: 40 AM
- Include practical lab sessions: Cryptool and OpenSSL

*: Byweekly

Credits

- The following slides are the adaptation of
  - Lecture slides of Lawrie Brown based on William Stallings book “Cryptography and Network Security: Principles and Practice”
  - Lecture Slides of Dan Boneh – Stanford University
  - Lecture slides of Pawel Wocjan – University of Central California
  - Lecture Slides of Ahmed Serhrouchni – Telecom ParisTech
  - Others (References in the note section)

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unattackable.

—*The Art of War,* Sun Tzu (500 B.C.)

4

Course Topics

- Context ⬅
- History/ Classical ciphers
- Symmetric Encryption
- Cryptographic hash functions
- Key Distribution
- Asymmetric Encryption
- Security Protocols
- …

Learning objectives

- Topics to be covered in this lecture:
  - Concepts and Definitions related to computer security
  - Classical vs. Modern Cryptography
  - Applications of Cryptography

CONTEXT

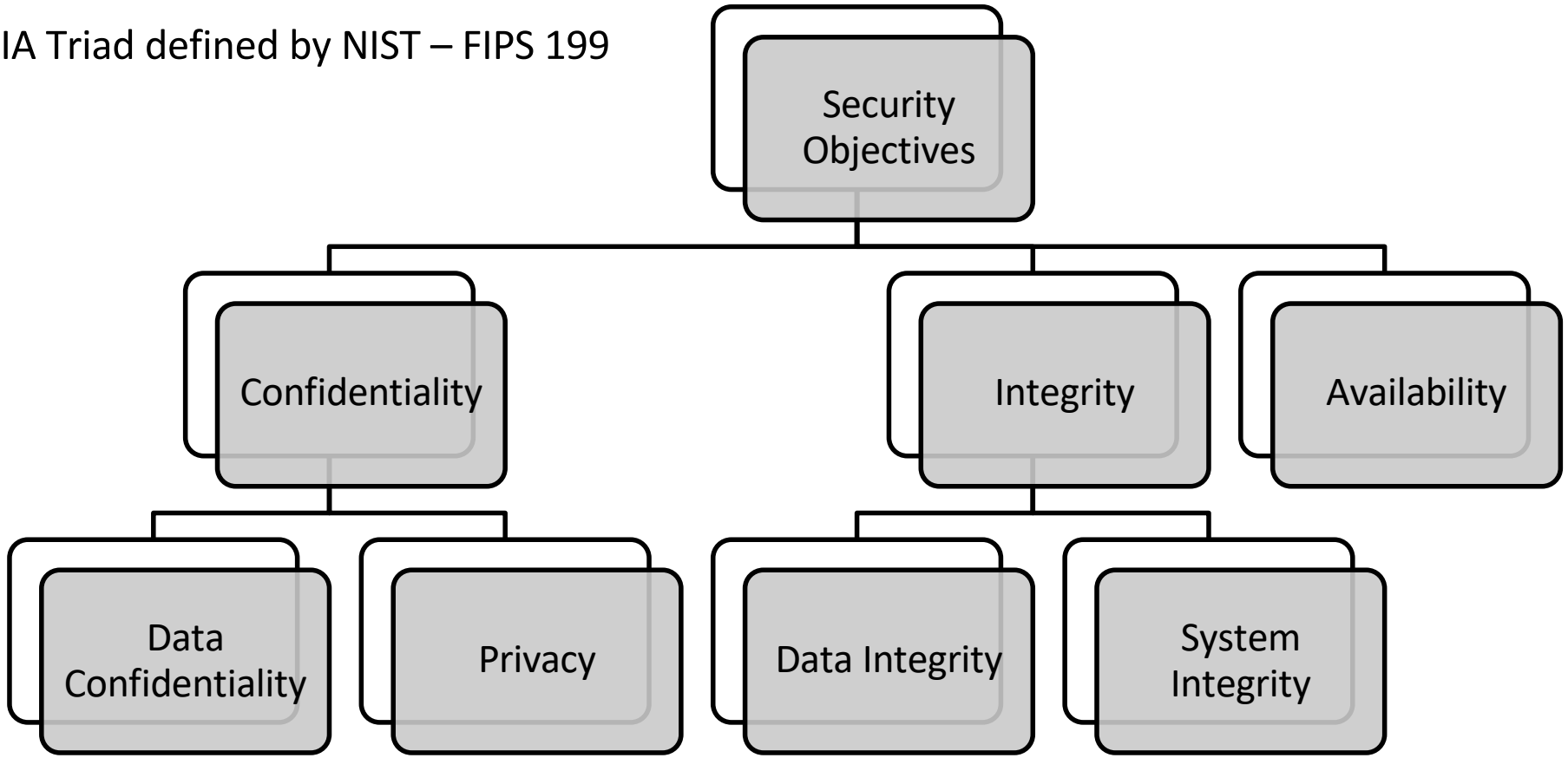
Computer Security – A definition

The protection afforded to an automated information system in order to ***attain the applicable objectives*** *of preserving the* ***Integrity***, ***Availability***, *and* ***Confidentiality*** *of information system resources (includes hardware, software, firmware, information/data, and telecommunications)*

