Handout zur Kryptologie

Jürgen Hermes - Institut für Digital Humanities – Universität zu Köln

Anwendungsbereiche für Kryptologie

Geheimhaltung – Kommunikationssicherheit (confidentiality), Computersicherheit (privacy)

Authentisierung – Sicherung gegen Fälschung und Unterschiebung

Archäo-Linguistik – Entzifferung vergessener Sprachen und Schriftsysteme

Glossar

Kryptologie: Technische Verfahren für die Informationssicherheit

Steganographie: Verschleiern der Existenz von Informationen

Kryptographie: Verschlüsselung von Informationen

Kryptoanalyse: Informationsgewinnung aus verschlüsselten Texten

Klartext (plain text): Unverschlüsselte Nachricht

Geheimtext (cipher text): Verschlüsselte Nachricht

Verschlüsselungsmethode: Algorithmus, der Verschlüsselung zugrunde liegt

Schlüssel: Information über die Anwendung der Verschlüsselungsmethode

Transposition: Umstellung von Klartexteinheiten

Substitution: Ersetzung von Klartexteinheiten

Code: Ersetzung linguistischer Entitäten (Morpheme, Silben, Wörter, Phrasen, Sätze)

Chiffre: Ersetzung von Einzelbuchstaben oder n-Grammen.

Chiffrenalphabet: Ersetzungseinheiten bezeichnet als Menge W

Klartextalphabet: Zu ersetzende Einheiten, bezeichnet als Menge V

Nullen: Ersetzungseinheiten, die keiner Klartexteinheit entsprechen

Homophone: Verschiedene Chiffren für einen Klartextbuchstaben

Polyphone: Chiffren für mehrere Klartextbuchstaben

Prinzipien

Injektivität: Linkseindeutigkeit, jede Chiffre ist eindeutig auf einen Klartextbuchstaben zurückzuführen, d.h. keine Polyphone erlaubt.

Shannon'sches System: Links- und rechtseindeutig, jede Klartexteinheit wird immer auf dieselbe Geheimtexteinheit abgebildet, d.h. weder Polyphone noch Homophone erlaubt.

Kerkhoff'sches Prinzip: Sicherheit durch Geheimhaltung des Schlüssels, keine Geheimhaltung des Verschlüsselungsverfahrens.

Security by Obskurity: Sicherheit durch Geheimhaltung des Verschlüsselungsverfahrens, evtl. zusätzliche Geheimhaltung des Schlüssels.

Terminologie der Substitutionsverfahren

Klartextzerlegung:

- Klartext wird in Einzelzeichen zerlegt: **monographisch** (auch: einfach)
- Klartext wird in Einheiten mehrerer Zeichen: **polygraphisch** (bi-, tri, tetragraphisch etc.)

Geheimtexterzeugung:

- Geheimtext wird aus Einzelzeichen erzeugt: **monopartit**
- Geheimtext wird aus Zeichen-Paaren erzeugt: **bipartit**
- Geheimtext wird aus Zeichen-Tripeln erzeugt: **tripartit**
- Geheimtext wird aus Zeichen-Oktetten erzeugt: **oktopartit**, z. B. Bytes

Anzahl der Geheimtextalphabete:

- Zur Verschlüsselung wird ein einziges Alphabet verwendet: **monoalphabetisch**.
- Zur Verschlüsselung werden verschiedene Alphabete verwendet: **polyalphabetisch**.

Umfang der Geheimtextalphabe:

- Das Alphabet besteht aus zwei Zeichen: **binäre** Chiffrierung, z. B. Binärcode
- Das Alphabet besteht aus drei Zeichen: **ternäre** Chiffrierung
- Das Alphabet besteht aus vier Zeichen: **quaternäre** Chiffrierung, usw.
- Das Alphabet besteht aus zehn Zeichen: **denäre** Chiffrierung, z. B. den zehn Ziffern
- Das Alphabet besteht aus 26 Zeichen, wie beim gewohnten lateinischen Alphabet
- Das Alphabet besteht aus 128 Zeichen (7 bit), beispielsweise beim ASCII-Code
- Das Alphabet besteht aus 256 Zeichen (8 bit), beispielsweise beim erweiterten ASCII-Code
- Das Alphabet besteht aus 18.446.744.073.709.551.616 Zeichen (64 bit), beispielsweise beim DES-Verfahren im ECB-Mode

Literatur (Auswahl)

Bauer, F. L. ([4]2007): *Decrypted Secrets. Methods and Maxims of Cryptology*. Berlin: Springer.

Kahn, D. ([7]1997): *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. London: Schuster & Schuster.

de Leeuw, K. & Bergsta, J. (2007): *The History of Information Security. A comprehensive Handbook*. Amsterdam: Elsevier.