Introduction to Modern Cryptography

Michele Ciampi

(Slides courtesy of Prof. Jonathan Katz)

Lecture 1, part 2

Introduction

Cryptography

Cryptography as an art

"The art of making and breaking secret codes"

Focused exclusively on ensuring private communication between two parties sharing secret information in advance using "codes" (i.e. private-key encryption)

- Historically, cryptography was an art: heuristic, unprincipled design and analysis
- Schemes proposed, broken, repeat...
- Used primarily for military/government applications

Modern cryptography

Cryptography as a science

Design, analysis, and implementation of mathematical techniques for securing information, systems, and distributed computations against adversarial attack

- Cryptography is now much more of a science
- Rigorous analysis, firm foundations, deeper understanding, rich theory

Modern cryptography

Scope

- Data integrity, authentication, protocols, ...
- The public-key setting
- Group communication
- More complicated trust models
- Foundations (e.g. number theory, quantum-resistance) and systems (e.g. electronic voting, blockchain, cryptocurrencies)

Modern cryptography

Applications

- Password-based authentication, password hashing
- Secure credit-card transactions over the internet
- Encrypted WiFi
- Disk encryption
- Digitally signed software updates
- Bitcoin
- ...

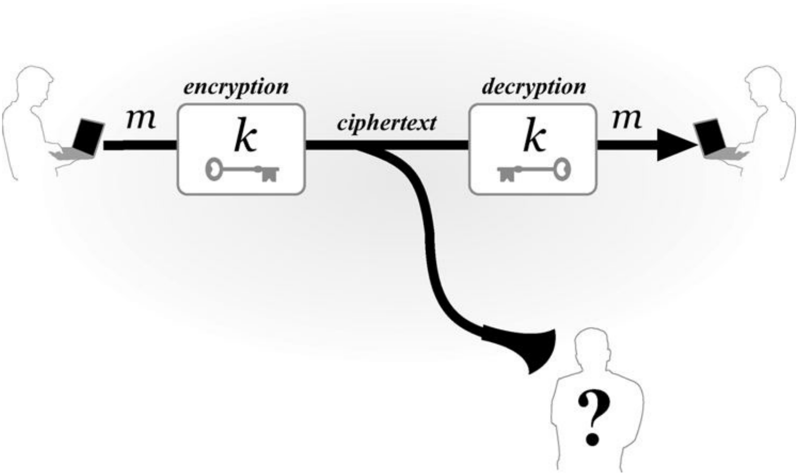
Course outline

	Secrecy	**Integrity**
Private-key setting (SK)	Private-key encryption	Message authentication codes
Public-key setting (PK)	Public-key encryption	Digital signatures

Classical cryptography

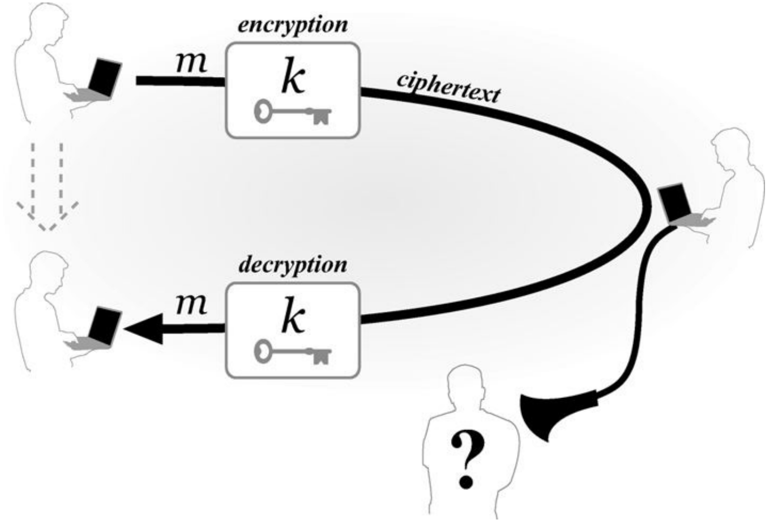
- Until the 1970s, exclusively concerned with ensuring secrecy of communication i.e. encryption
- Relied exclusively on secret information (a key) shared in advance between the communicating parties
- Private-key cryptography
  - aka secret-key / shared-key / symmetric-key cryptography

Private-key encryption



IMC Textbook 2nd ed. CRC Press 2015

Private-key encryption (Single User)



IMC Textbook 2nd ed. CRC Press 2015

Private-key (symmetric-key) encryption

- A private-key encryption scheme is defined by a message space $\mathcal{M}$, key space $\mathcal{K}$ and algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$:
  - Gen (key-generation algorithm): outputs $k \in \mathcal{K}$
  - Enc (encryption algorithm): takes key k and message $m \in \mathcal{M}$ as input; outputs ciphertext $c \leftarrow \mathsf{Enc}_k(m)$
  - Dec (decryption algorithm): takes key k and ciphertext c as input; outputs m or "error": $m = \mathsf{Dec}_k(c)$
- For all $m \in \mathcal{M}$ and k output by Gen: $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$

Kerckhoffs's principle

The encryption scheme is not secret

- The attacker knows the encryption scheme
- The only secret is the key
- The key must be chosen at random; kept secret

Arguments in favour of Kerckhoffs's principle

- Easier to keep key secret than algorithm
- Easier to change key than to change algorithm
- Standardisation
  - Ease of deployment
  - Public scrutiny

End