— NIST Computer Security Handbook

Security Objectives : CIA Triad

CIA Triad defined by NIST – FIPS 199



Security Objectives : Confidentiality

- One of the first motivations for cryptography
- Covers two concepts
  - Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals
  - Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

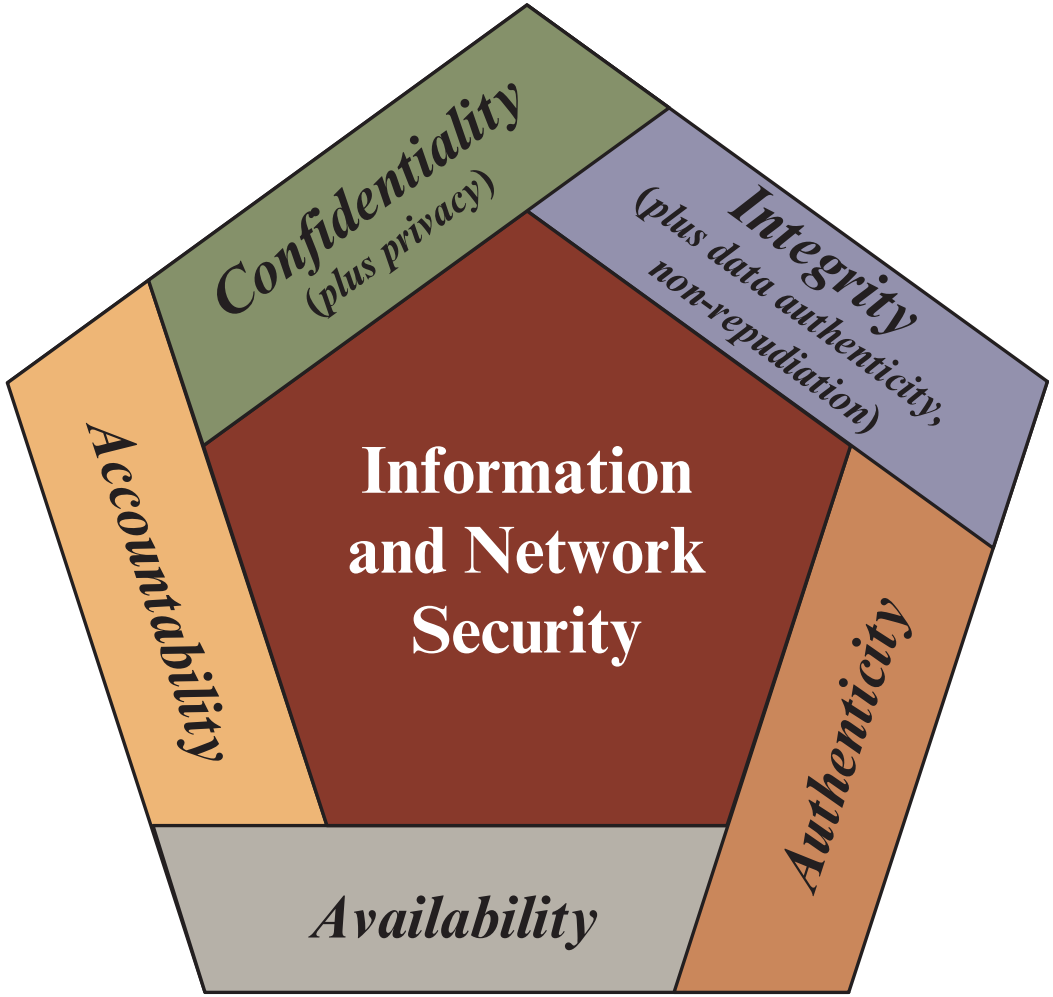
Security Objectives : Integrity

- Validating data/ system is trustworthy and accurate
- Covers two related concepts:
  - Data integrity: Assures that information and programs are changed only in a specified and authorized manner.
  - System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Security Objectives : Availability

- Assures that systems work promptly and service is not denied to authorized users.

More Security Objectives



More Security Objectives: Authenticity

- The property of being genuine and being able to be verified and trusted.
- Confidence in the validity of a transmission, a message, or message originator.

