**Kryptographie**

Einführung:

Ziele der Kryptographie:

* Verschlüsselung
* Entschlüsselung
* Authentifikation
* Anonymität

Symmetrische Verfahren: Ein und derselbe Schlüssel wird für Ent- und Verschlüsselung benutzt

m = message

k = key

c = Geheimtext

c = f(k,m)

m = f\*(k, c)

Caesar Code

* Symmetrisches Verfahren, welches Buchstabe nach Buchstabe codiert
* f(k, m) = m + k mod 26
* f\*(k, c) = c – k mod 26

Vigenere Code

* Weiterentwicklung des Caesarcode
* Schlüssel ist ein Wort
* Schlüssel wird so auf aufgefüllt wie möglich
* Rest ist gleich wie bei Caesar

Ein Verfahren gilt nur als sicher, wenn Eve das Verfahren bekannt ist, nur der Schlüssel nicht, und sie denoch praktisch ist.

Ciphertext only attack: Eve kennt nur einen oder mehrere Geimtexte

Known plaintext attack: Eve kennt ein oder mehrere Klartext-Geheimtext-Paare

Chosen plaintext attack: Eve kann f nutzen (kennt aber nicht den Schlüssel k bzw e)

Chosen ciphertext attack: Eve kann f\* nutzen (kennt aber nicht den Schlüssel k bzw d)

Ein Verfahren gilt als effizient und sicher, falls für alle m das f(e, m) einfach zu berechnen ist f\*(d,c) ebenso, falls man das d kennt und f\*(d, c) soll für alle c schwer zu berechnen sein, falls an das d nicht kennt

Leicht: in polynomieller Zeit berechenbar (in realistischer Zeit)

Schwer: in randomisiert polynomieller Zeit berechenbar (nicht realistischer Zeit)

Ein symmetrisches Verfahren sicherer machen:

* Schlüssel k so lang wie die Nachricht m
* Schlüssel k nur einmal benutzen
* Schlüssel k zufällig ist, sowie natürlich
* Schlüssel k geheim ist

Mathematische Grundlagen

Erweiterter Euklidischer Algorithmus:

Berechnet zu k, m Element N den ggT(k, m) sowie Zahlen c, d Element Z mit ck + dm = ggT(k, m)

Ein Bild, das Text, Anzeigetafel enthält.

Automatisch generierte Beschreibung

Chinesischer Restsatz: