# Introduction to Cryptography

All copyrights for the slides remain with Christof Paar and Jan Pelzl.

# INDEX

- Introduction
- Classification of the field of Cryptology
- What is Cryptography?
- Purpose Of cryptography
- Symmetric Cryptography
- Types of Cryptography
- Process of cryptography
- Conclusion
- References

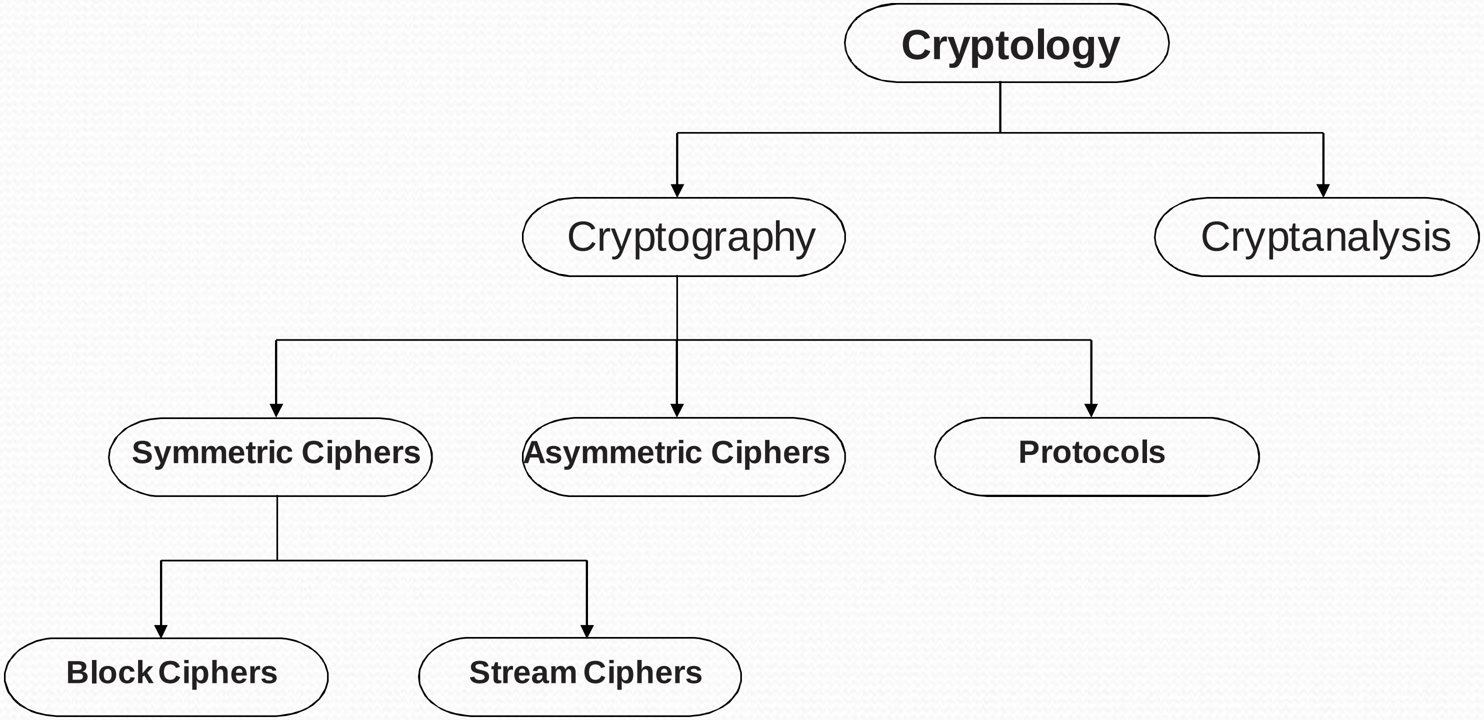
## INTRODUCTION

- The **Internet** is the internationally connected network of computer networks with addresses that are administrated by IANA (Internet address and Naming Authority).

- There are many aspects to security and many applications, reaching from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of **cryptography**.

All copyrights for the slides remain with Christof Paar and Jan Pelzl.

# Classification of the Field of Cryptology



Cryptology is the mathematics, such as number theory, and the application of formulas and algorithms, that underpin cryptography and cryptanalysis.