More Security Objectives: Accountability

- The requirement for actions of an entity to be traced uniquely to that entity.
- This supports Non-repudiation, *fault isolation*, *intrusion detection and prevention*, and *after-action recovery* and *legal action*.
- Truly secure systems are not yet achievable=> need to trace a security breach to a responsible party

More Security Objectives: Accountability

- Non-Repudiation

Security Objectives

- System Security Requirements might include more than one objective (sometimes all of them)
- Security Objectives are interdependent: Implement one security objective should not affect other objectives
  - One can get confidentiality and integrity simply by turning off a computer => Loss of availability.
  - Confidentiality without integrity is generally useless since you may access data that was modified without your knowledge

Thinking About Security

- Security is a systems issue and is based on all the components of the system

Hardware	Firmware	Operating Systems
Application software	Networking Components	People

Thinking About Security

"*Security is a chain:*

it's only as secure as the weakest link"

— Bruce Schneier

Challenges of Computer Security

1. **Security is not as simple as it might first appear to the novice**: Objectives/Requirements looks simple (confidentiality, integrity, etc.) but the mechanisms to meet the requirements are quite complex
2. **Need to consider the potential attack on the security features** => increase the complexity of the security mechanisms
3. **Need to decide where (physical / logical) to use the designed security mechanisms**

Challenges of Computer Security

4. **Need to share secret information in some security mechanisms** => how to manage the secret information?
5. **Security mechanisms might rely on communication protocols** => more complications (e.g., timeliness of transmitting messages for a security protocol)
6. **Attacker** needs to **find one weakness** while the **defender** should find and **eliminate all weaknesses**

Challenges of Computer Security

7. Natural tendency to **little invest in security until an event occurs**
8. **Security requires regular and even constant monitoring**
9. Security should be an integral part in the system design and **not to be included after the design**
10. **Security vs. User-friendliness**

What is a threat?

What is an attack?

What is the relation between them?

Security Attacks

Any action that compromises the security of information owned by an organization.

Threats

- A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
- A threat is a possible danger that might exploit a **vulnerability**
- Accidental vs. Intentional threats

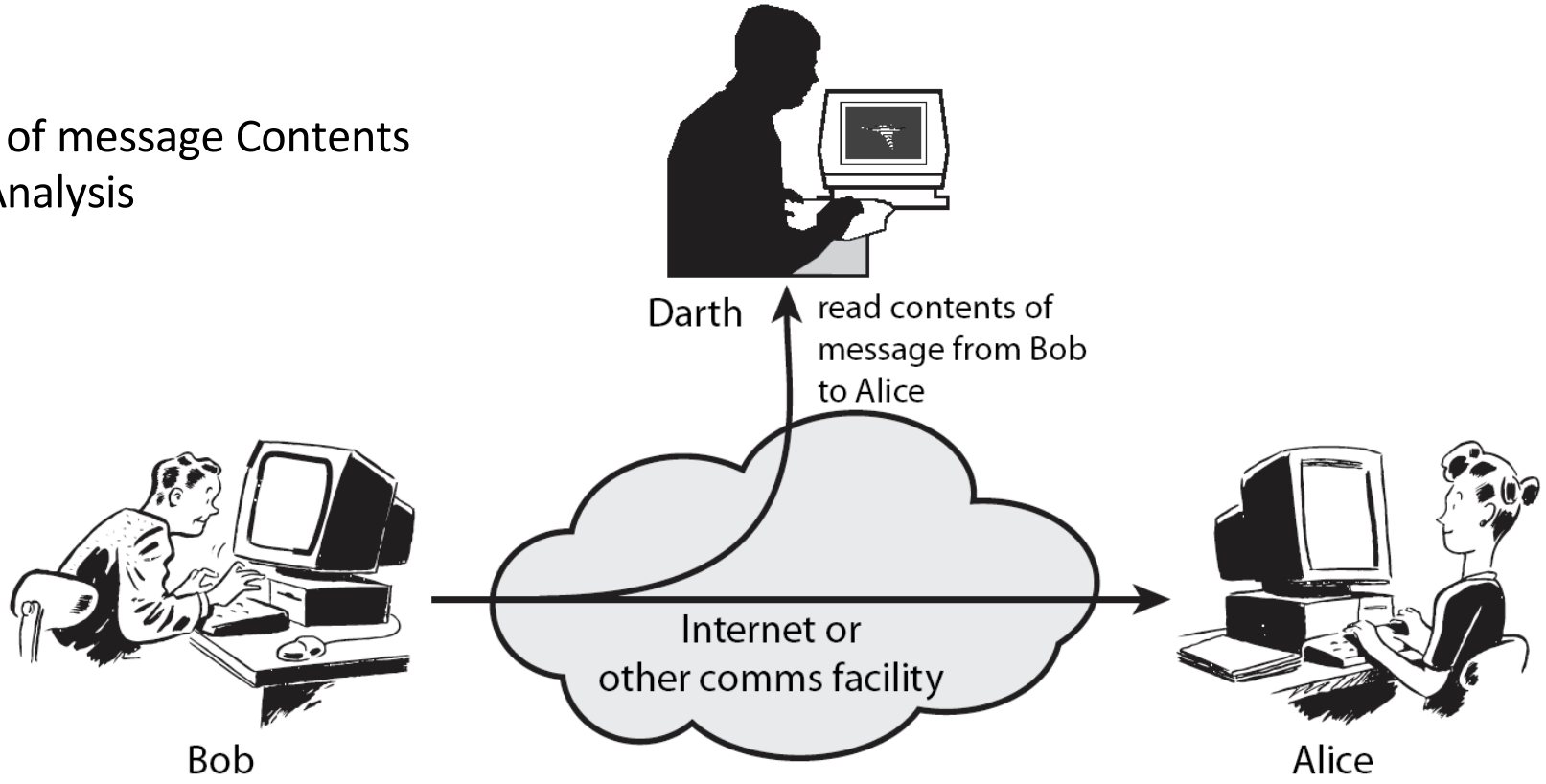
Attacks

- An **assault** on system security that derives from an **intelligent threat**
- An intelligent act that is a **deliberate attempt** (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.
- Two types of attacks
  - Active vs. Passive attacks

