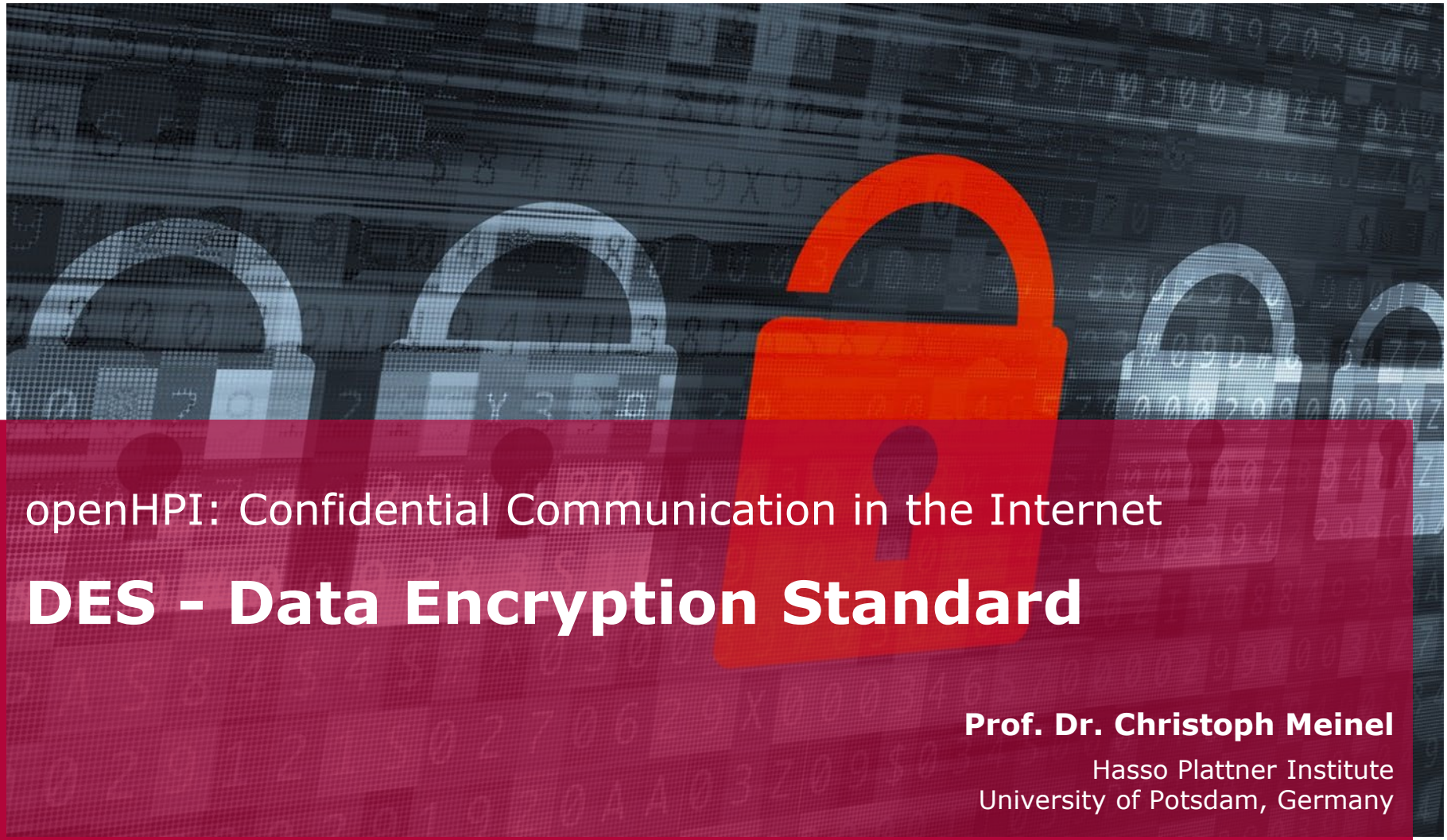


openHPI: Confidential Communication in the Internet

DES - Data Encryption Standard

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

Block Ciphers

With a block cipher, plaintext is split into blocks and then encrypted in blocks

Shannon calls for good encryption

- **Confusion** – cipher text should be a sequence of random letters and
- **Diffusion** - each plaintext bit should influence as many cipher text bits as possible during encryption

Good compromise between confusion and diffusion:

Block length 64

- Number of possible keys ≈ 18 trillion
- Many of the possible keys are far too long for practical use!

DES - Data Encryption Standard (1/9)

DES has **long** been the most popular symmetric encryption

- Developed in the early 70s by Horst Feistel at IBM
- Recognized as a standard for data encryption by the US standardization authority NIST in 1977 after a public tendering process (Kerckhoffs principle)
- Re-certification after every 5 years is mandatory (last certification in 1993)
- 1981 also by ANSI (American National Standards Institute) recognized as an encryption standard

DES is the basis of many real live application:

- PIN encryption
- financial transactions
- key distribution

DES - Data Encryption Standard (2/9)

Overview of how it works (1/2):

XOR	0	1
0	0	1
1	1	0

- DES encryption uses only the following very simple operations:
  - exclusive-or (XOR)
  - permutation (sequence in a bit sequence is changed)
  - substitution (bit sequence is replaced by others)
- DES is a combination of one-time pad, permutation and substitution cipher
- Applied operations have been selected to be able to implement it very effectively in hardware

DES - Data Encryption Standard (3/9)

