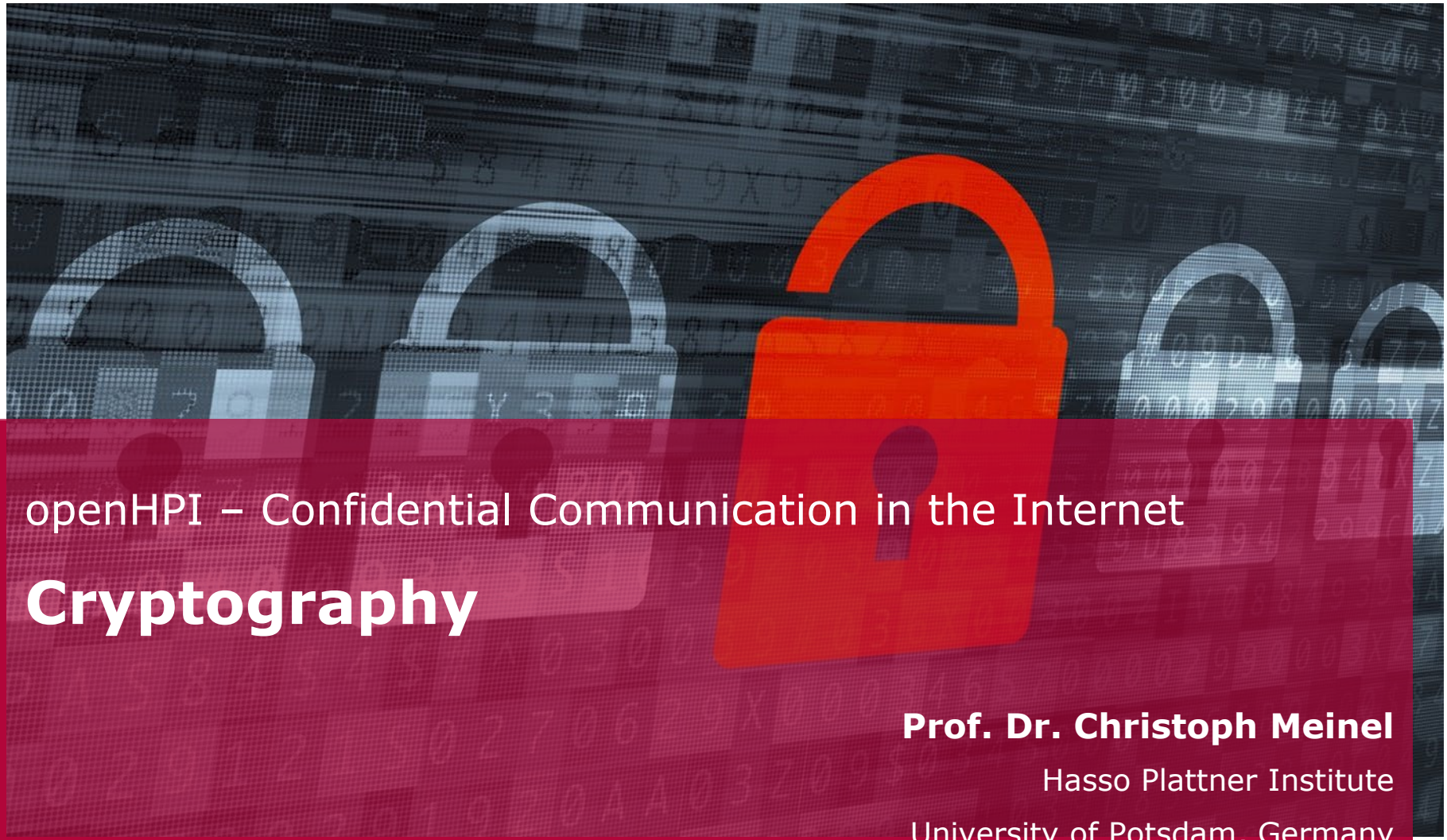


openHPI – Confidential Communication in the Internet

Cryptography

Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

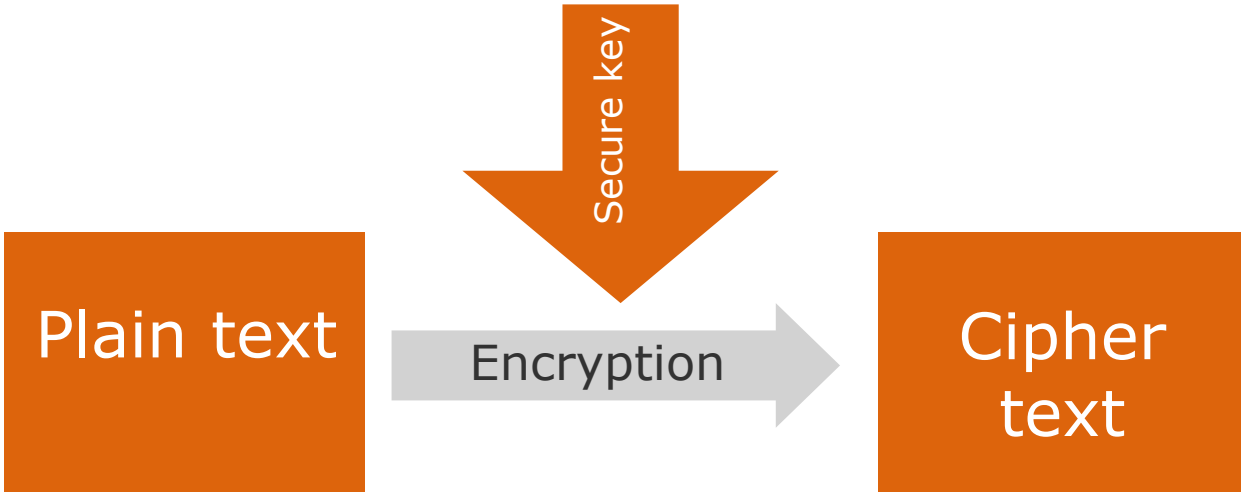
Cryptography – Science of Encoding and Decoding Information (1/2)

Basic idea:

"**Encryption**" - makes information incomprehensible to unauthorized outsiders

- Only insiders who know how to reverse the encryption can "**decrypt**" information
- Encryption and decryption are carried out using cryptographic methods which can be controlled by parameters, so-called "**keys**"

Cryptography - Science of Encoding and Decoding Information (2/2)



Example with DES encryption algorithm:

- Message: "*This is a confidential message!* "
- Key: "secure key"
- Encrypted message – cipher text:

FH64hpCiT/Q3SnMBcQvjjgTEm68PD25KJDOLwKtKOcJz8qgewQCgcQ==

Requirements for Cryptographic Procedures: **Kerckhoffs' Principle**

Auguste Kerckhoffs (1835-1903):

- Security of a cryptographic process should only be based on the secrecy of the keys and not on the secrecy of the cryptographic process

Justification:

- Independent experts can always check the procedure for weaknesses

Cryptography
Symmetric Encryption Methods …

… use the same key for encryption and decryption

Attention:

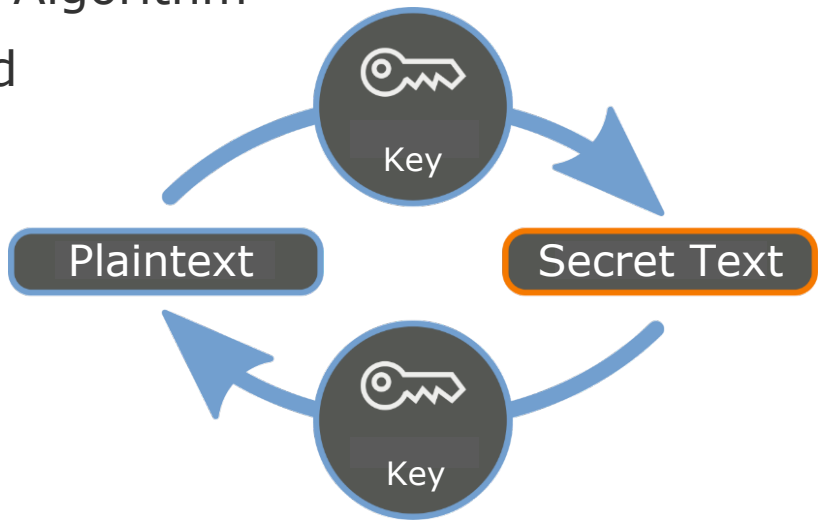
Only sender and receiver may know this key

Known symmetrical encryption methods:

- DES – Data Encryption Standard
- IDEA – International Data Encryption Algorithm
- AES – Advanced Encryption Standard

Fundamental problem:

- How to securely exchange the encryption key?