Passive attacks vs. Active Attacks

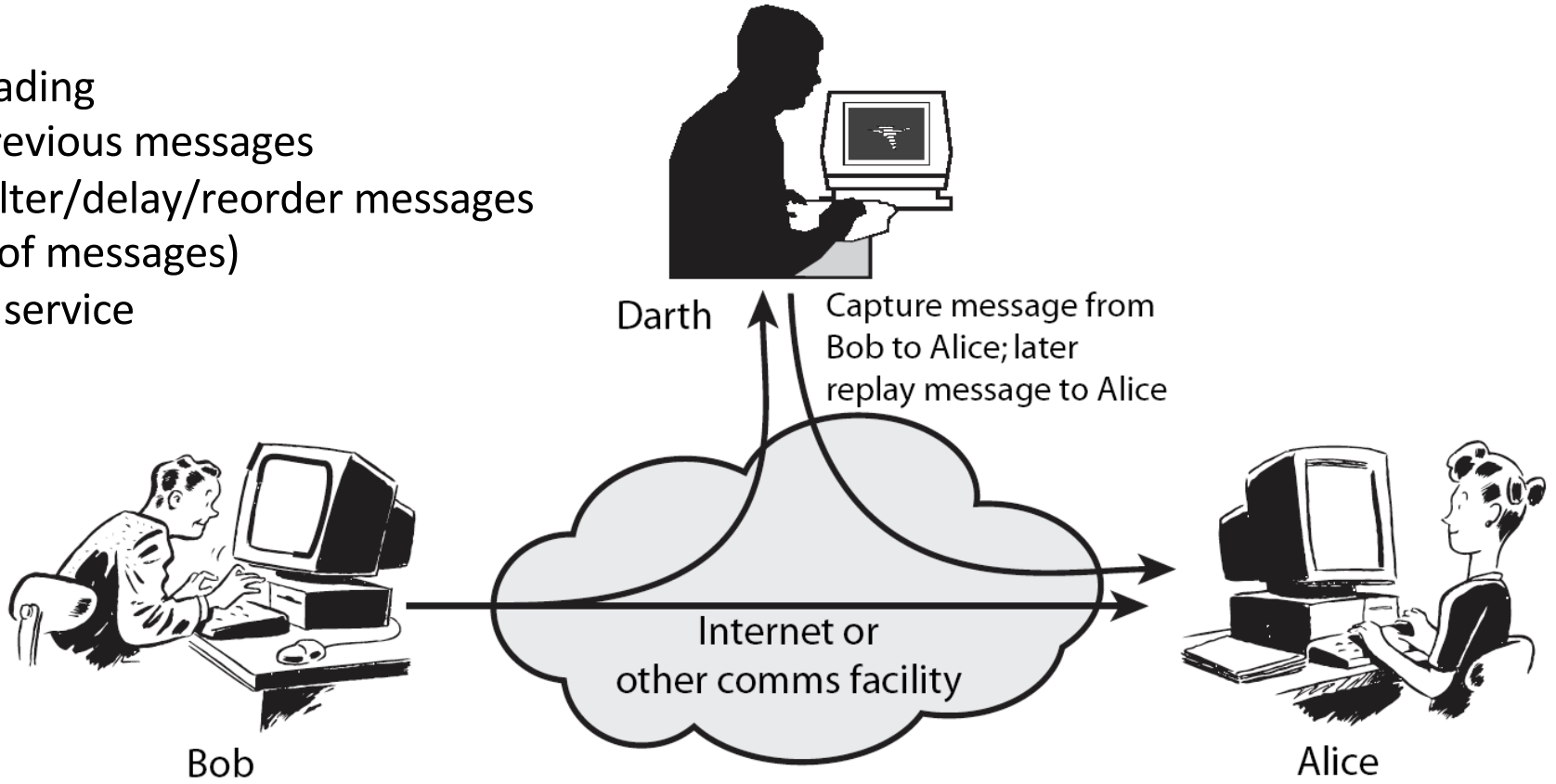
Passive Attacks

Release of message Contents
Traffic Analysis



Active Attacks

Masquerading
Replay previous messages
Modify/alter/delay/reorder messages (or parts of messages)
Denial of service



Security Services

- Enhance security of data processing systems and information transfers of an organization
- Intended to counter security attacks
  - Using one or more security mechanisms
- Often replicates functions normally associated with physical documents

Security Services

- **Authentication**
  - Assurance that communicating entity is the one claimed
  - have both peer-entity & data origin authentication
- **Data Confidentiality**
  - protection of data from unauthorized disclosure
- **Data Integrity**
  - Assurance that data received is as sent by an authorized entity
- **Non-Repudiation**
  - protection against denial by one of the parties in a communication
- **Access Control**
  - prevention of the unauthorized use of a resource
- **Availability**

Security Mechanisms

- Features designed to detect, prevent, or recover from a security attack
- **Specific security mechanisms**
  - Implemented in a specific protocol layer
  - Examples: Encryption, digital signatures, …
- **Pervasive security mechanisms**
  - Not specific to any protocol layer or security service
  - Examples: event detection, security audit trails, etc.

