openHPI – Confidential Communication in the Internet

AES - Advanced Encryption Standard

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

AES - Origin (1/2)

Secure successor for DES sought (1/2):

- 1997 by NIST "Call for Algorithms" - Call for proposals for a DES successor

Requirements:

- Well documented block cipher with reference implementation
- Block length: 128 bit
- Variable key lengths: 128, 192 and 256
- Equally feasible in hardware and software
- More efficient than Triple-DES
- Available worldwide licence-free

AES - Origin (2/2)

Secure successor for DES sought (2/2):

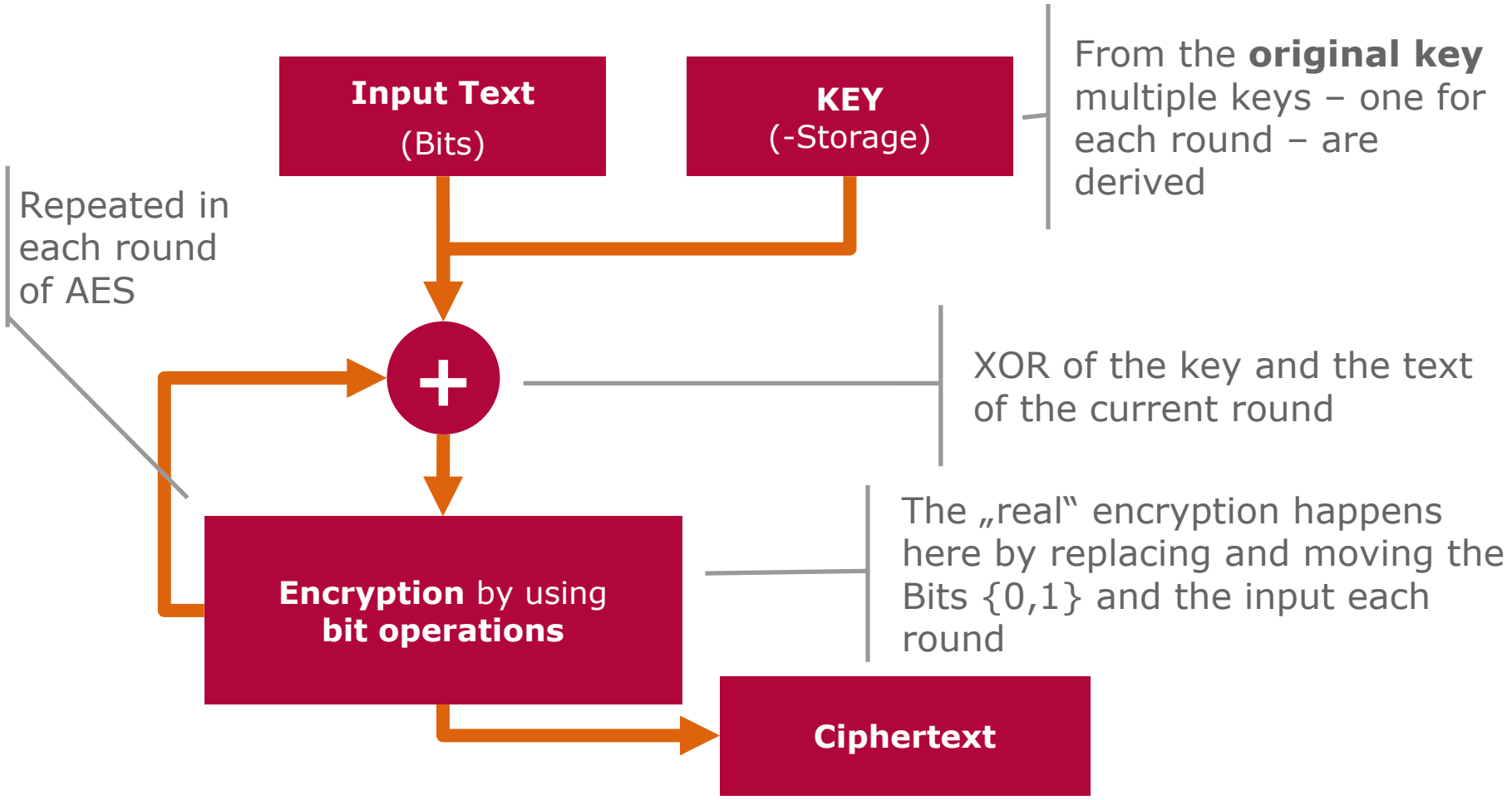
2000 NIST announces the winner: **Rijndael**

- Developed by Vincent Rijmen and Joan Daemen
- Variable block and key lengths: 128, 160, 192, 224, 256 bit
- Fast, simple, little memory space

2001 Rijndael became the **AES standard**

Functionality of AES (1/2)

AES – Abstract Overview



Functionality of AES (2/2)

AES – An Example

- When encrypting

Secure Communication

… with AES:

- **Results:**
  - Key: *password*

pbbnSYHWJjMAMoCW2yGVadq8vl73tOWMu1Grl8rRZpA=

  - Key*: password1*

teuIOxrvv7JhyfX4TuqaZj8aevMVNK7gaSKQa7GDRrE=

In comparison to classic methods, similar keys are producing extremely unique results

AES - Performance

Performance by AES:

- Many times faster than DES:
  - With block length 256 bit and key length 192 bit:

    4 core computers with 3.4GHz: 1033 MB/sec
- AES can be easily parallelized
- Easy to implement in hardware, because
  - only simple operations (XOR, cyclic shifts)
  - operations can be efficiently computed by 8-bit processors and on smart cards