Cryptography
Hash Procedures (1/2)

In information security, hash methods are used to generate "**fingerprints**" for documents, which characterize the possibly large document by a limited number of characters as unambiguously as possible

Objectives:

- Compression of a document to a **fixed length**, for example 160 bits, which "practically" cannot be undone ("**one-way hash function**")
- It should be very difficult to find a second document with the same hash value ("**collision resistance**")

Cryptography
Hash Procedures (2/2)

Hash functions which are currently regarded as secure:

- RIPEMD-160 (Dobbertin, Bosselaers, Preneel 1992)
- SHA-256:
  - **SHA(„abcd“)**: 88d4266fd4e6338d13b845fcf2…
  - **SHA(„abcde“)**: 36bbe50ed96841d10443bcb67…
- SHA-512
- …

Hash methods still used, but not considered safe today:

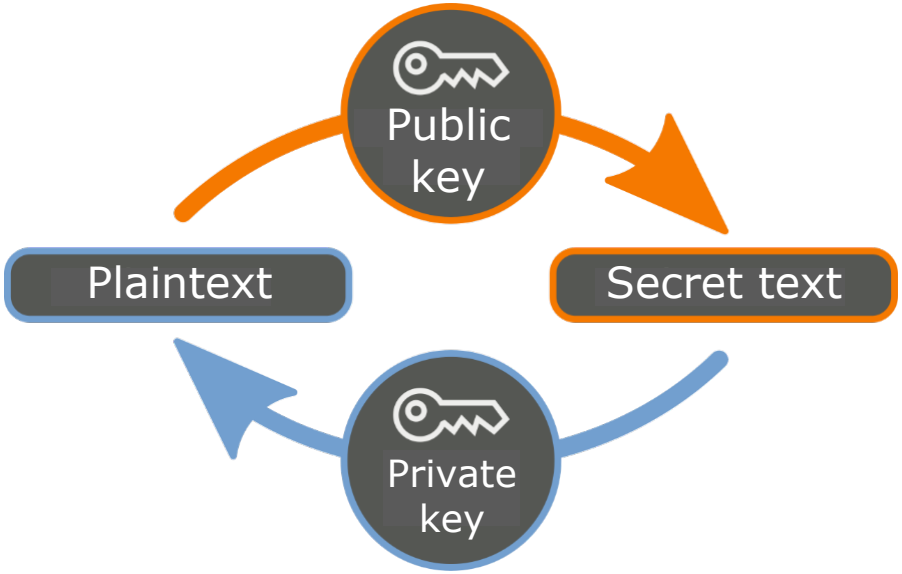
- MD4, MD5 (Rivest 1990/1991)
- RIPEMD-128 (Dobbertin, Bosselaers, Preneel 1992)
- SHA (NSA 1992)
- …

Asymmetric Encryption Methods …

… use two different keys for encryption and decryption

Every user gets

- A secret key – "**private key**"
- A public key – "**public key**"



Cryptography
Asymmetric Encryption Methods (2/4)

Important:

- **Public key** is published, everyone can / should know it
- **Private key**: **Must remain absolutely secret**
- Must not be derivable from public key by calculating

Asymmetric Encryption Methods (3/4)

Application example 1: Encryption

- Encryption is done with the **public key of the recipient**
- Decryption with **private key** of the recipient

Only the **recipient** can decrypt the message

Asymmetric Encryption Methods (4/4)

Application example 2: **Digital signature**

- Document is encrypted with the **signee's private key**
- The signee's public key can be used to decrypt the encrypted documents

Successful decryption of the message proves that the message is coming from the signee. Only he/she has the associated private key

Brute Force Attacks on Encryption

Any symmetric or asymmetric cryptographic encryption method can be cracked by **Brute-Force Attacks**:

- Attacker systematically try our **all theoretically possible keys** until a meaningful text is obtained

The only protection against brute force attack:

- The number of possible keys must be so large that **systematic testing is practically impossible**, i.e. takes thousands of years …

Important Differences between Symmetric and Asymmetric Encryptions

- Symmetrical procedures, also called **secret key procedures**, are based on very simple mathematical functions
- Asymmetric procedures, also known as **public key procedures**, are based on very complex mathematical facts
- Public key procedures require considerably more **computing power** than secret key procedures and are **more susceptible to implementation errors**
- In case of secret key procedures, key, plaintext, ciphertext are considered as bit strings,
  in case of public key procedures as large numbers