Universität Ulm
Proseminar Informationsübertragung SS2006
(Betreut von Prof. Dr. Jacobo Toran)

Moderne Kryptographie

Claus Näveke
claus@naeveke.de

Inhalt

1. Mathematische Grundlagen

1.1 Primzahlen

In vielen Verfahren der modernen Kryptographie kommt Primzahlen eine besonders wichtige Bedeutung zu. Deshalb ist es wichtig sich zunächst nocheinmal deren Eigenschaften zu verdeutlichen.

Jede Primzahl besitzt genau zwei Teiler, nämlich 1 und sich selbst (0 und 1 sind also NICHT prim). Daraus ergeben sich folgende Schlußfolgerungen:

- Primzahlen lassen sich nicht als Produkt zweier natürlicher Zahlen, die beide größer als eins sind, darstellen.
- *Lemma von Euklid:* Ist ein Produkt zweier natürlicher Zahlen durch eine Primzahl teilbar, so ist bereits einer der Faktoren durch sie teilbar.
- *Eindeutigkeit der Primfaktorzerlegung:* Jede natürliche Zahl lässt sich als Produkt von Primzahlen schreiben. Diese Produktdarstellung ist bis auf die Reihenfolge der Faktoren eindeutig.

Multipliziert man als zwei Primzahlen p und q mit einander, so hat das Produkt n genau eine Faktorisierung, nämlich p*q.

n zu berechnen stellt dabei kein großes Problem dar, da es sich um eine einfache Multiplikation handelt, aus n wiederum auf p und q zu schließen ist dagegen sehr schwierig, denn es ist bis heute kein effizientes Faktorisierungsverfahren bekannt.

1.2 Modulo

Die Modulo-Funktion gibt den Rest einer Division zweier ganzer Zahlen an. Mathematisch definiert man Modulo über folgende Formel:

$$(a \bmod m) = a - \left\lfloor \frac{a}{m} \right\rfloor \cdot m$$

Eine Besonderheit der Modulo-Funktion im Zusammenhang mit Primzahlen stellt der kleine fermatsche Satz dar. Er besagt, dass für jedes ganzzahlige a sowie jede Primzahl p folgendes gilt:

$$a^p \equiv a \pmod{p},$$

oder anders geschrieben:

$$a^p \bmod p = a \bmod p$$

1.3 Eulersche φ-Funktion

Die eulersche Phi-Funktion gibt für jede natürliche Zahl n an, wieviele natürliche Zahlen zwischen 1 und n teilerfremd zu n sind.

Beispiel: Die Zahl 6 ist zu zwei Zahlen zwischen 1 und 6 teilerfremd (1 und 5), also ist φ(6) = 2

Da alle Primzahlen *p* nur durch 1 und sich selbst teilbar sind, sind sie sicher zu den Zahlen 1 bis *p*-1 teilerfremd, daher ist φ(p) = p-1

2. Methoden der Modernen Kryptographie

2.1 Symmetrische Verschlüsselung

Eines der ältesten Verfahren der Kryptographie stellt die symmetrische Verschlüsselung dar: Nachrichten werden mit einem (geheimen) Schlüssel verschlüsselt und können nur mit diesem Schlüssel auch wieder entschlüsselt werden.

Die Algorithmen werden dabei in zwei Kategorien unterteilt:

2.1.1 Blockchiffren

Bei einer Blockchiffre werden die Nachrichten in einzelne Blöcke fester Länge (beispielsweise 64 Bit) geteilt und anschließend jeder Block einzeln unter Verwendung des Schlüssels verschlüsselt.

