Introduction to Cryptology

Lecture-01
Introduction and Lecture's Overview

28.02.2023, v2

Prof. Wael Adi
Technical University of Braunschweig
Electrical Engineering Dept.
Computer Engineering

Prof. Nizamettin Aydin
Yıldız Teknik Üniversitesi

Lecture Material

- Lecture slides would be offered in Electronic form before the lecture-
- It is highly recommended to make a printout of the slides to put your comments online on the printed paper slides.

Possible Readings:

1. **Cryptography: An Introduction**
   https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf
   By Nigel Smart
   (3rd Edition) Free on the Web.
2. **Introduction to Modern Cryptography: Principles and Protocols**
   J. Katz, Y. Lindell, CRC Press 2021

Recommended basic reference handbook:

Recommend to download

3. **Handbook of Applied Cryptography**
   by Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone
   CRC Press (October 16, 1996) (available free of charge on the WEB)

- Homepage in Germany: https://www.tu-braunschweig.de/en/kns/faculty-and-staff/wael-adi

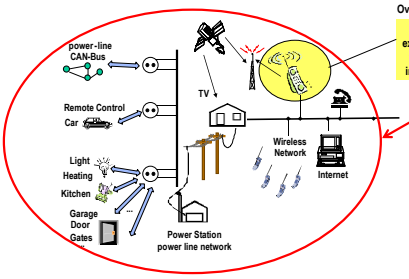
Introduction

This introduction presents few simple examples demonstrating main course contents with minimum mathematics !

- Why Security ?
- The Evolution of Security Technology
- Overview on the course contents

Why Security ?

Open World of Information Network Evolution



Over 6 000 Million mobile devices

Widespread expanding worldwide network with unlimited applications in every day's life .. IoT.. etc.

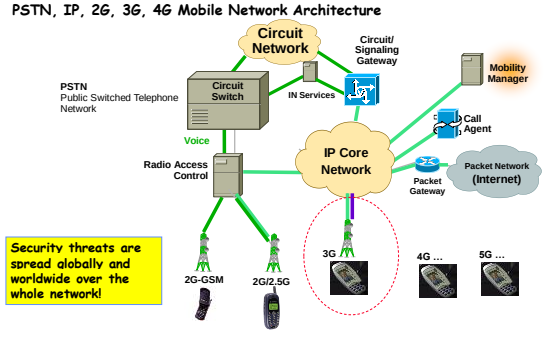
Global Information *Short-Circuit*

(AAA Scenario)

Anywhere
Any time
Any device

Evolution of Communication Networks

PSTN, IP, 2G, 3G, 4G Mobile Network Architecture



Security threats are spread globally and worldwide over the whole network!

Impacts of the Globalization of Information Technology !

- Globalization (Borderless)
- Unlimited resources
- Unrestricted resources
- Easy untraceable access

- No national boarders/Law?
- Manageability ?
- controllability ?
- Abuse-ability

Security is still a serious issue in most communication systems and is a very essential one !!

Two Major Security Tasks

- *Authentication*
  Securely identify network entities
- *Secrecy*
  Keep data secret against illegal users

Security tasks require to deploy cryptographic mechanisms
Cryptography: deals with securely hiding and identifying information and entities

Major lecture contents

- Mathematics for cryptography. Number Theory (4)
- Secrecy Theory (1)
- Secret-Key Cryptography (2)
- Public-Key Cryptography (5)
- Cryptographic Protocols and Schems (1)
- Physical Security and Identification (1)

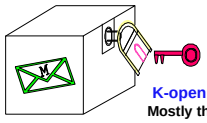
The contents are design and engineering-oriented with Less or no proofs,

1. Secret-Key Cryptography

Overview Concepts

Secret Key Cryptography

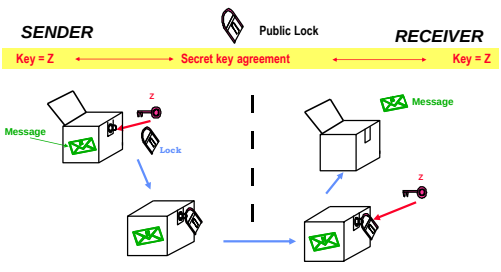
(Symmetric System)



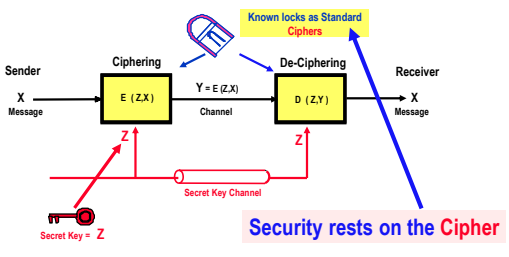
K-open = K-close
Mostly the same key

- Open and close using shared secret keys (mostly one shared key) !!
- A Secret key agreement is required !

