


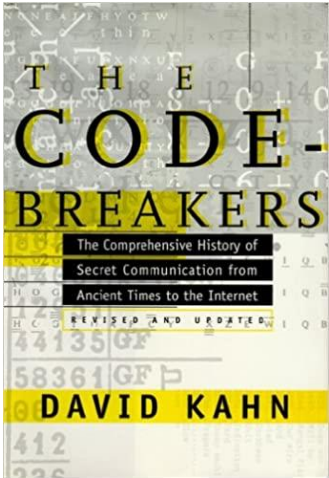
Applied Cryptography

Introduction

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

1

Historical perspective



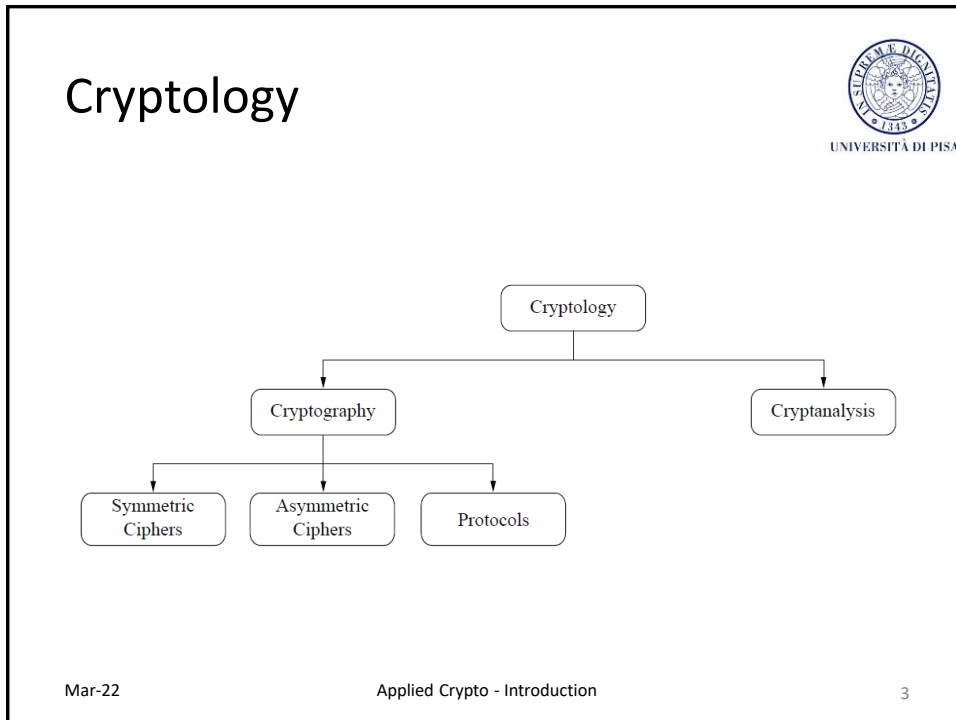
UNIVERSITÀ DI PISA

Mar-22

Applied Crypto - Introduction


2

2



3

Why are secrets so important?



UNIVERSITÀ DI PISA

- 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

Mar-22 Applied Crypto - Introduction 4

4

The adversary



UNIVERSITÀ DI PISA

- There is an *intelligent* adversary, with an *objective* and some *resources* and *abilities*



Mar-22

Applied Crypto - Introduction

5

5

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-22

Applied Crypto - Introduction

6

6

Why “applied” cryptography?



UNIVERSITÀ DI PISA

- Don't invent your own crypto-but use well-established ones
- “Anyone who tries to create his or her own cryptographic primitive is either a genius or a fool. Given the genius/fool ratio of our species, the odds aren't very good.” — Bruce Schneier, [Secrets and Lies: Digital Security in a Networked World](#)

Mar-22

Applied Crypto - Introduction

7

7

Why “applied” cryptography?



UNIVERSITÀ DI PISA

- Use cryptography as a building block
- We will learn to
 - Understand and use crypto-primitives
 - Ciphers, hash functions, digital signatures, key exchange
 - Reason about security
 - Whether and why primitives and protocols are secure
 - Analyze, design and implement protocols
 - Authentication protocols
 - Key management protocols
 - Crypto-protocols in general


Mar-22

Applied Crypto - Introduction

8

8

What does “security” mean?



UNIVERSITÀ DI PISA

- <https://forms.office.com/r/7x6w41VZEK>


Mar-22

Applied Crypto - Introduction

9

9

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-22

Applied Crypto - Introduction

10

10

Things to remember



UNIVERSITÀ DI PISA

- Cryptography is
 - a very useful tool
 - the basis for many mechanisms
- Cryptography is not
 - The solution to all security problems
 - Software bugs, social engineering
 - Reliable if not designed, implemented and used properly
 - WEP, Heartbleed,...
 - Something you should try to invent yourself

March 22

FoC - Symmetric Encryption

11

11

To remember



UNIVERSITÀ DI PISA

- “Whoever thinks his problem can be solved using cryptography, doesn’t understand his problem and doesn’t understand cryptography.” – Attributed by Roger Needham and Butler Lampson to each other

Mar-22

Applied Crypto - Introduction

12

12

Mar-22Applied Crypto - Introduction13