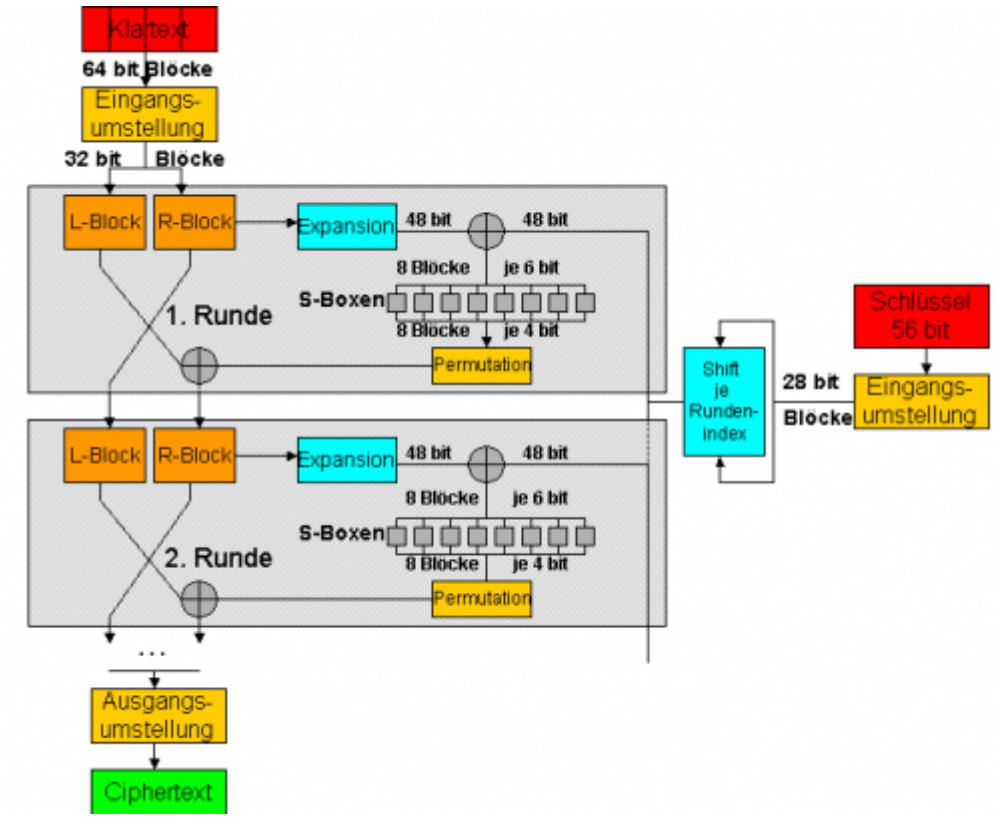
Die bekanntesten Beispiele für Blockchiffren sind der DES (Data Encryption Standard), sowie der IDEA (International Data Encryption Algorithm). Beide arbeiten mit einer Blocklänge von 64Bit, sowie einer Schlüssellänge von 56Bit (DES) bzw. 128Bit (IDEA).

Da der DES im kommerziellen Bereich der am häufigsten Eingesetzte Algorithmus ist(/war), wird dessen Funktionsweise exemplarisch für alle Blockchiffren behandelt:

Wie bereits erwähnt, wird die zu verschlüsselnde Nachricht zu nächst in 64Bit Blöcke zerlegt, welche dann bei der (schlüsselunabhängigen) Eingangspermutation wiederum in zwei 32Bit-Blöcke (L- und R-Block) zerlegt werden. Nun beginnen 16 Durchläufe: Der R-Block der ersten Runde wird zum L-Block der zweiten Runde. Der L-Block der ersten Runde wird mit einer Funktion, dem sog. Rundenschlüssel, addiert, die den R-Block der ersten Runde und den Schlüssel verwendet. Das Ergebnis ist der R-Block der zweiten Runde. Im 16. Durchlauf erfolgt dann statt der Vertauschung von L- und R-Block eine Ausgangspermutation, welche zur Eingangspermutation invers ist.

Der 56Bit Schlüssel wird nach einer festen Regel umgestellt und in zwei 28Bit Blöcke geteilt. Diese Blöcke werden je nach Durchlauf um ein oder zwei Stellen nach links geshiftet. Aus diesen Blöcken wird dann der 48Bit Teilschlüssel für die

jeweilige Runde ermittelt. Die 32Bit des R-Blocks werden durch Duplizierung bestimmter Bitstellen auf 48Bit erweitert. Diese beiden 48Bit Blöcke werden modulo 2 addiert und aus dem Ergebnis durch Substitutionen der aktuelle Rundenschlüssel berechnet.



Zur Entschlüsselung muß lediglich der Algorithmus in umgekehrter Reihenfolge durchlaufen werden. Da der DES bereits Mitte der 90er durch sog. Brute-Force-Attacken (einfaches Durchprobieren aller möglichen Schlüssel) geknackt werden konnte wurde als Ersatz der Triple-DES oder 3DES eingeführt. Hierbei wird ein 168Bit Schlüssel verwendet, welcher in drei 56Bit Schlüssel zerlegt wird. Anschließend führt man dreimal eine einfache DES Verschlüsselung mit diesen Teilschlüsseln durch.

