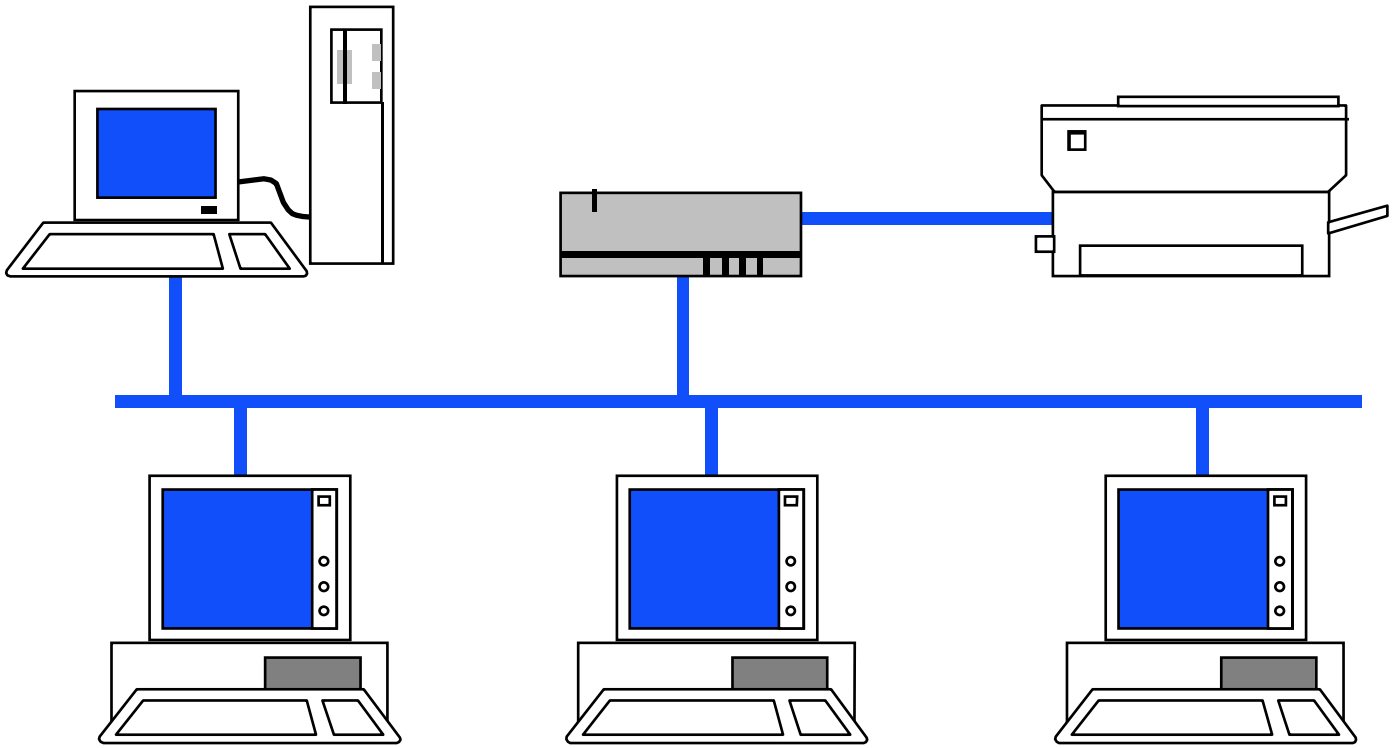
Einführung Verschlüsselung

Mag. Dr. Klaus Coufal



Verschlüsselung

- Symmetrisch
- Asymmetrisch
- Rechenleistung
- Primzahlenzerlegung
- Quantenkryptographie
- Schlüsselverwaltung

Symmetrische Verschlüsselung

- Der Schlüssel für die Verschlüsselung und Entschlüsselung ist gleich und muß daher beiden Kommunikationspartnern bekannt sein.
- Schlüsseltausch problematisch
- Bleibt lange Zeit konstant und ist daher der leichter herauszufinden

Einfachverschlüsselung

- Substitutionsverfahren
  - Cäsarcode, Zeichencodes, ...
- Transpositionsverfahren
  - Permutation, Zick Zack, ...
- Kombinationen daraus

Private Key Verfahren

- Polyalphabetische Substitution
- Produktverschlüsselung
- Blockverschlüsselungen
  - ECB (Electronic Code Book)
  - CBC (Cipher Block Chaining)
  - CFB (Cipher Feed Back)
  - OFB (Output Feed Back)
- Bitstromverschlüsselungen

Asymmetrische Verschlüsselung

- Bei der asymmetrischen Verschlüsselung sind die Schlüssel für die Verschlüsselung bzw. Entschlüsselung verschieden
- Kein Schlüsseltausch notwendig
- Einer der beiden Schlüssel wird öffentliche verfügbar (public) gemacht.

Public Key Verfahren

- Merkel Hellman Verfahren
- RSA (Rivest, Shamir, Adleman, 1978) Verfahren
- Für verschlüsselte Kommunikation wird der Verschlüsselungsschlüssel „public“
- Für die digitale Unterschrift wird der Entschlüsselungsschlüssel „public“

DES

- DES (Data Encryption Standard)
  - Amerikanischer Standard, in Polen entwickelt, Chip unterliegen dem Exportembargo
- 3DES (Triple-DES)

Sicherheit – RSA

- $\text{Schlüsseltext} = \text{Klartext}^{e} \pmod{n}$
- $\text{Klartext} = \text{Schlüsseltext}^{d} \pmod{n}$
- (e,n) Public Key
- (d,n) Secret Key
- n ist das Produkt zweier sehr großer Primzahlen (100-stellig und mehr)

Zahlenbeispiel

- p=11, q=19 und e=17
- $\Rightarrow$ n=209, d=53
- Klartext 5 ergibt Schlüsseltext 5^{17} (mod 209) = 80
- und Schlüsseltext 80 ergibt Klartext 80^{53} (mod 209) = 5
- Kann durch Faktorisieren von n gebrochen werden (zeitaufwendig)

Sicherheit – PGP

- PGP ist eine Anwendung des RSA-Verfahren, daß diese Methode in das e-Mail-System (den Client) einbindet bzw. beliebige Texte über die Zwischenablage behandeln kann.
- lokale Schlüsselverwaltung integriert
- Verschlüsselung und Signatur möglich

Rechenleistung

- Mit steigender Rechenleistung (Taktrate, Parallelisierung) wird das Brechen der Verschlüsselung in kürzerer Zeit möglich.
- Mit steigendem Hauptspeicher ebenfalls, da vorberechnete Tabellen zum Einsatz kommen können.

Primzahlenzerlegung

- Der Schutz der meisten bestehenden Verfahren beruht darauf, daß die Primzahlenzerlegung (Faktorisierung) von großen Zahlen sehr zeitaufwendig ist.
- Das ist aber weder bewiesen noch widerlegt!

Quantenkryptographie

- Quantencomputer ermöglichen eine einfache Faktorisierung auch großer Primzahlen.
- Quantenkryptographie gilt derzeit als unknackbar, da jeder Versuch die Daten abzufangen diese zerstört.

Schlüsselverwaltung 1

- Das verbleibende Problem ist die Schlüsselverwaltung
- Wie kann sichergestellt werden, daß bestimmter Schlüssel zu einer bestimmten Person gehört?
- Persönliche Übergabe weltweit?
- Übertragung über e-Mail?

Schlüsselverwaltung 2

- Zentrale hierarchische Schlüsselverteilung