Cryptography in security mechanisms

- No single mechanism that will support all services required
- However, one particular element underlies many of the security mechanisms in use:
  - Cryptographic Techniques

Cryptography - Definition

"…the art of writing or solving codes…"

— ***Oxford dictionary***

- Historically accurate, but it does not capture the essence of modern cryptography

Classical Cryptography

- **Main focus:** problem of secret communication
- **Cryptography was an art**
  - Constructing good codes, or breaking existing ones, relied on creativity and personal skills.
  - Very little theory that could be relied upon
    - There was not even a well-defined notion of what constitutes a good code.
- **Main consumers:** military and intelligence organizations

Modern Cryptography

- Much broader scope!
  - Data integrity, authentication, protocols, …
- Cryptography is now a science
  - Rigorous analysis, firm foundations, deeper understanding, rich theory
- Cryptography is ubiquitous

Modern Cryptography – better definitions

*"Design, analysis, and implementation of **mathematical techniques** for securing information, systems, and computation against adversarial attack"*

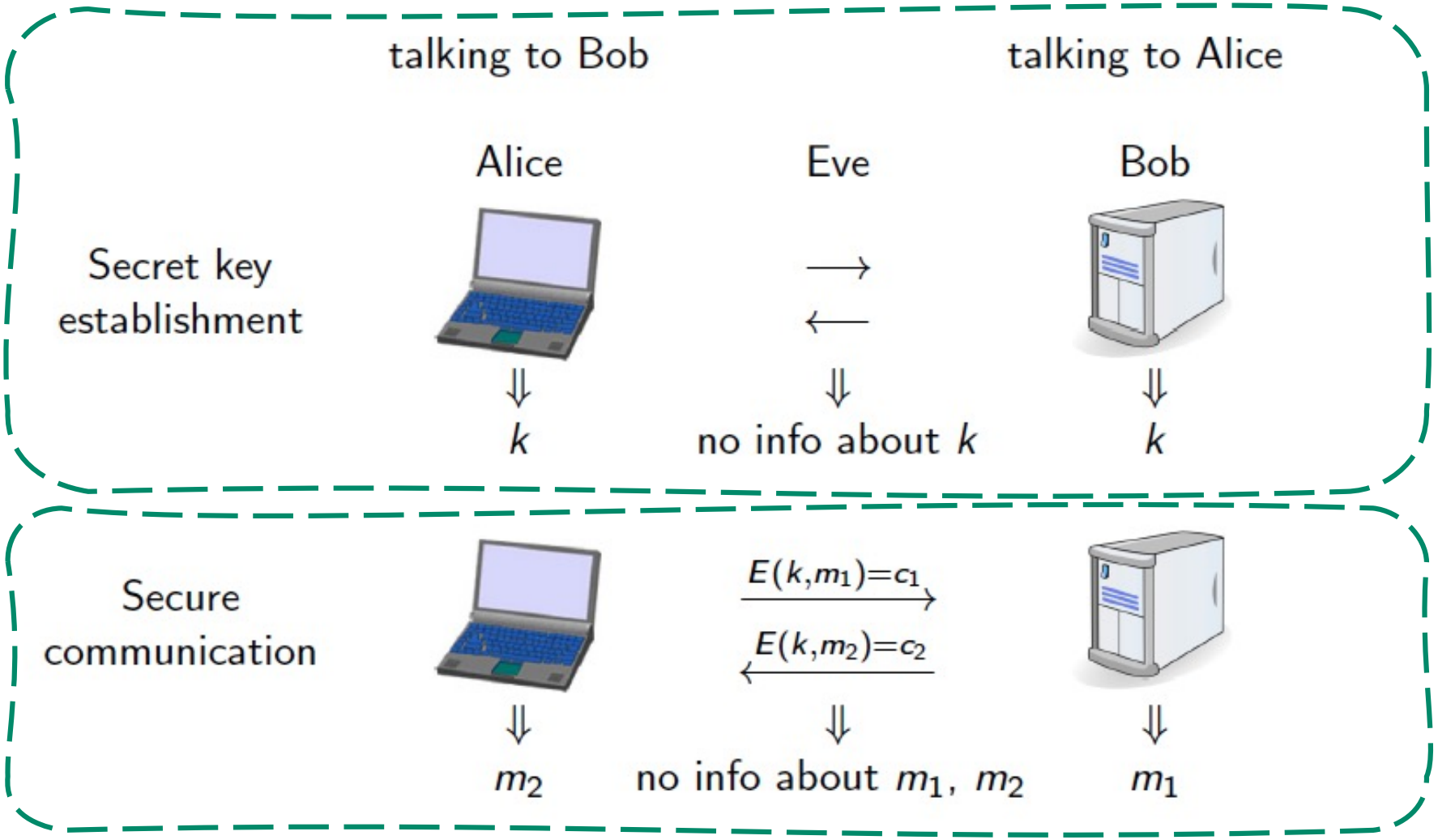
Cryptography for everyone

- Military
- Diplomatic
- Society (General Public, Private or Secret)
- Financial
- Informatics
- …