2.1.2 Stromchiffren

Bei einer Stromchiffre werden Nachrichten nicht blockweise, sondern Zeichenweise verschlüsselt, wobei sich in der Regel der verwendete Schlüsselstrom von Zeichen zu Zeichen ändert. Ich Gegensatz zu den Blockchiffren werden gleiche Klartext-Blöcke also nicht zwangsläufig in gleiche Geheimtextblöcke verschlüsselt.

Die einfachste und effektivste aller Stromchiffren stellt das One-Time-Pad dar: Dazu ist es nötig, dass die Nachricht in Form von Binärdaten vorliegt. Zusätzlich benötigt man als Schlüssel eine zufällig erzeugte Binärfolge, die mindestens so lang ist, wie der Ursprungsnachricht. Verknüpft man beide Binärströme durch ein bitweises XOR, so erhält man einen Geheimtext, der ohne Schlüssel keinerlei Rückschlüsse auf den Klartext zuläßt. Man spricht deshalb von einem perfekten Verschlüsselungsverfahren.

Der Einsatz in der Praxis ist häufig problematisch, da wirklich zufällige Zufallszahlen schwierig zu erzeugen sind. Außerdem benötigt der Schlüsseltransfer einen sicheren Kanal, welcher wiederum die Verschlüsselung unnötig werden ließe. Ein weiteres Problem stellt die Länge des Schlüssels dar, denn es wird für jede

Nachricht ein neuer Schlüssel mit gleicher Länge wie die Nachricht selbst benötigt. Eine mögliche Lösung dieser Probleme wird in Abschnitt 2.6 dargestellt.

2.2 Asymmetrische Verschlüsselung

Symmetrische Verschlüsselungen haben den großen Nachteil, dass der Schlüsseltausch geheim erfolgen muß. Gelingt es einem dritten Zugriff auf den Schlüssel zu bekommen, so kann er alle Nachrichten entschlüsseln und beliebige Nachrichten selbst verschlüsseln. Mit dem Tausch der Schlüssel steht und fällt also die komplette Verschlüsselung. Der Mangel an sicheren Übertragungskanälen ist es aber gerade, der in vielen Fällen den Einsatz von Verschlüsselung nötig macht. Abhilfe schaffen hier seit Anfang der 1970er asymmetrische Verschlüsselungsverfahren. Diese funktionieren ähnlich einem Briefkasten: Jeder kann einen Brief einwerfen(/eine Nachricht verschlüsseln), aber nur der Besitzer eines (geheimen) Schlüssels kann die Nachrichten entnehmen(/entschlüsseln).

Eines der bekanntesten und meist verwendeten Verfahren stellt hierbei der RSA-Algorithmus dar, welchen die Mathematiker Ronald L. **R**ivest, Adi **S**hamir und Leonard **A**dleman „entdeckten“, als sich versuchten zu beweisen, dass sichere asymmetrische Verschlüsselung unmöglich ist.

Bei diesem Verfahren werden zwei Schlüssel generiert: Ein Öffentlicher und ein Privater. Der öffentliche Schlüssel kann (und muss) bedenkenlos veröffentlicht werden. Mit seiner Hilfe werden die Nachrichten des Senders verschlüsselt. Einmal chiffriert hat der Sender keine Möglichkeit mehr daraus den Originaltext zu erhalten. Nur der Empfänger der im Besitz des privaten Schlüssels ist kann damit die Nachricht wieder entschlüsseln.

Im Einzelnen funktioniert das so:

Zunächst gilt es passende Schlüssel zu generieren. Dazu werden zwei zufällige Primzahlen p und q mit $p \neq q$ generiert (raten einer Zahl und anschließender Primzahltest) und daraus der Produkt $N=p*q$ berechnet. Anschließend berechnet man $\varphi(N)=(p-1)*(q-1)$. Nun wählt man eine Zahl e, für die gilt $1<e<\varphi(N)$ und die teilerfremd zu $\varphi(N)$ ist. Schließlich berechnet man noch eine Zahl d so, dass das Produkt e*d kongruent bezüglich des Modulus $\varphi(N)$ ist ($e*d \equiv 1 \pmod{\varphi(N)}$).

