Kryptographie

ein erprobter Lehrgang

AG-Tagung Informatik, April 2011
Alfred Nussbaumer, LSR für NÖ

Variante: Kryptographie in 5 Tagen

- Ein kleiner Ausflug in die Mathematik (Primzahlen, Restklassen, Stochastik)
- „Klassische“ Verschlüsselungsverfahren
- Asymmetrische Verfahren (Zahlentheorie/Primzahlen, Diffie-Hellman Schlüsseltausch, Elgamal, Digitale Unterschrift, RSA, Fiat-Shamir Nullwissenprotokoll)
- Hash-Verfahren
- „Moderne“ Verschlüsselungsverfahren (DES, AES, Quantenkryptographie)

Aufgaben der Kryptographie

- Vertraulichkeit
- Integrität
- Authentizität

Ausflüge in die Mathematik

- **Primzahlen**
  - Es gibt unendlich viele Primzahlen, Satz von Euklid
  - Sophie-Germain-Primzahlen (2p + 1)
  - Primzahlfaktorisierung
  - Der kleine Fermat: $a^{p-1} \equiv 1 \pmod{p}$, falls a kein Vielfaches von p
  - Satz von Euler: $a^{\varphi(n)} \equiv 1 \pmod{n}$

Ausflüge in die Mathematik

- **Restklassen**
  - Restklassenarithmetik
  - Zyklische Gruppe
  - Erzeugende Elemente
  - Diskreter Logarithmus – Problem, Einwegfunktion
- **Stochastik**
  - Häufigkeitsanalyse
  - Nullwissenprotokoll

Erkenntnisse aus den „klassischen Verfahren“

- Sender – Empfänger, Klartext, Schlüssel, Geheimtext
- Symmetrische Verschlüsselung
- Können oft einfach programmiert werden (JavaScript, PHP, Python, Java, …)
- Häufigkeitsanalyse
- Monoalphabetische / Polyalphabetische Verfahren

Diffie-Hellman Schlüsseltausch

- Sicherer Austausch eines Schlüssels
- Fußt auf (großen) Primzahlen, Modul g (erzeugendes Element einer primen Restklassengruppe?), Zufallszahlen a, b …
- Angreifer kennen genau den Algorithmus, aber nicht die (geheimen) Zufallszahlen

Primitivwurzeln für $\mathbb{Z}_p$ (p groß)!!!

(1) p, g .... Primitivwurzel mod p

$2 \leq g \leq p-2$

(2) Alice | Bob

Alice: Zufallszahl

$1 \leq a \leq p-2$

$\alpha = g^a \mod p$

Bob: $1 \leq b \leq p-2$

$\beta = g^b \mod p$

Alice: $\underline{K} = \beta^a \mod p$

$= (g^b \mod p)^a \mod p$

$= (g^b)^a \mod p$

$= g^{ba} \mod p$

Bob: $\underline{K} = \alpha^b \mod p$

$= (g^a \mod p)^b \mod p$

....

$= g^{ab} \mod p$

$=$ $(ba = ab)$

Elgamal

- Austausch verschlüsselter Nachrichten.
- Vergleiche den Algorithmus von Diffie-Hellman

2 Elgamal-Verfahren

1 p, so dass $p-1$ hat großen Primfaktor q

$$2\cdot q+1 = p \ ?$$

$\underline{g} \bmod p$, g Primitivwurzel

2 Alice | Bob

Alice	Bob
a ... Zufallszahl	b
$1 \le a \le p-2$	
$\alpha = g^a \bmod p$	$\beta = g^b \bmod p$

Bob verschlüsselt N $\qquad p, g, \alpha, b$

$$V = N \cdot \alpha^b \mod p$$

$\Rightarrow$ Alice entschlüsselt V:

$$E = V \cdot \beta^{p-1-a} \mod p$$

$$= (N \cdot \alpha^b) \cdot \beta^{p-1-a} \mod p$$

$$= (N \cdot (g^a)^b) \cdot (g^b)^{p-1-a} \mod p$$

$$= N \cdot \underbrace{g^{ab} \cdot g^{-ba}}_{1} \cdot g^{b \cdot (p-1)} \mod p$$

$$= N \cdot \Big(\underbrace{g^{p-1}}_{\equiv 1}\Big)^b \mod p$$

(Kleiner Fermat)

$$= N$$

Digitale Unterschrift

- Empfänger soll sicher nachprüfen können, dass eine Nachricht von einer bestimmten Person stammt.
- … z.B. nach Elgamal

p, g, α, β (vgl. Diffie-Hellman, Elgamal)

(a), (b)

---

(1) $1 < r < p-1$, $ggT(r, p-1) = 1$

(r und p-1 teilerfremd)

Alice

$k = g^r \mod p$

$s = (N - a \cdot k) \cdot r^{-1} \mod p-1$

r^{-1} ... „modulo Inverse zu r"

Die digitale Unterschrift zur Nachricht N ist (k, s).

