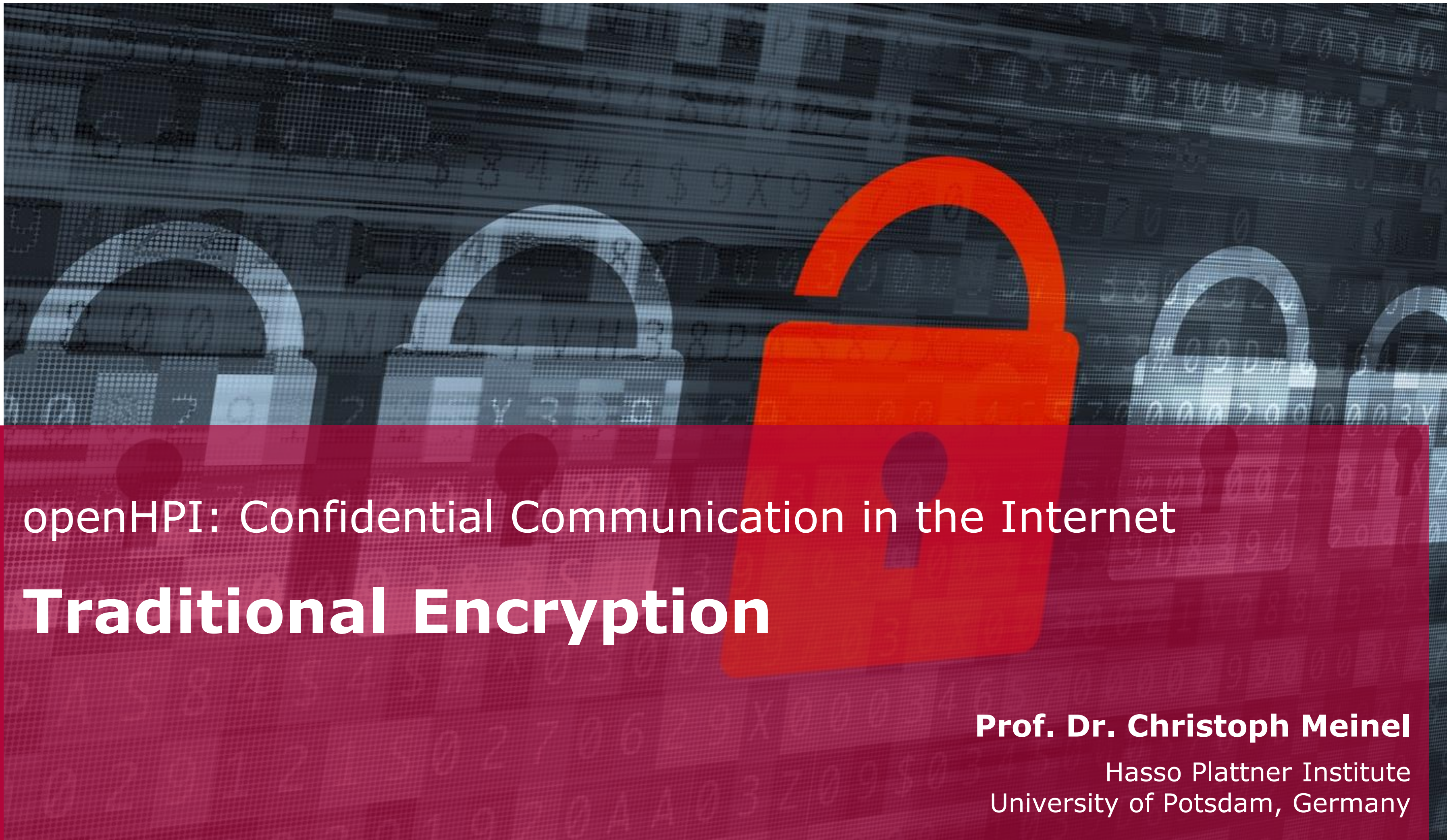


openHPI: Confidential Communication in the Internet

Traditional Encryption

Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

Substitution Ciphers (1/3)