Cryptography is everywhere

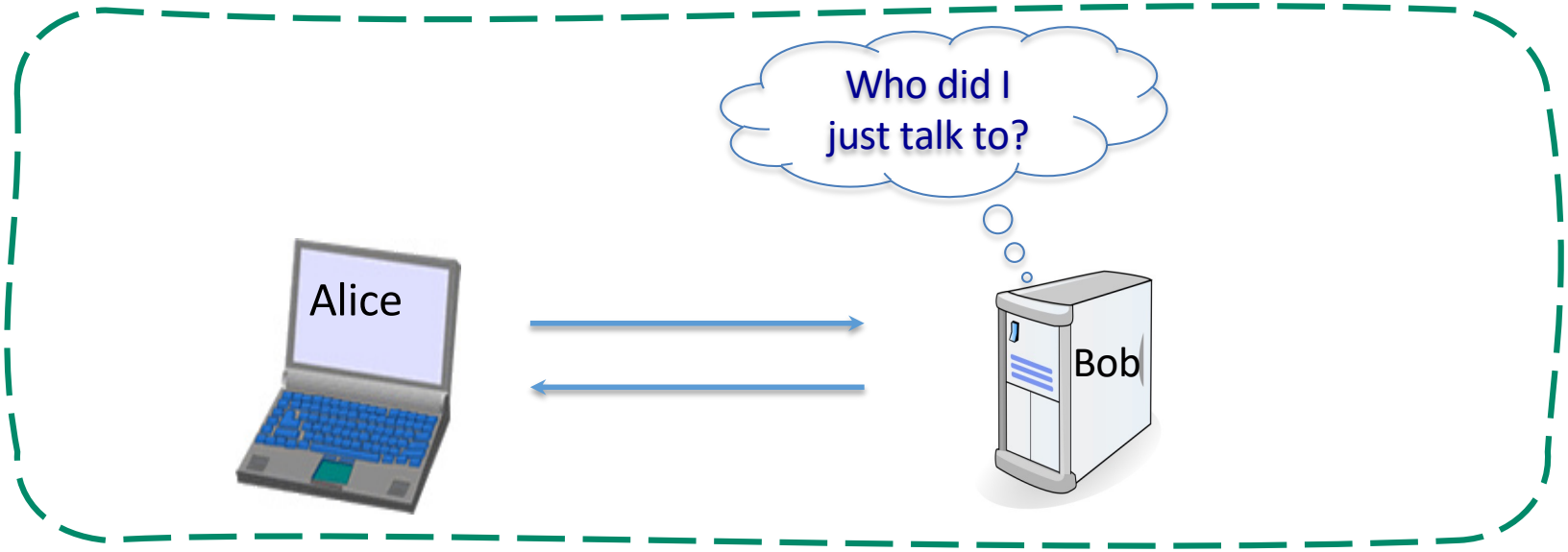
- **Secure communication**
  - Web traffic: HTTPS
  - Wireless traffic: 802.11i WPA2 (Wi-Fi protected access) and WEP (wired equivalent privacy), GSM (global system for mobile), Bluetooth
- **Encryption of files**: EFS (Encrypting File System), TrueCrypt
- **Content protection** (e.g. On DVD and Blue-ray): CSS (Content Scrambling System), AACS (Advanced Access Content System)
- **User authentication**: SSH
- And many more applications….