Bob:

$$g^N \overset{?}{\equiv} \alpha^k \cdot k^s \mod p$$

$$= (g^a)^k \cdot (g^r)^s \mod p$$

$$\equiv g^{\underline{a\cdot k + r\cdot s}} \mod p$$

$$N \overset{?}{\equiv} a\cdot k + r\cdot s$$

$$\Rightarrow s\cdot r = N - a\cdot k \mod p-1$$

$$\underline{a\cdot k + s\cdot r} = N + x\cdot(p-1) \quad (\underline{\text{mod } p-1})$$

$$= g^{N + x\cdot(p-1)} \mod p$$

$$= g^N \cdot \underbrace{\left(g^{p-1}\right)^x}_{\equiv 1 \text{ (Kleiner Fermat)}} \mod p$$

$$= g^N \mod p$$

RSA

- „typisches“ Public-Key-Verfahren
- Ronald Rivest, Adi Shamir, Leonard Adleman (MIT)
-

Wähle p, q; $N = p \cdot q$

Berechne $\phi(N) = (p-1) \cdot (q-1)$

Wähle e: $1 < e < \phi(n)$, $ggT(e, \phi(N)) = 1$

(1) Suche d, sodass $e \cdot d \equiv 1 \mod \phi(N)$

(2) (N, e) Öffentl. Schl.

(N, d) priv. Schl.

p, q werden dann gelöscht

Alice

Klartext „m"

$V = m^e \mod N$

Bob

$V^d = \mod N$

$= (m^e)^d \mod N$

$= m^{e \cdot d} \mod N$

$= m$

z.z.: $m^{ed} \equiv m \mod N$ $\qquad N = pq$

Wir wählen $m < p, m < q$ $\qquad e.d \equiv 1 \mod \phi(N)$

$m^{p-1} \equiv 1 \mod p$ $\qquad m^{q-1} \equiv 1 \mod q$

$m^{k(p-1)(q-1)} \equiv 1^{k(q-1)} \mod p$

$m^1 \cdot m^{k.(p-1)(q-1)} \equiv m \cdot 1 \mod p$

$m^{1+k.(p-1)(q-1)} \equiv m \mod p$ $\qquad m^{1+k.(p-1)(q-1)} \equiv m \mod q$

(Chinesischer Restsatz)

