FRI3D 2026

Cryptography: For Kids and Managers

About me

- Jürgen Pabel
- IT-Security-Management guy at day, hacker/maker at night

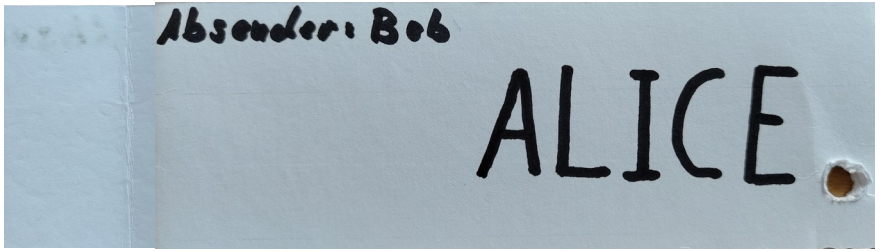
A very first look

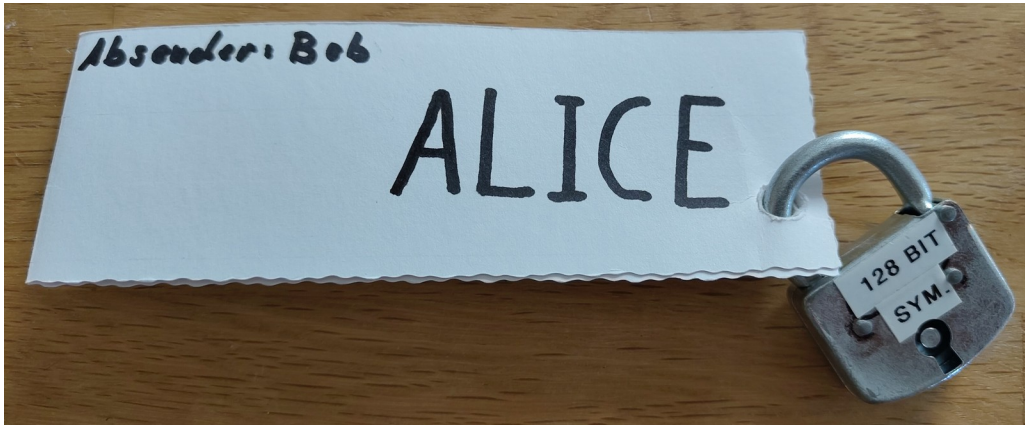
- The three “classic” security goals
  - Confidentiality
  - Integrity
  - Availability
- Encryption
  - Prevents “others” from viewing the contents (confidentiality)
- Signatures
  - Prevents “others” from modifying the contents (integrity)

Before we continue...let’s get to know….

