openHPI – Confidential Communication in the Internet

Crypto Patents and Standards

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

Introduction

In daily practice, cryptography is constantly evolving:

- New cryptographic knowledge and procedures are published in **scientific publications** or applied for a **patent**
- Cryptographic processes must be interoperable in the context of their various applications
  - to achieve this, various specifications and fixations, so-called **standards**, must be agreed upon
  - **standards** then also be adhered to the various software providers
- Use of cryptographic methods and implementation in crypto products (special hardware and/or software) should be carried out in compliance with the relevant standards whenever possible

Crypto Patents (1/2)

Many cryptosystems and crypto algorithms are patented

Five particularly important crypto patents:

- **DES** block ciphers
  (1976, Ehrsam, Meyer, Powers, Smith, Tuchman, IBM)
- First public key patent: **Diffie-Hellman Key Exchange** (1980, Hellman, Diffie, Merkle, Stanford)
- **Merkle-Hellman Knapsack** and **PKI**
  (1980, Hellman, Merkle, Stanford Junior University)
- **Tree authentication method**
  (1982, Merkle, Stanford University)
- **RSA** encryption and signature
  (1983, Rivest, Shamir, Adleman, MIT)

Crypto Patents (2/2)

Other significant crypto patents:

- Generation of **RSA prime numbers**
  (1986, Hellman, Bach)
- **One-Time Signatures**
  (1989, Merkle)
- **IDEA** cipher
  (1993, Massey, Lai, ASCOM Tech AG Bern)
- **DSA** signatures
  (1993, Kravitz, Chamber of Commerce, Washington)
- Modulo Arithmetic Processing Chip
  (auch **Elliptic Curves**, 1993, Cylink)
- **IBE - Identity Based Encryption**
  (2007, Voltage)

Crypto Standards (1/2)

Important security standards of NIST:

- **AES** (October 2000)
  - Advanced Encryption Standard
  - Symmetric encryption method as successor of DES and 3DES
- **SHA** - Family
  - Group of Hash Algorithms
- SHS (2015)
  - Secure Hash Standard - Defines the use of hash functions
- **DSA** (1991)
  - Algorithm for digital signatures

Crypto Standards (2/2)

Important security standards for banks

- **DES**:
  - ANSI X3.92, ANSI X9.9, ANSI X9.52
- **PIN** management:
  - ISO 9564, ANSI X9.8
- **Signatures**:
  - ANSI X9.30, ANSI X9.31
- **Certificates**:
  - ANSI X9.45, ANSI X9.57, ISO 10202