$m^{1+k.\underbrace{(p-1)(q-1)}_{\phi(N)}} \equiv m \mod p.q$

$N = p.q$

$\phi(N) = (p-1)(q-1)$

$e \cdot d \equiv 1 \mod \phi(N)$

d.h. $e \cdot d = k \cdot \phi(N) + 1$

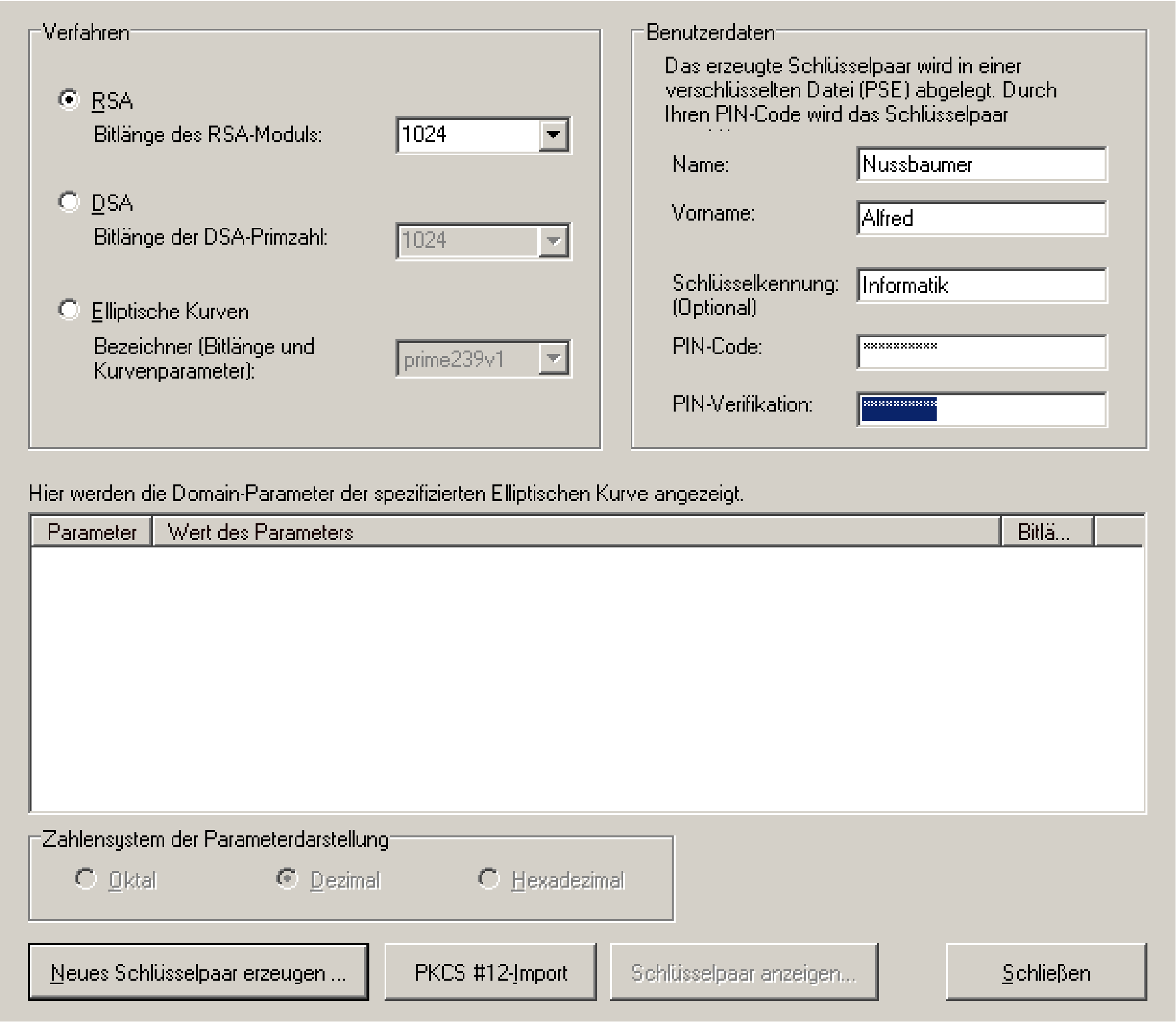
$m^{e.d} \equiv m \mod N$ $\square$

(das ist für Bob wichtig :-))

Wie kann ich die asymmetrischen Verfahren „programmieren“?

- Aufwändig (Primzahltest für große Primzahlen, Restklassenarithmetik, …)
- Lösung: Computer-Algebra-System (z.B. MuPad, Maxima)
- GeoGebra (für kleine Primzahlen)
- Cryptool 1.4