Crypto core Applications



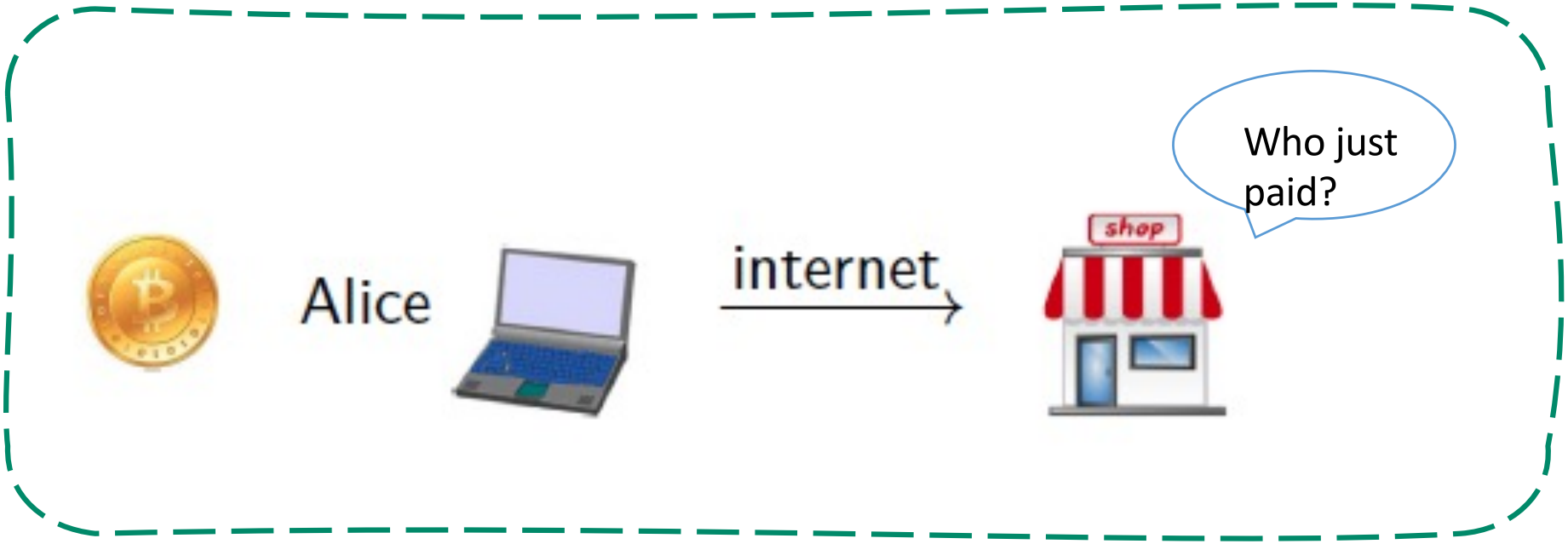
More Cryptographic Applications

- Digital signatures
- Anonymous communication
  - Anonymous communication: Mix network, TOR (The Onion Router)



