Kryptografie & Kryptoanalyse

Eine Einführung in die klassische Kryptologie

Caesar-Verfahren

- *Wie viele Schlüssel-Möglichkeiten gibt es beim Caesar-Verfahren?*
- 26 (Anzahl Buchstaben des Alphabetes → Anzahl Verschiebungen)

Substitutionsverfahren (1)

- *Was müssen sie als Schlüssel eingeben damit keine Verschlüsselung stattfindet?*
- A oder AB oder ABC … (einfach so dass das Alphabet nicht durcheinander kommt)
  - `abcdefghijklmnopqrstuvwxyz`
  - `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

Substitutionsverfahren (2)

- *Wieso sollte der Text mindestens 200 Zeichen umfassen?*
- Bei einem zu kurzen Text kann es sehr gut sein dass die Analyse nicht mit der Statistik übereinstimmt, d. h. dass der häufigste Buchstaben nicht unbedingt ein ‚e‘ ist

Vigenère-Verfahren (1)

- *Wieso wird beim Programm „Vigenère“ in der Mitte das Alphabet nicht angezeigt?*
- Vigenère ist ein polyalphabetisches Verfahren, d. h. pro Klartextbuchstaben gibt es mehrere mögliche Geheimtextbuchstaben und umgekehrt

Vigenère-Verfahren (2)

- *Wie sieht die Häufigkeitsverteilung aus?*
- Bei einem genügend langen Text gibt es keinen einzelnen „Maximalausschlag“, da aus dem häufigen ‚e‘ mehrere verschiedene Buchstaben werden können (polyalphabetisches Verfahren)

Vigenère-Verfahren (3)

- *Wieso klappt die Häufigkeitsanalyse hier nicht?*
- Dies folgt aus der letzten Frage: Ohne klare Häufigkeitsverteilung kann man auch keine Häufigkeitsanalyse machen. Die Häufigkeitsanalyse ist bei polyalphabetischen Verfahren machtlos

Vigenère-Verfahren (4)

- Wieso ist das Knacken der Nachricht auch bei einer polyalphabetischen Verschlüsselung noch möglich?
- Der Schlüssel hat eine bestimmte Länge, z. B. 3 wie hier im Beispiel:
  - `diesistderklartext`
  - `+ keykeykeykeykeykey`
  - `--------------------`
  - `NMCCMQDHCBOJKVROBR`

Knacken von Vigenère (1)

- Das hat zur Folge das jeder 3. Buchstabe um die gleiche Anzahl Buchstaben verschoben wird (der 1., der 4., etc., alle werden um k = 11 Stellen verschoben)
- Wenn nun wie im Beispiel an 2. und 5. Stelle der gleiche Buchstabe steht (‚i‘) so wird aus diesem auch der gleiche Geheimtextbuchstabe (‚M‘)

```
    diesistderklartext
+   keykeykeykeykeykey
    ------------------
    NMCCMQDHCBOJKVROBR
```

Knacken von Vigenère (2)

- Durch solche auftretende Muster lässt sich per Computer relativ einfach die Schlüssellänge l bestimmen, indem man gleiche Buchstabenfolgen im Geheimtext sucht und deren Abstand bestimmt
- Hat man erst einmal die Schlüssellänge l nimmt man zur Bestimmung des 1. Buchstabens des Schlüssels den 1., den 1+l., den 1+2l. etc. Buchstaben und macht auf diesen eine einfache Häufigkeitsanalyse

Knacken von Vigenère (3)

- **N***MC***C***MQ***D***HC***B***OJ***K***VR***O***BR**
  → verschoben mit ‚k' →
  d*ie***s***ist***d***e***r***kl***a***rt***e***xt***
- Dies funktioniert da ja alle diese Buchstaben um die gleiche Anzahl Stellen verschoben wurden (wie beim Caesar-Verfahren)
- Man muss nur denn häufigsten Buchstaben finden, und schon ist die Verschiebung bekannt (durch Vergleich mit ‚e')

Ist denn nichts sicher?

- Das Knacken von Vigenère gelingt, da es wegen der fixen Schlüssellänge zu Wiederholungen kommt.
- Nimmt man einen Schlüssel der gleich lang ist wie der zu verschlüsselnde Text gibt es keine Wiederholungen
- Dieses Verfahren heisst „One-Time-Pad“

One-Time-Pad

- Das One-Time-Pad ist ein 100% sicheres Verfahren, denn jeder Schlüsselbuchstabe wird nur ein mal (one-time) verwendet
- Es hat nur einen - leider relativ grossen - Nachteil: Im vornherein muss ein riesengrosser geheimer Schlüssel vereinbart werden
- Dieses Verfahren wurde während des Kalten Krieges zwischen Moskau und Washington eingesetzt („heisser Draht“)

Der Schlüsselaustausch

- Dafür mussten regelmässig Diplomaten mit Koffern voller Zufallszahlen hin- und herreisen
- Denn auch beim One-Time-Pad gilt:
  - Der Schlüssel muss über einen sicheren separaten Kanal übermittelt werden
  - Ist der Schlüssel dem Gegner bekannt ist die Sicherheit dahin

Moderne Verfahren

- Das heute im kommerziellen Gebrauch am häufigsten eingesetzte Verfahren heisst DES
- DES steht für „Data Encryption Standard“
- Es funktioniert im Prinzip wie ein mehrfach hintereinander angewandtes Substitutionsverfahren

Sicherheit von DES

- Der DES erlaubt mit 56 Bits Schlüssellänge 2^{56} = 72’057’594’037’927’936 = 72 Billiarden mögliche Schlüssel
- Dennoch ist dies heute nicht mehr ausreichend: DES kann in 5 Tagen mittels der Brute-Force-Methode geknackt werden