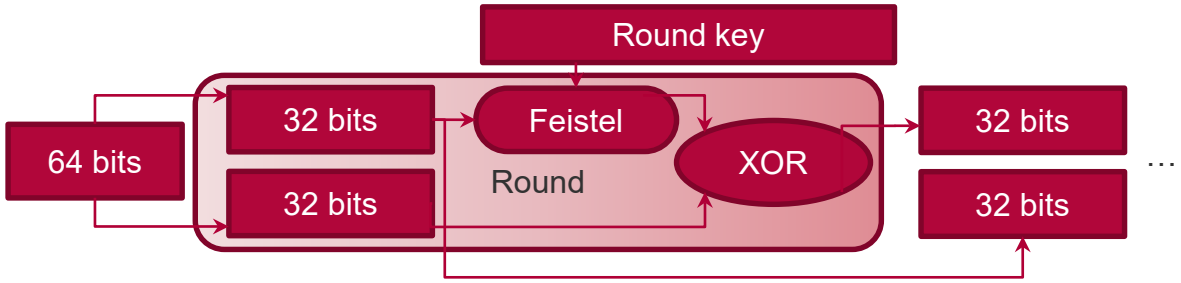
Overview of how it works (2/2):

- In DES, keys have a length of 64.
  8 bits of which are used as a checksum, i.e.
  the actual key length of DES is **56 bits**,
  so there are ≈72 quadrillion possible keys ...
- Plain text is divided into 64-bit blocks, i.e.
  - 8 letters at 8 bits per character
- Each block is processed in 16 rounds
- Ciphertext is also block of length 64

DES - Data Encryption Standard (4/9)

The 16 rounds of DES (1/2):

- Input is broken down into 64-bit blocks
- 64-bit block is divided into two 32-bit blocks
- The "**Feistel**" function is applied to one of the sub-blocks
- Both blocks are linked with XOR operator and
- Swapped with each other for the next round

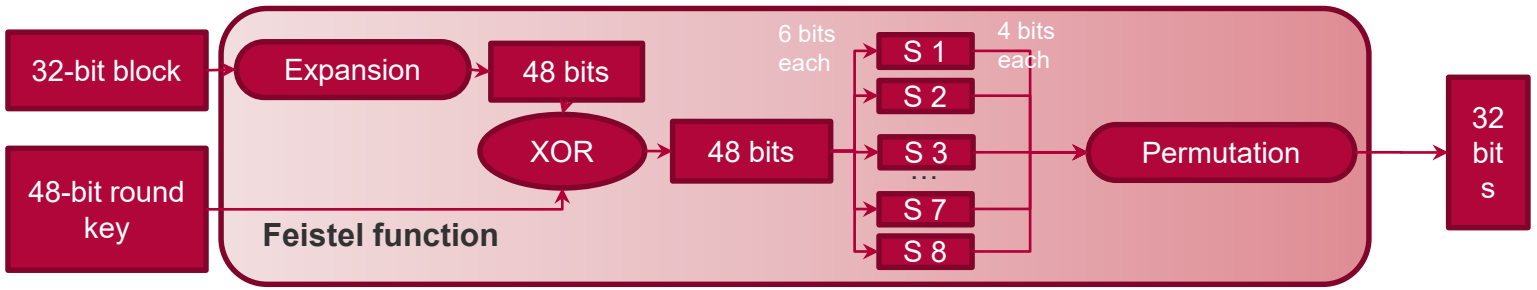


DES - Data Encryption Standard (5/9)

The 16 rounds of DES (2/2):

"**Feistel**" **function:**

- 32-bit block is expanded to 48-bit and XORed with 48-bit **partial key** (round key)
- 6 bits each are compressed to 4 bits with S-Boxes (substitution boxes)
- 32 bits are re-sorted with a permutation
- Permutation and substitution allow **diffusion** & **confusion**



DES - Data Encryption Standard (6/9)

Decryption of DES:

- For decryption, the same algorithm can be used as for encryption, only the partial keys must be applied in reverse order (shift to the right instead of to the left)

Attention:

- Weak keys (few differences, recurring bit patterns), avoid making partial keys different

DES - Data Encryption Standard (7/9)

Crypto analysis of DES (1/2):

- DES provides confirmation for Kerckhoff's principle:
  - Disclosure of the algorithm increases its security
- Even after more than 30 years, crypto analysts have not found a weakness in DES
- Only **brute-force attacks** have reached their goal since the middle of the 90s due to the greatly increased performance of computers

DES - Data Encryption Standard (8/9)

Cryptanalysis of DES (2/2):

"**DES-Challenge**" - Company RSA Data Security offered 10,000 US dollars to decrypt DES

- 1997: First successful (public) Known Plaintext attack:
  - Key is cracked with the help of 14,000 PCs distributed on the Internet over a period of 4 months
- Early 1998: Decoding after 39 days
- Mid 1998: Decryption in 56 hours using a $250.000 expensive special computer
- 1999: Decryption by 100,000 Internet users in 22 hours

DES - Data Encryption Standard (9/9)

Weaknesses of DES:

- Designed for hardware implementation, in software the process is relatively slow ..., e.g. permutations ...
- New possibilities in chip design make faster computation possible for hardware as well
- Initial and final permutation do not improve security but slow down software implementations
- Key length too short (56 bit)

3-DES – Further development of DES

Initially try 2-DES

- Dual use of DES with 2 different keys to increase the key space by doubling the length of the key
- Meet-in-the-Middle attack allows calculation of the key in $2^{1+56=57}$ attempts, not $2^{56+56=112}$ as assumed

Better idea: **3-DES**

- Improved process compared to DES by **triple** DES with different keys "**Triple-DES**" s
- Size of the key space:
  - Not $2^{(1+56)}$ as due to the Meet-in-the Middle attack in 2-DES, but $\mathbf{2^{56+56=112}}$