# What is Cryptography?

- Cryptography derived its name from a Greek word called "**krypto's**" which means "**Hidden Secrets**".

- Cryptography is the practice and study of hiding information. It is the Art or Science of converting a plain intelligible/understandable data into an unintelligible/meaningless data and again retransforming that message into its original form.

- It provides Confidentiality, Integrity, and Accuracy.

# PURPOSE OF CRYPTOGRAPHY

- **Authentication:** The process of proving one's identity. Both the sender and receiver need to confirm the identity of other party involved in the communication.
- **Privacy/confidentiality:** Ensuring that no one can read the message except the intended receiver.
- **Integrity:** Assuring the receiver that the received message has not been altered in any way from the original.
- **Non-repudiation:** A mechanism to prove that the sender really sent this message. Non-repudiation is the assurance that someone cannot deny the validity of something. Digital signatures can offer non-repudiation when it comes to online transactions.

## Some Basic Facts

- **Ancient Crypto:** Early signs of encryption in Eqypt in ca. 2000 B.C.

Letter-based encryption schemes (e.g., Caesar cipher) popular ever since.

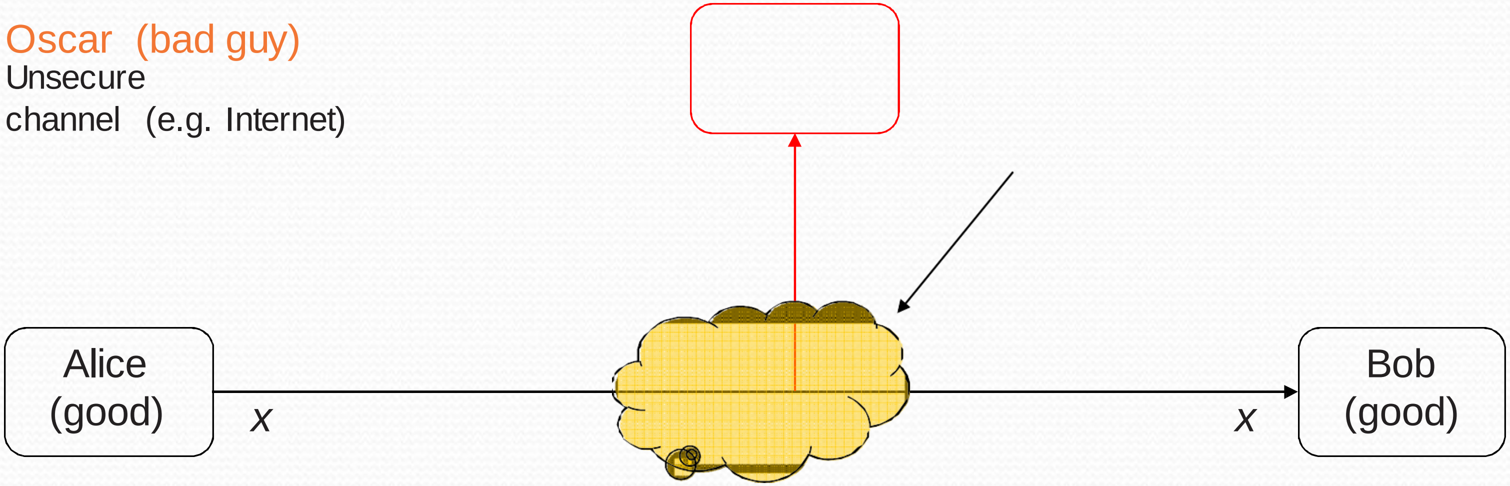
- **Symmetric ciphers:** All encryption schemes from ancient times until 1976 were symmetric ones.

- **Asymmetric ciphers:** In 1976 public-key (or asymmetric) cryptography was openly proposed by Diffie, Hellman and Merkle.

- **Hybrid Schemes:** The majority of today's protocols are hybrid schemes, i.e., the use both
  - symmteric ciphers (e.g., for encryption and message authentication) and
  - asymmteric ciphers (e.g., for key exchange and digital signature).

## Symmetric Cryptography

- Alternative names: **private-key**, **single-key** or **secret-key** cryptography.



