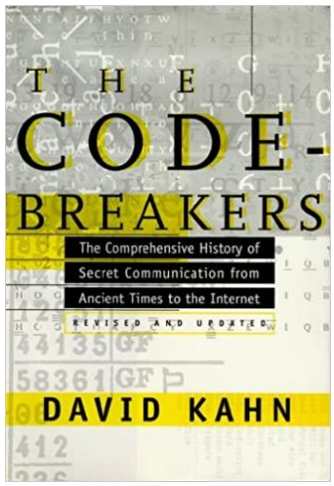
Applied Crypto Introduction

Gianluca Dini
Dept. of Ingegneria dell'Informazione
University of Pisa
gianluca.dini@unipi.it
Version: 2021-02-27

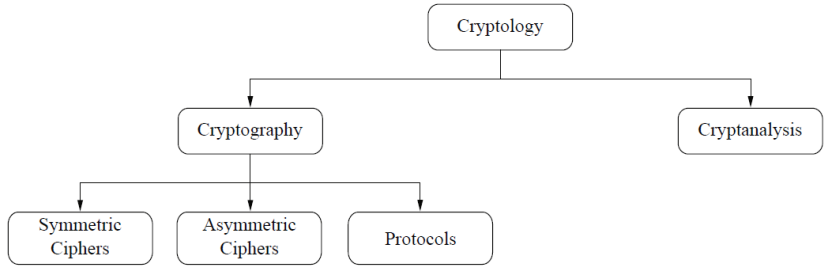
1

Historical perspective



2

Cryptology



3

What does "cryptography" mean?

Cryptography

secret writing

4

Why "applied" cryptography?

- Don't invent your own crypto-but use well-established ones
- Use cryptography as a building block of secure protocols and applications

5

Why are secrets so important?

- They are everywhere
  - Secure communication
    - Web traffic: HTTPS
    - Wireless traffic: 802.11i WPA2, GSM, Bluetooth
  - Encrypting files on disks
    - EFS, TrueCrypt
  - Content protection
    - DVD (CSS); Blu-ray (AACS)
  - User authentication
    - Pwd, 2FA,…
  - …and much more

6

Cybersecurity

- There is an adversary, with an objective and some resources

7

We will learn to

- **Understand and use crypto-primitives**
  - Ciphers, hash functions, digital signatures, key exchange
- **Analyse, design and implement protocols**
  - Authentication protocols
  - Key management protocols
  - Crypto-protocols in general
- **Reason about security**

8

What does "security" mean?

UNIVERSITÀ DI PISA

- Many very smart, highly motivated people tried to break it but couldn't **3**
- There are 834 quadrillions possible keys so it must be secure **4**
- Here is a mathematical proof, accepted by experts, that shows it is secure **1**
- Here is a strong argument why breaking it is as hard as solving a problem we believe is hard **2**

Mar-21 Applied Crypto - Introduction 9

9

A security engineer thinks differently

UNIVERSITÀ DI PISA

- Unfair competition against the adversary
- Security vs. performance and usability
- What's the ROI?
- Devil hides in details

Mar-21 Applied Crypto - Introduction 11

11

12