- Alice
- Bob
- Malory

Encryption



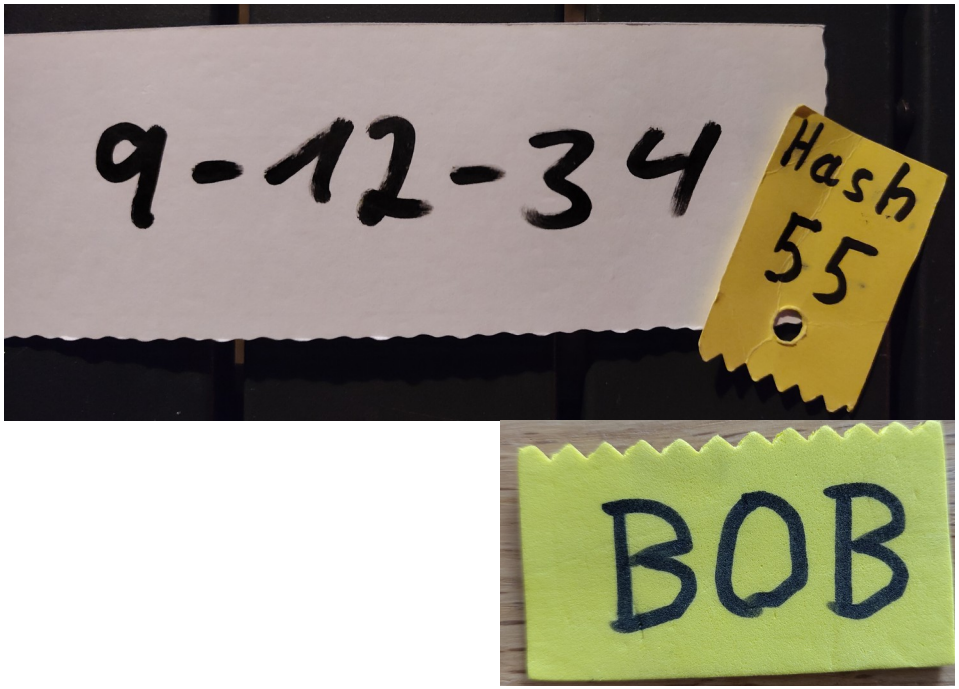


Hashes

- Hashes convert (any) input data into a (fixed) length output value
  - Cross sum: 9 – 12 – 34 = 9+12+34 = 55
    - Not collision resistant: 1 – 5 – 49 = 55

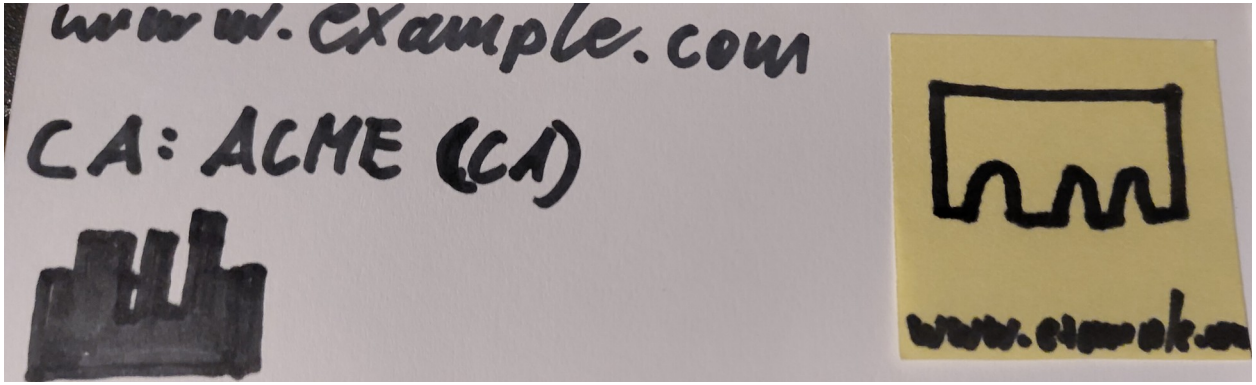
- Cryptographic hashes are collision resistant
  - MD5: 128 bit (collisions resistance fully broken)
  - SHA-1: 160 bit (collision resistance mostly broken)
  - SHA-2: 256/384/512 bit
  - SHA-3: 224/256/384/512 bit

Signatures



Certificates

- National-IDs are issued by the government and declare identities
- Certificates are issued by certificate-authorities (CAs) and declare identities



That’s it

- Everything beyond this point is expert-knowledge

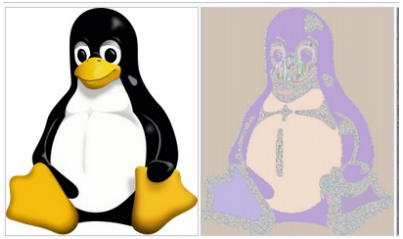
Encryption: 1970s break-through

- Symmetric encryption

- Asymmetric encrytion

(Symmetric) Encryption ciphers

- Stream ciphers
  - Encrypt byte-by-byte
  - Problem: Inherently insecure
- Blocker ciphers
  - Encrypt block-by-block
  - Problem: Insecure by default



Ask me anything...some ideas

- Hashes
  - Salting
  - Peppering
  - Rainbow tables
  - PBKDF
- Block-Cipher-Modes
  - Initialization vectors
  - Padding
- Certificates
  - Root-CAs
  - Certificate Transparency
  - Revokation
  - Let’s encrypt
- Randomness
- Zero-Knowledge-Proofs