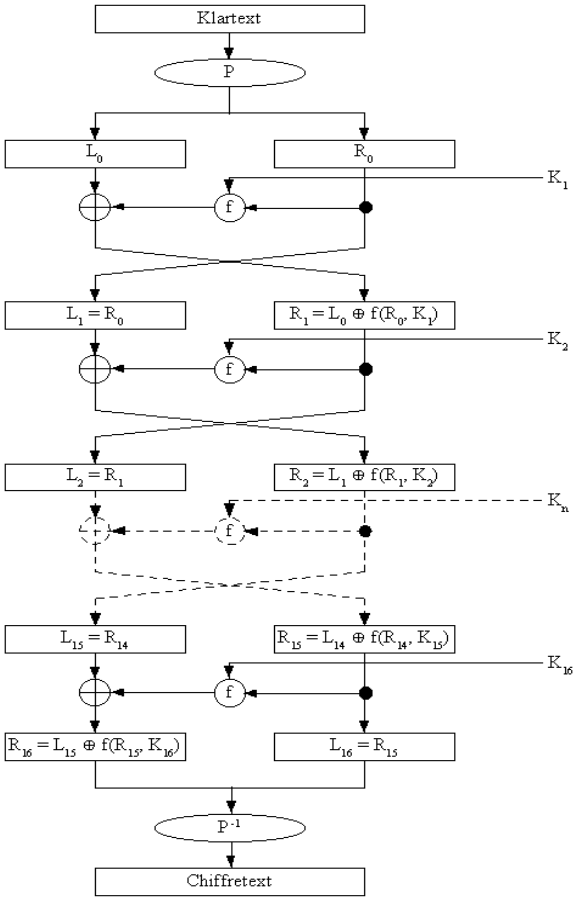

Abbildung: Struktur von DES
(Quelle: http://www.linux-magazin.de/Artikel/ausgabe/1997/09/Krypto/krypto3.html)

Genügen dann 128 Bits?

- Der IDEA (= „International Data Encryption Algorithm“) arbeitet mit 128 Bits Schlüssellänge, sonst ähnlich wie der DES
- $2^{128} = 3.43669 * 10^{38}$ Dies zu knacken benötigt etwa 10^{12} Jahre
- Deshalb gilt der IDEA heute als sicher

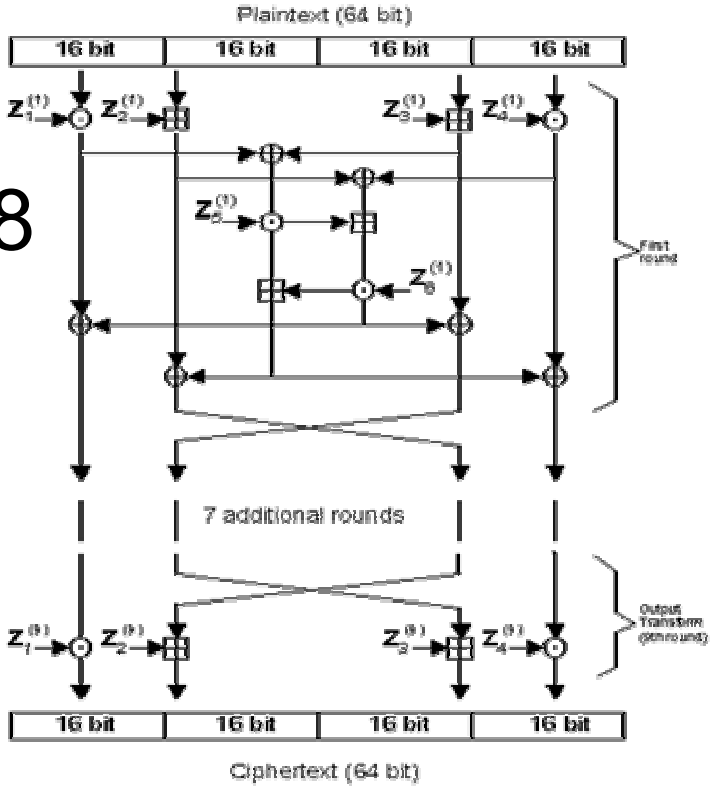

Abbildung: Struktur von IDEA
(Quelle: http://www.media-crypt.com/engl/Content/technical_description.htm)

Vergleich Klassisch - Modern

- Sowohl die klassischen Verfahren wie Vigenère als auch die modernen Verfahren wie IDEA…
  - …benötigen einen Schlüssel der beiden Parteien im Vornherein bekannt ist
  - …sind symmetrisch (Entschlüsselung ist Umkehrung der Verschlüsselung)
  - …sind in gewissen Masse anfällig auf Kryptoanalyse (z.B. Brute-Force)

Der Schlüsselaustausch

- Sicherheitsrelevant für alle bisher kennen gelernten Verfahren ist der Schlüsselaustausch, der zuvor über einen geheimen Kanal stattfinden muss
- Nicht immer hat man aber die Möglichkeit sich z. B. persönlich zu treffen
- Es gibt jedoch ein Möglichkeiten, auch über einen unsicheren Kanal den Schlüsselaustausch durchzuführen
- Diese Verfahren tragen den Namen „Public-Key“

Fazit:

- Die Geschichte der Kryptografie ist ein Wettbewerb zwischen Verschlüsselungsspezialisten und Kryptoanalysten
- Momentan liegen die Verschlüssler mit dem IDEA vorne, da dieses Verfahren nur mit Brute-Force geknackt werden kann, und dies wegen der grossen Schlüssellänge auch auf modernsten Computern noch zu lange geht