Cryptool 1.4

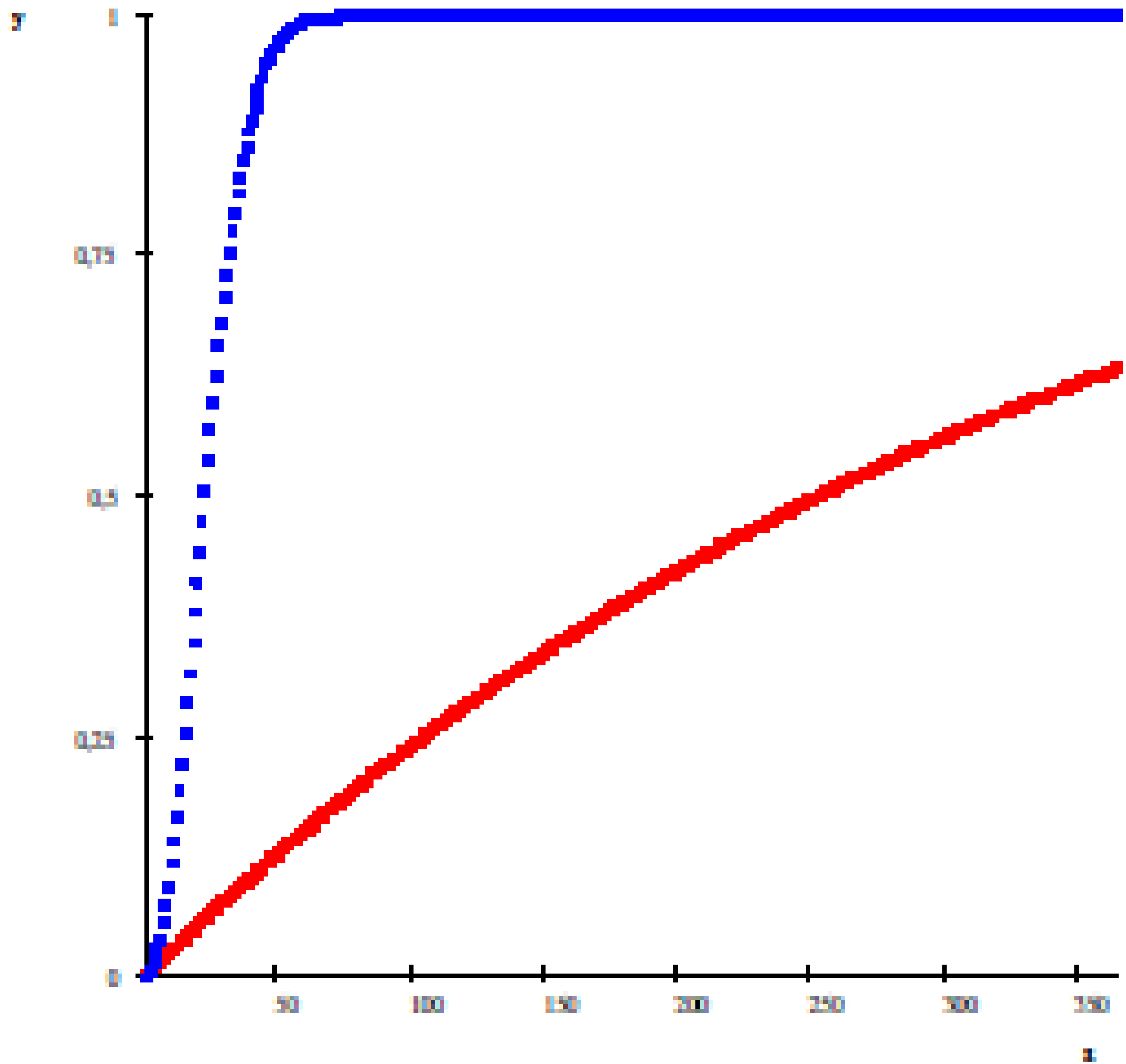

Verfahren
RSA
Bitlänge des RSA-Moduls:
1024
DSA
Bitlänge der DSA-Primzahl:
1024
Elliptische Kurven
Bezeichner (Bitlänge und Kurvenparameter):
prime239v1
Benutzerdaten
Das erzeugte Schlüsselpaar wird in einer verschlüsselten Datei (PSE) abgelegt. Durch Ihren PIN-Code wird das Schlüsselpaar
Name:
Nussbaumer
Vorname:
Alfred
Schlüsselkennung: (Optional)
Informatik
PIN-Code:
PIN-Verifikation:
Hier werden die Domain-Parameter der spezifizierten Elliptischen Kurve angezeigt.
Parameter
Wert des Parameters
Bitlä...
Zahlensystem der Parameterdarstellung
Oktal
Dezimal
Hexadezimal
Neues Schlüsselpaar erzeugen ...
PKCS #12-Import
Schlüsselpaar anzeigen...
Schließen

Hash-Verfahren

- Was kennzeichnet ein gutes Hash-Verfahren?
  - Rasch berechenbar
  - Hashwerte müssen eindeutig sein
  - Hashwerte müssen sich bei geringfügigen Abweichungen in den Daten dramatisch ändern
  - Kollisionsfrei
  - de facto unumkehrbar
- Was hat das „Geburtstagsproblem“ mit der Kryptographie zu tun???

Das Geburtstagsproblem

- **Aufgabe 1:** Wie groß ist die Wahrscheinlichkeit, dass zwei Personen ein einem ganz bestimmten Tag gemeinsam Geburtstag haben?
- **Aufgabe 2:** Wie groß ist die Wahrscheinlichkeit, dass zwei Personen an irgendeinem Tag gemeinsam Geburtstag haben?


1
0,75
0,5
0,25
0
50
100
150
200
250
300
350

Hashfunktionen?