Der öffentliche Schlüssel besteht dann aus dem Primzahlprodukt N, sowie dem öffentlichen Exponenten e. Der geheime Schlüssel besteht ebenfalls aus N und dem geheimen Exponenten d.

Will man nun eine Klartext-Nachricht K verschlüsseln, so verwendet man die Formel $C \equiv K^e \bmod N$ und erhält daraus den Geheimtext C. Die Entschlüsselung funktioniert genauso, nur wird hier Anstelle von e d verwendet: $K \equiv C^d \bmod N$

Zahlenbeispiel:

- Wir wählen p=11 und q=13, woraus sich N=143 ergibt
- Für $\varphi(143)=(11-1)*(13-1)$ ergibt sich dann ein Wert von 120
- Für e wählt man beispielsweise 23
- d nimmt dann den Wert 47 an.

Es ergibt sich also ein öffentlicher Schlüssel aus e=23 und N=143, sowie der private Schlüssel durch d=47

Wollen wir nun beispielsweise die Zahl 7 verschlüsseln, so berechnen wir $C \equiv 7^{23} \bmod 143$. Die verschlüsselte Nachricht heißt also 2. Zur Entschlüsselung berechnet man $K \equiv 2^{47} \bmod$

143, was wiederum die von uns verschlüsselte 7 ergibt.

Asymmetrische Verschlüsselungsverfahren sind im Vergleich zu symmetrischen Verfahren sehr langsam (Faktor 1000 und mehr). Deshalb werden in der Praxis häufig Mischungen daraus eingesetzt. So kann man beispielsweise das RSA-Verfahren zur sicheren Übermittlung eines DES Schlüssels verwenden und die eigentliche Chiffrierung der Daten dann mit dem DES Verfahren durchführen.

2.3 Elektronische Signatur

Mit Hilfe von elektronischen Signaturen, auch digitale Unterschrift genannt, wird versucht sämtliche Eigenschaften einer „normalen“ Unterschrift auf ihr elektronisches Gegenstück zu übertragen. Die wichtigsten Eigenschaften sind

- **Echtheitseigenschaft:**

  Es wird sichergestellt, dass das Dokument vom Unterzeichner stammt. Dazu ist ein enger Zusammenhang zwischen Dokument und Signatur nötig; beispielsweise dadurch, dass Unterschrift und Erklärung auf dem selben Blatt stehen.

- **Identitätseigenschaft:**

  Eine Signatur ist persönlich, kann also nur von einem einzigen Menschen ausgestellt werden.

- **Abschlusseigenschaft:**

  Die Unterschrift vollendet eine Erklärung, deshalb steht sie am Ende der selbigen.

- **Warneigenschaft:**

  Sie soll den Unterzeichnenden vor übereilten Entscheidungen bewahren.

- **Verifikationseigenschaft:**

  Die Echtheit einer Signatur kann verifiziert werden, etwa durch einen Vergleich.

Bis auf die Warneigenschaft lassen ich diese Eigenschaften ohne größere Probleme auf elektronische Signaturen übertragen. Im Prinzip läßt sich solch eine Unterschrift als Gegenstück zur asymmetrischen Verschlüsselung sehen: Es soll nur einer einzigen Person möglich sein die Signatur zu erzeugen, aber alle anderen sollen in der Lage sein sie zu verifizieren. Außerdem soll eine nachträgliche Manipulation erkannt werden können. Deshalb verwendet man in der Praxis meistens asymmetrische Verschlüsselungsverfahren in der Umgekehrten Richtung: Der Unterschreibende wendet seinen geheimen Schlüssel auf das zu signierende Dokument an und „verschlüsselt“ es damit. Der Empfänger kann den Verschlüsselten Text mit Hilfe des öffentlichen Schlüssels entschlüsseln und mit dem unverschlüsselten Text vergleichen. Solange die Sicherheit des privaten Schlüssels gewährleistet ist, ist also auch die Sicherheit der Signatur sichergestellt.

Da asymmetrische Verfahren zu zeitintensiv für ganze Dokumente sind und die Signatur dadurch zusätzlich nocheinmal die Länge des Ursprungsdokumentes hätte wird in der Praxis meist nur der Hashwert des Dokuments signiert. Der Empfänger bildet dann ebenfalls den Hashwert und vergleicht ihn mit dem entschlüsselten aus der Signatur, um Manipulation auszuschließen.