In a **substitution cipher,** each letter of the plain text is replaced by a different letter of the alphabet

Example: **Shift ciphers**

The cipher text is generated by shifting the letters of the plaintext by n positions in the alphabet

- **Caesar cipher**: Each character is moved 3 positions, e.g. hello → khoor
- **Key**: n with $1 \leq n \leq 26$, **Number of keys**: 26

Symmetric Cryptography
Substitution Ciphers (2/3)

Possible attacks on shift ciphers:

- Small number of keys makes brute force attack simply possible
- Successful attacks on cipher text are possible

Frequency Analysis

Idea:

- Not all letters appear in the plaintext with the same frequency (applies to all languages), e.g. "e" comes in English texts most frequently (11%), then “a" (8%) and “r" (7%), ...
- Number of occurrences of individual letters in the cipher text enables determination of the shift key

Example: Permutation ciphers

The cipher text is generated by applying to the plaintext a fixed permutation of the letters of the alphabet:

- Permutation $\boldsymbol{\pi}$: Alphabet → Alphabet

  $$Z \rightarrow \boldsymbol{\pi}(Z), \quad \boldsymbol{\pi} \in \mathrm{Perm}_{\text{Alphabet}}$$

- Key: $\boldsymbol{\pi}$
- Number of keys: (#alphabet)!

  I.e. 26! > 400 quadrillion (4 * 10^{26})

Polyalphabetic Ciphers (1/4)

A substitution cipher is called a **polyalphabetic cipher**, if a letter of the plaintext may be replaced by different letters during encryption

Examples:

(1) Homophonic ciphers:

- Frequently occurring letters are encoded by different characters, so that each character in the cipher text occurs equally often, e.g.
  - "e" is encrypted by 11 different characters
- **Attacks**:
  - Statistical evaluation of frequent letter combinations

Polyalphabetic Ciphers (2/4)

Examples:

(2) Vigenère cipher

Idea:

- By constantly repeating an agreed keyword, a key text is generated in the length of the plaintext. The cipher text is obtained by "adding" the plaintext and the key text letter by letter
- **Example**:

  Keyword: `secretkey`
  Plain text: **`state secret`**
  Keyword: **`secretkeysecret`**
  Ciphertext: **`kxcki logpwx`**

Polyalphabetic Ciphers (3/4)

Examples:

(3) One-time pad (1/2)

- Special case of the Vigenère cipher:
  - Choice of a purely random sequence of letters of unlimited length as keyword ...
- Most frequent application:
  - Encryption of messages via **binary alphabet {0,1}**
- **Theorem**:
  - One-time pads, which are operated with true random sequences, have perfect security

Polyalphabetic Ciphers (4/4)

Examples:

(3) One-time pad (2/2):

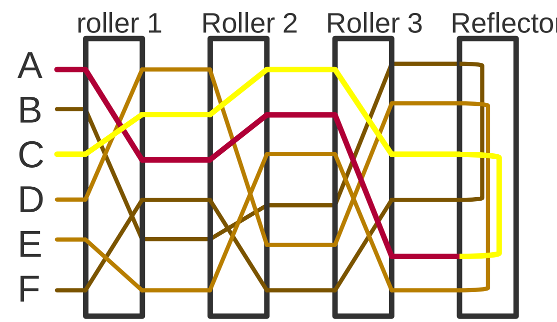
- Advantages:
  - Very simple procedure, can be used even by laymen with paper and pencil. Agents always carry a sealed envelope with a longer random sequence for emergencies ...
- Problems with the application:
  - Very complex to generate **real random sequences**
  - Very complex **key exchange** due to the key length
  - Transmitter and receiver must store very long keys

Symmetric Cryptography
Rotor Ciphers and Enigma

Hasso Plattner Institut

Historical facts:

- As late as the 1st World War, radio messages were encrypted with the further developed Vigenère cipher
- Around 1918, the **rotor ciphers** became independently invented by at least four different inventors
- The most famous representative of the rotor ciphers was the **Enigma** encryption machine used by the German Wehrmacht in the Second World War



Excursus on
Rotor Ciphers and the Enigma!