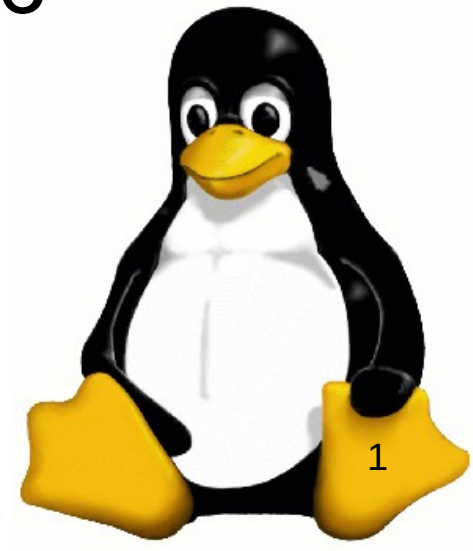
Kryptographie

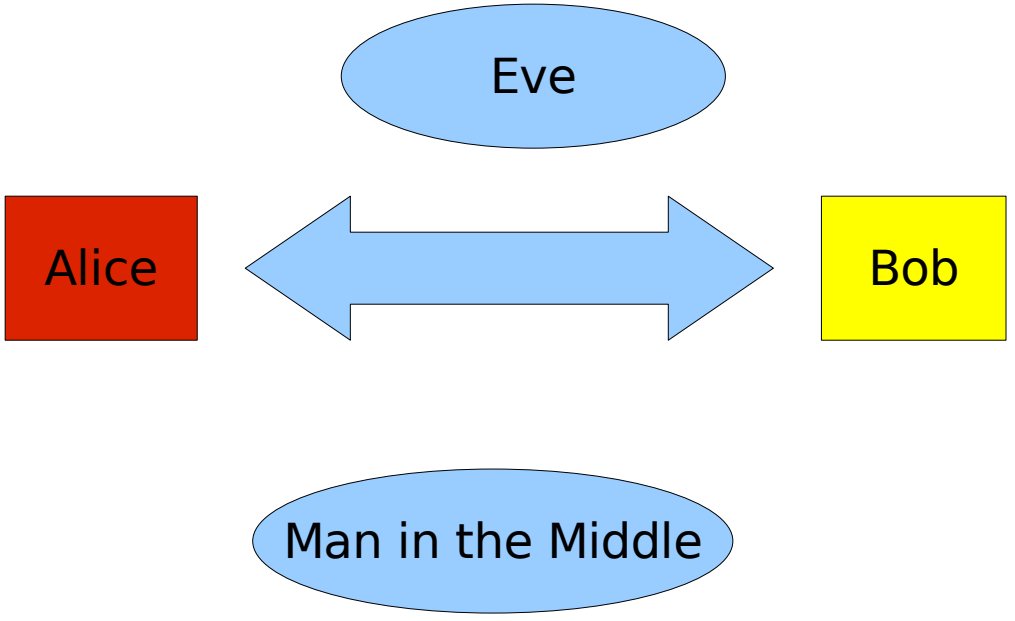
Manuel Blechschmidt
&
Volker Grabsch
CdE Sommerakademie 2006
Kirchheim



Gliederung

- Ausgangslage
- Verschlüsselung
- Verfahren
  - Symmetrische Verfahren
  - Public Key
- Standards
  - S/MIME, PGP - Emails
  - SSL - Websites
- Certified Authorites

Ausgangssituation



Verschlüsselung

- Sinn
  - Geheime Botschaften austauschen
    - Kommunikationskanal ist sicher
  - Identität des Autors sichern
    - Elektronische Ausweise
  - Daten nicht veränderbar

Verfahren

- Symmetrische Verfahren
  - AES
  - 3-DES
  - etc.
- Public Key Verfahren
  - RSA
  - ElGamal
- Hashing Verfahren
  - SHA-1
  - MD5

Symmetrische Verfahren

- Es wird ein Schlüssel gebraucht
- Der Schlüssel wird für Verschlüsselung und Entschlüsselung genutzt
- Alice und Bob müssen sich auf einen Schlüssel einigen
- Schlüsselübergabe unsicher
  - Sicher durch Diffie-Hellmann-Schlüsselaustausch
- Schnell

Public Key

- Asymmetrische Verfahren
- Für Entschlüsselung und Verschlüsselung werden unterschiedliche Schlüssel benutzt
- Jeder hat ein Schlüsselpaar
  - Private Key
  - Public Key
- Public Key wird für alle veröffentlicht

Probleme von PK

- Woher weiß ich, von wem der Schlüssel ist?
- Lösungen:
  - 1. Certified Authorities
  - 2. Web of Trust

Certified Authorities

- Juristische Verantwortung über Information
- Im Browser eingebaut
- Bestimmt durch Distributor
- Beispiele:
  - VeriSign
  - Thatwe
  - TrustCenter Telekom

Web of Trust

- Großes Netzwerk von Leuten
- Jeder kennt jeden über Verbindungen
- Man muss aktiv Schlüssel signieren