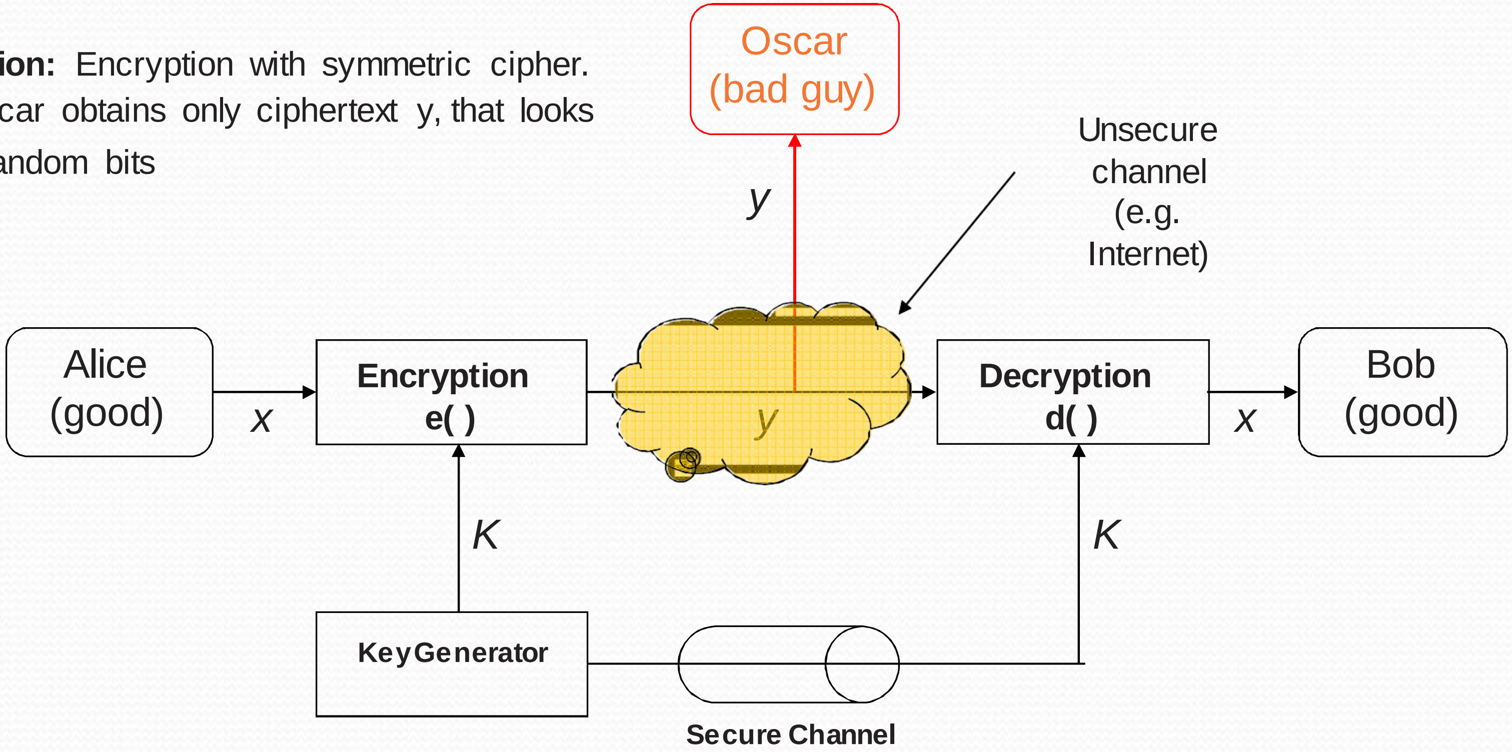
Oscar (bad guy)

Unsecure channel (e.g. Internet)

- **Problem Statement:**
  1) Alice and Bob would like to communicate via an unsecure channel (e.g., WLAN or Internet).
  2) A malicious third party Oscar (the bad guy) has channel access but should not be able to understand the communication.

## Symmetric Cryptography

**Solution:** Encryption with symmetric cipher. ⇒ Oscar obtains only ciphertext y, that looks like random bits



- x is the. **plaintext**
- y is the **ciphertext**
- *K* is the **key**
- Set of all keys {*K*1, *K*2, ...,*Kn*} is the **key space**

# Types of Cryptography

**Secret Key Cryptography**

- Single key used to encrypt and decrypt.
- Key must be known by both parties.
- Assuming we live in a hostile environment (otherwise - why the need for cryptography?), it may be hard to share a secret key.