Secret Key Crypto-System : mechanical simulation



Conventional Cryptography till 1976 : Secret Key systems



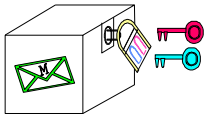
Security rests on the Cipher

2. Public-Key Cryptography

Scientific Breakthrough 1976

Secure-Communication
without prior shared secret keyes

Public-Key Secrecy Systems



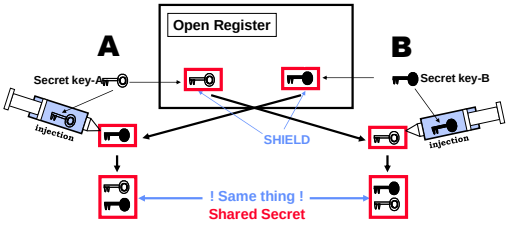
- Open and close with different keys!!
- No Secret Key Agreement required

Two Major Schemes in Public Key Cryptography:
- Diffie-Hellman Public Key exchange scheme
- RSA public Key secrecy system

Sharing Secrets without prior exchange of secrets

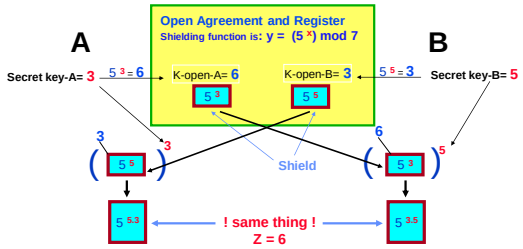
Public-Key Cryptography Breakthrough 1976 (Diffie & Hellman)

"Mechanical Scenario"



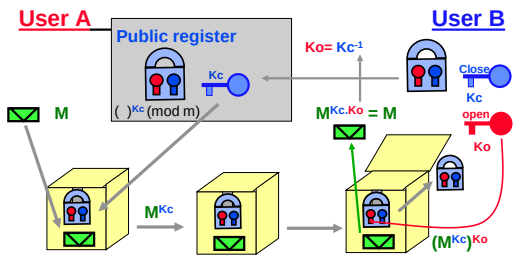
Example for *Diffie-Hellman* key exchange scheme 1976

Widely use in internet, banking etc...



Basic Public Key Secrecy System (RSA system1978)

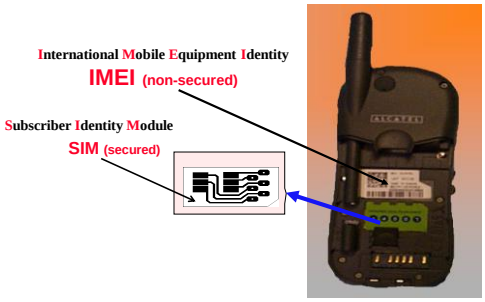
(Mechanical simulation: user B gets a secured message from A)



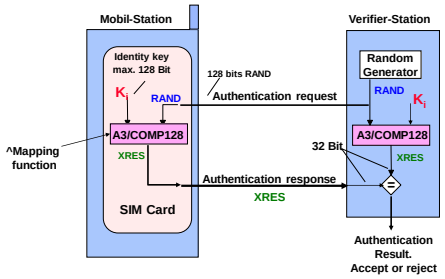
3. Authentication

Identification, Signature ..

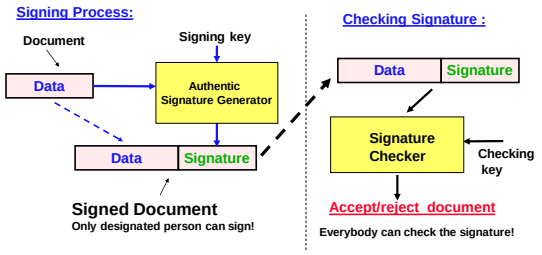
Secured Identity (Authentic Entities)



GSM Authentication: Challenge-Response Subscriber Identification Mechanism



Secured Signature (Data Authentication)
(source authentication)

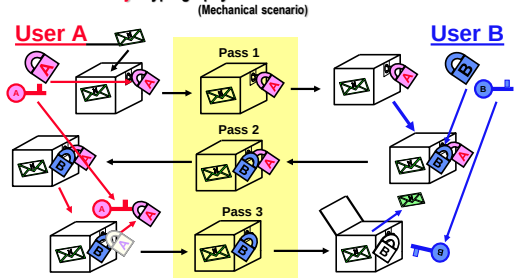


4. Cryptographic Protocols

Secret Sharing, Security Management, Standards, Mobile Security & Applications

A sample Cryptographic Protocol

No Key Cryptography : Shamir's 3-Pass Protocol
(Mechanical scenario)

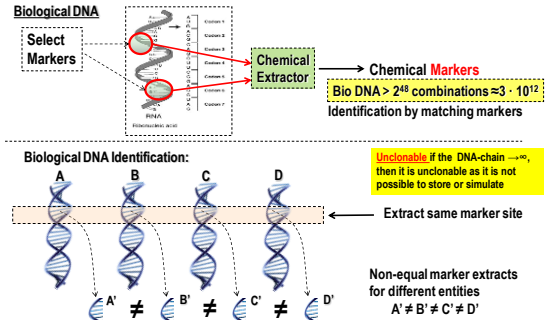


5. Physical Security

DNA-like Identity for Physical Units

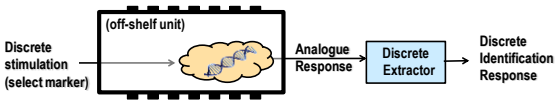
- Unclonable Physical Units (PUFs)
- Clone-Resistant Physical Units

Unclonable physical Identity: the born DNA-like as provable identity



Electronic born DNA-like identification

PUF: Physically Unclonable Functions



Physical Unclonable Functions PUFs offer DNA like Identification Properties

PUFs are: Born unpredictable and unclonable physical VLSI properties.
In other words: PUFs are physical non-linear, unpredictable huge mappings (impossible to model or simulate) in a semiconductor VLSI device

Course objectives

- The aims of this course is to give a basic understanding of the design fundamentals and tools used in modern information security systems
- Some contemporary standards would be introduced to enhance technical and practical understanding

Course strategy: less proofs, more practical design hints targeting to offer security engineering skills!

The course start with introducing basic mathematics for cryptography