2.4 Kryptographische Hashfunktionen

Hashfunktionen dienen dazu größere Datenmengen zu einen digitalen „Fingerabdruck“ fester Länge zu komprimieren. Dabei ist es wichtig, dass das Verfahren möglichst kollisionsfrei arbeitet, die Wahrscheinlichkeit, dass unterschiedliche Daten den selben Hash bekommen also möglichst gering ist. Außerdem darf es nicht ohne weiteres möglich sein absichtlich zweimal den gleichen Hash mit unterschiedlichen Daten zu erzeugen. Einfache Prüfsummen (Quersumme) sind deshalb als Hashfunktion ungeeignet. Bekannte Hashfunktionen sind beispielsweise MD5 oder SHA.

2.5 Einwegfunktionen

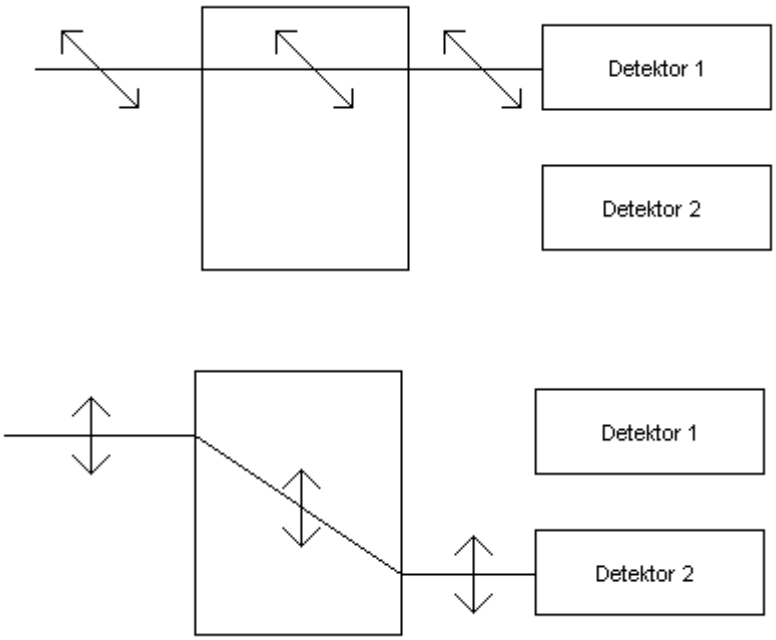
Einwegfunktionen verschlüsseln, wie der der Name bereits sagt nur in eine Richtung. Mit ihrer Hilfe ist es einfach einen Klartext in einen Chiffretext zu überführen. Der Umgekehrte Weg ist aber nahezu unmöglich. Realisieren läßt sich das z.B. durch ein symmetrisches Verschlüsselungsverfahren, dem eine feste Nachricht und der zu verschlüsselnde Text als Schlüssel übergeben wird. Ohne Kenntnis des Ursprungstextes kennt man also den Schlüssel nicht und kann somit keine Entschlüsselung durchführen.

Einsatz finden diese Verfahren häufig bei der Speicherung von Passwörtern. Zur Überprüfung wird dann einfach die Eingabe verschlüsselt und mit dem gespeicherten verschlüsselten Wert verglichen. Stimmen diese über, so stimmen auch die Passwörter überein. Gelingt es einem Eindringling Zugriff auf die Passwortdatenbank zu bekommen, so hat er dadurch dennoch keinen Zugriff auf die Klartextpasswörter.

2.6 Quantenkryptographie

Bei der Quantenkryptographie handelt es sich um ein, von Charles H. Bennett und Gilles Brassard im Jahr 1984 entwickeltes Verfahren zur abhörsicheren Informationsübertragung. Dabei wird das fundamentale Prinzip der Quantentheorie ausgenutzt: Die Heisenbergsche Unschärferelation, welche besagt, dass jede Messung in einem quantenmechanischen System eine Störung desselben hervorruft.