## Symmetric Cryptography

- Encryption equation $y = e_K(x)$
- Decryption equation $x = d_K(y)$

- Encryption and decryption are inverse operations if the same key K is used on both sides: $d_K(y) = d_K(e_K(x)) = x$

- Important: The key must be transmitted via a **secure channel** between Alice and Bob.
- The secure channel can be realized, e.g., by manually installing the key for the Wi-Fi Protected Access (WPA) protocol or a human courier.
- However, the system is only secure if an attacker does not learn the key K!

**⇒ The problem of secure communication is reduced to secure transmission and storage of the key K.**

# Why do we need Cryptanalysis?

- There is no *mathematical proof of security* for any practical cipher
- The only way to have assurance that a cipher is secure is to try to break it (and fail) !

**Kerckhoff's Principle** is paramount in modern cryptography:

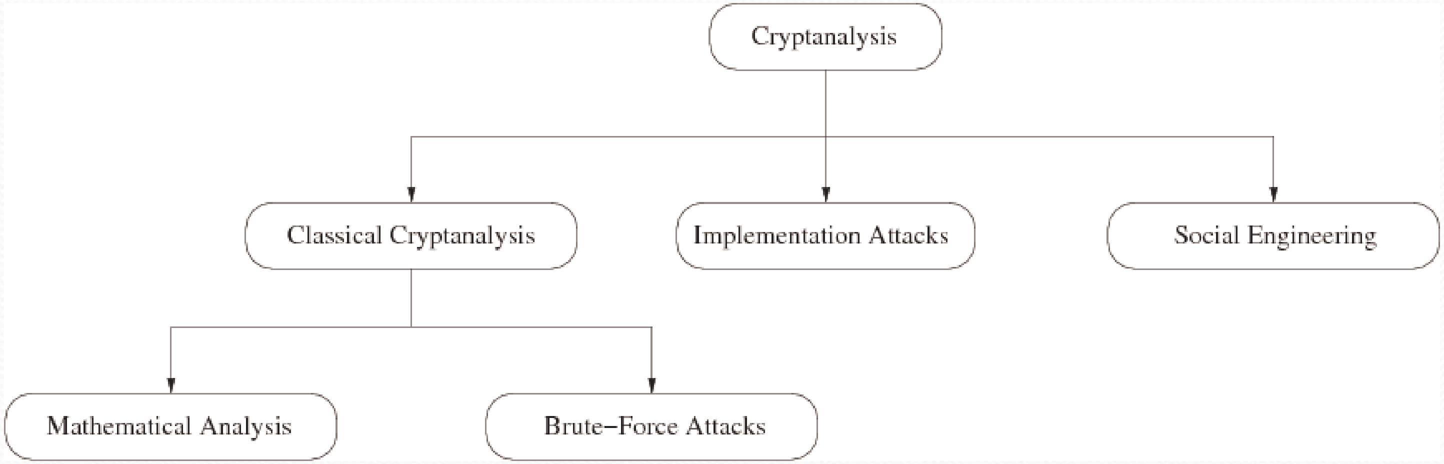
> A cryptosystem should be secure even if the attacker (Oscar) knows all details about the system, with the exception of the secret key.

- In order to achieve Kerckhoff's Principle in practice:

**Only use widely known ciphers that have been cryptanalyzed for several years by good cryptographers!** (*Understanding Cryptography* only treats such ciphers)

- **Remark:** It is tempting to assume that a cipher is „more secure" if its details are kept secret. However, history has shown time and again that secret ciphers can almost always been broken once they have been reversed engineered. (Example: Content Scrambling System (CSS) for DVD content protection.)

# Cryptanalysis: Attacking Cryptosystems



- **Classical Attacks**
  - Mathematical Analysis
  - Brute-Force Attack
- **Implementation Attack**: Try to extract key through reverse engineering or power measurement, e.g., for a banking smart card.
- **Social Engineering**: E.g., trick a user into giving up her password

# References

- www.researchgate.net
- www.swayam.com
- www.wikipedia.com

# THANKS….!!!

- Any Query