- Ziffernsumme
- ISBN
- ISBN-13
- EAN
-

Hash-Verfahren

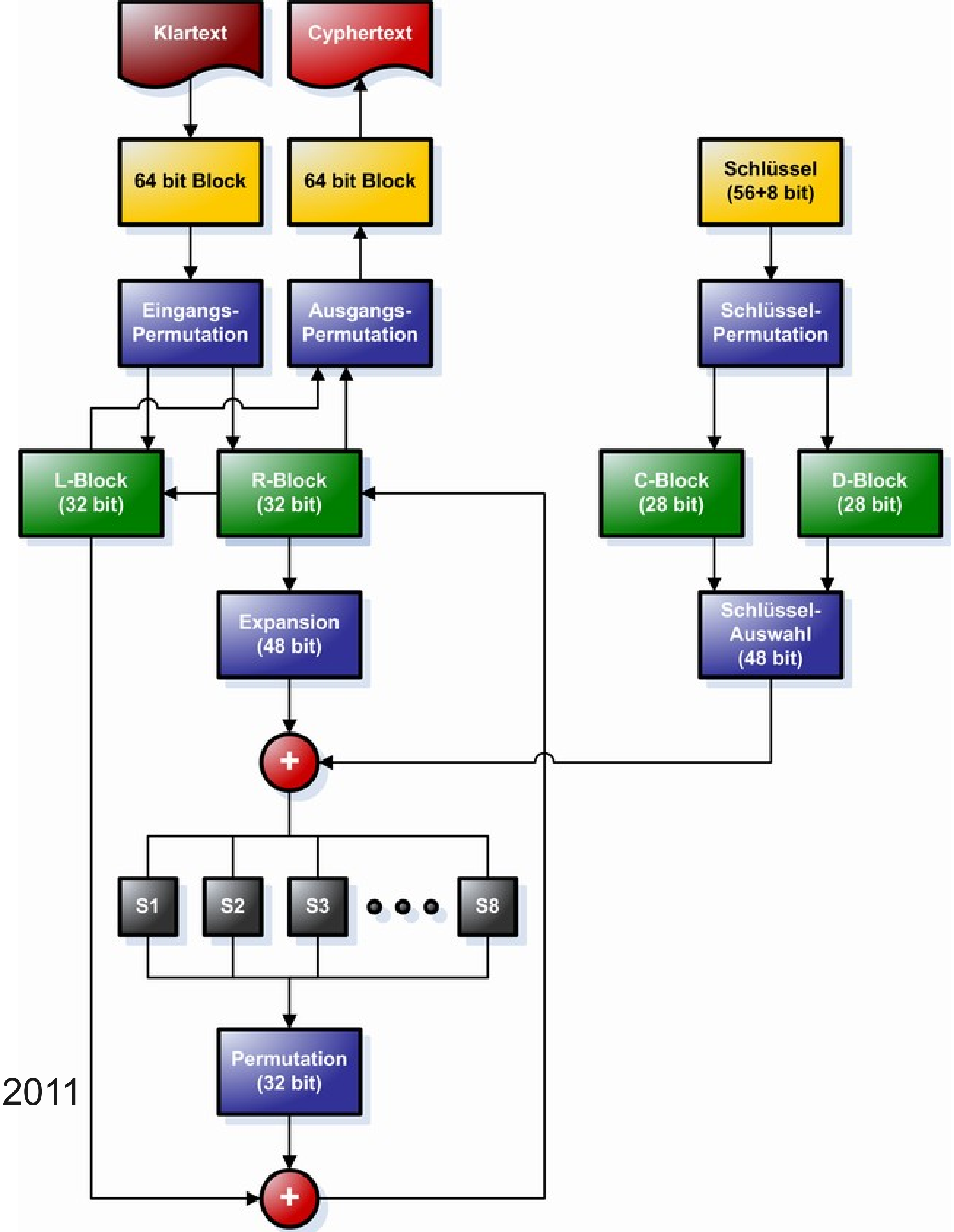
- MD5
- SHA-1
- RIPEMD-160

Unterricht:

- „MD5-Summen“ für verschiedene Daten bestimmen und vergleichen
- Bedeutung für Download?