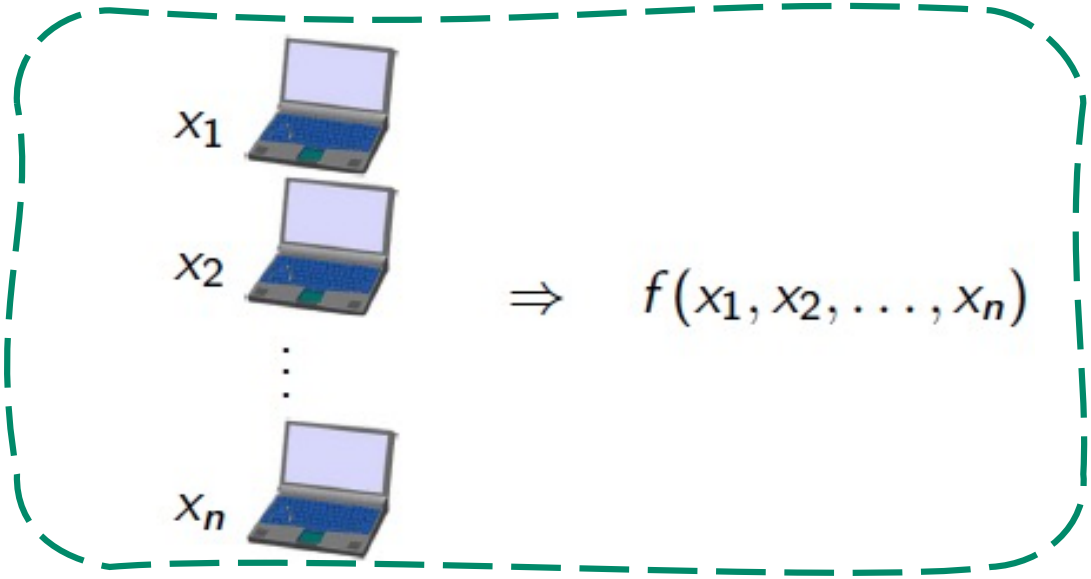
More Cryptographic Applications

- Anonymous digital cash



More Cryptographic Applications

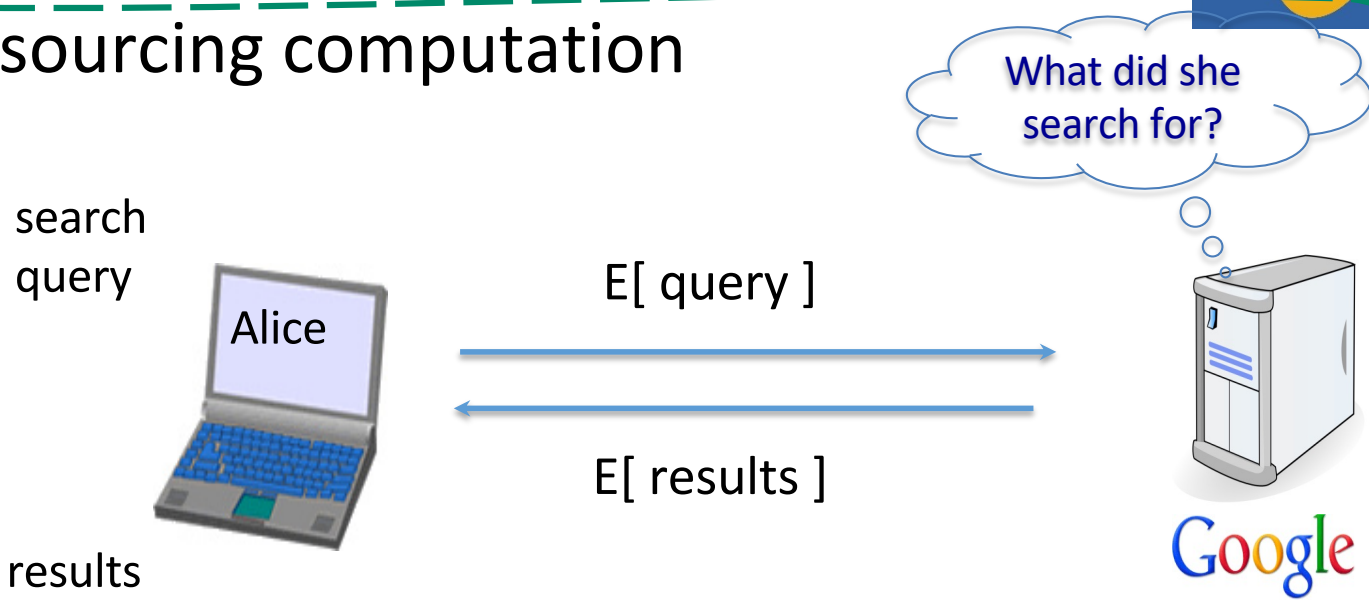
- Secure Multiparty Computation
  - Evaluate the function $f(x_1, \ldots, x_n)$ without revealing their inputs to each other
  - Examples: Elections, Private Auctions



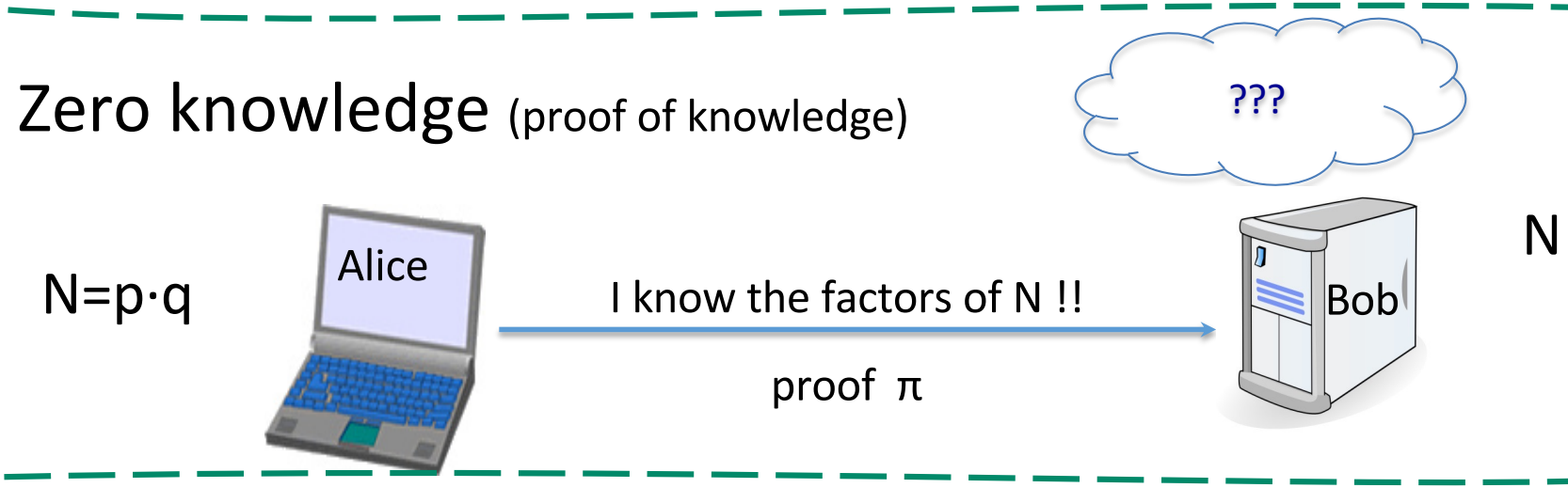
More Cryptographic applications

- Privately outsourcing computation

  - homomorphic encryption
  - Doable but not practical for google search



- Zero knowledge (proof of knowledge)



Standards Organizations

NIST
National Institute of
Standards and Technology

Things to remember

- Cryptography is:
  - A tremendous tool
  - The basis for many security mechanisms
- Cryptography is **NOT**:
  - The solution to all security problems (software bugs, social engineering attacks, etc.)
  - Reliable unless implemented and used properly
  - Something you should try to invent yourself
    - Many examples of broken ad-hoc designs