Die Quantenkryptographie nutzt Lichtquanten (Photonen) zur Übertragung der Informationen. Dabei wird ausgenutzt, daß jedes Lichtquant senkrecht zu seiner Ausbreitungsrichtung in eine bestimmte Richtung schwingt (Polarisation). Mittels Polarisationsfiltern kann man diese Polarisation für wohldefinierte Richtungen erzeugen bzw. bestimmen. Bei Filtern aus doppelbrechendem Kristall kann zwischen horizontal und vertikal polarisierten Photonen unterschieden werden:

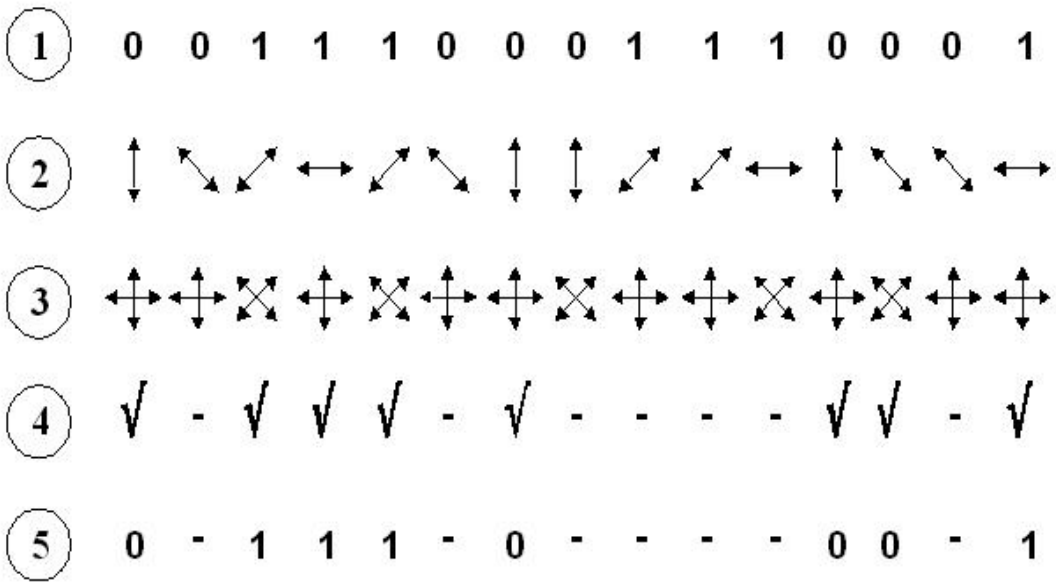


Polarisationsfilter

Horizontal polarisiertes Licht wird in Detektor 1, vertikal polarisiertes in Detektor 2 gelenkt.

Schräg polarisiertes Licht (45 Grad oder 135 Grad) wird zufällig als horizontal oder vertikal erkannt. Um dieses schräg polarisierte Licht exakt messen zu können, muß der Filter um 45 Grad gedreht werden.

Dies macht man sich der Quantenkryptographie nun zu Nutze: Zunächst definiert man je eine „gerade“ und eine „schräge“ Richtung als 0, die übrigen als 1. Der Sender sendet eine Reihe von Photonen mit zufälliger Polarisation (1, 2) und merkt sich die Nummer, das benutzte Schema und die gemessene Polarisationsrichtung. Der Empfänger seinerseits misst mit zufälligen Schemata (3) und merkt sich die gleichen Kriterien. Anschließend sendet der Empfänger seine verwendeten Einstellungen über einen öffentlichen Kanal an den Sender, welcher wiederum eine Liste mit Nummern zurücksendet, bei welchen die Einstellungen richtig waren (4). Streichen beide nun falsch gemessenen Werte (5), so erhalten beide eine gemeinsame zufällig erzeugte Bitfolge, welche als Schlüssel für ein One-Time-Pad verwendet werden kann.



Anschließend überprüfen beide noch einige zufällig ausgewählte Bits der Bitfolge. Bei einer Fehlerrate von mehr als 14% kann davon ausgegangen werden, dass die Übertragung gestört/abgehört wurde, ansonsten kann der Schlüssel bedenkenlos verwendetet werden.

Der Vollständigkeit halber sei noch das Verfahren der verschränkte Photonen erwähnt, auf welches hier jedoch nicht weiter eingegangen werden soll.

3. Quellen

- http://www.wikipedia.org
- A. Beutelspacher, J. Schwenk, K.-D. Wolfenstetter, Moderne Verfahren der Kryptographie
-
- http://www-ivs.cs.uni-magdeburg.de/bs/lehre/wise0102/progb/vortraege/stepan/index.htm
- http://www.regenechsen.de/phpwcms/index.php?krypto_des