DES

- Symmetrisches Verfahren
- Blockchiffre
- Feistel-Funktion
- ECB, CBC
- Verbesserung 3DES
- Heute durch AES abgelöst

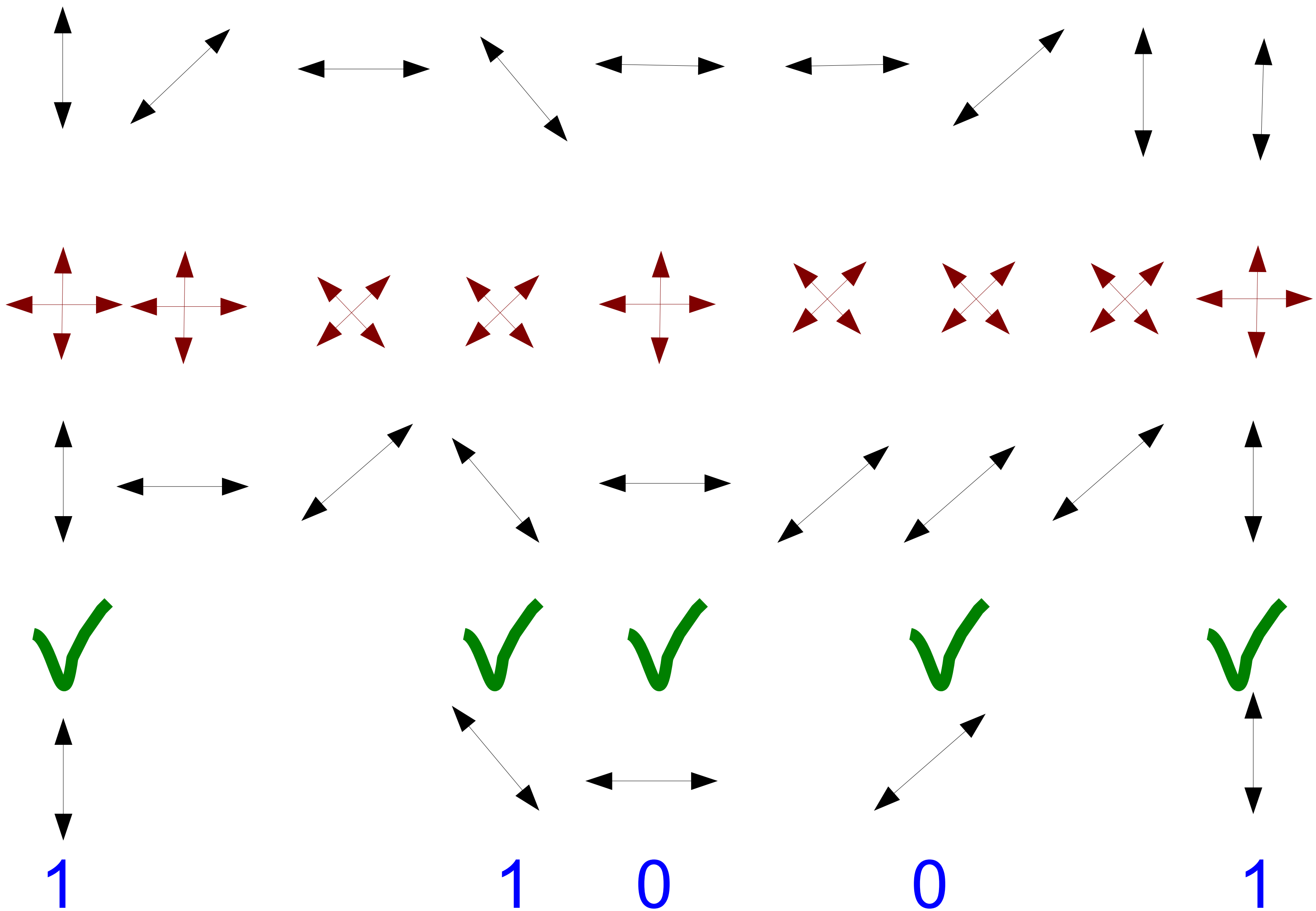


Grafik: WikiPedia, 26. April 2011

Cryptool 2 (Beta)

- Verfahren werden als „Bausteine“ mit Ein-/Ausgabeschnittstelle zur Verfügung gestellt.
- Bausteine können kombiniert werden (z.B. Triple-DES).
- Texteingabe und -ausgabe für Klartext und Geheimtext.
- Analyseverfahren.
- ...

Quantenkryptographie



Praktische Anwendung: TrueCrypt

- Frei verfügbar (http://www.truecrypt.org)
- Für Linux, Mac OS und Windows verfügbar
- Verschlüsselt beispielsweise USB-Sticks, Festplatten(bereiche), …
- Verschieden hohe Sicherheitsstufen wählbar
- Praktisch kein Zeitverlust durch Verschlüsselung / Entschlüsselung der Daten.
- Wichtig: Speichern von Reifeprüfungsaufgaben