

NICHTKRYPTOGRAPHISCHE VERFAHREN

Steganographie

Gliederung

- ① Definition
- ② Unterschied zur Kryptographie
- ③ Arten der Steganographie/Beispiele
- ④ Sicherheit
- ⑤ Demonstration
- ⑥ Quellen

Definition

- ⦿ Aus dem Griechischen:
 - „steganós“ = bedeckt
 - „gráphein“ = schreiben
- ⦿ verborgene Speicherung oder Übermittlung von Informationen in einem Trägermedium (Container)
- ⦿ modifiziertes Medium = Steganogramm

Unterschied zur Kryptographie

- ◉ Steganographie

→ ein Außenstehender ist nicht in der Lage, die Existenz der steganographierten Information zu erkennen

- ◉ Kryptographie

→ ein Außenstehender weiß zwar um die Existenz von Informationen, aber aufgrund der Verschlüsselung ist er nicht in der Lage, den Inhalt zu verstehen

Arten der Steganographie/Beispiele

Historisches:

- Antike: Rasur + Tätowierung
- Geheimtinte (z.B.: Zitronensaft)
- schwer erkennbare Wasserzeichen auf Banknoten

Technische Steganographie:

- Computergestützte Stenographie
- Einsatz von Mikrofilmen

Arten der Steganographie/Beispiele

Linguistische Steganographie:

- Johannes Trithemius - Ave-Maria-Chiffre
- Open Code
- Getarnte Geheimschriften

<i>A</i> Deus	<i>A</i> clemens
<i>B</i> Creator	<i>B</i> elementissimus
<i>C</i> Conditor	<i>C</i> pius
<i>D</i> Opifex	<i>D</i> piissimus
<i>E</i> Dominus	<i>E</i> magnus
<i>F</i> Dominator	<i>F</i> excelsus
<i>G</i> Consolator	<i>G</i> maximus
<i>H</i> Arbitrator	<i>H</i> optimus
<i>I</i> Iudex	<i>I</i> sapientissimus
<i>K</i> Illuminator	<i>K</i> inuisibilis
<i>L</i> Illustrator	<i>L</i> immortalis
<i>M</i> Recltor	<i>M</i> aeternus
<i>N</i> Rex	<i>N</i> sempiternus
<i>O</i> Imperator	<i>O</i> gloriosus
<i>P</i> Gubernator	<i>P</i> fortissimus
<i>Q</i> Factor	<i>Q</i> sanctissimus
<i>R</i> Fabricator	<i>R</i> incomprehensibilis
<i>S</i> Conseruator	<i>S</i> omnipotens
<i>T</i> Redemptor	<i>T</i> pacificus
<i>V</i> Auctor	<i>V</i> misericors
<i>X</i> Princeps	<i>X</i> misericordissimus
<i>Y</i> Pastor	<i>Y</i> cunctipotens
<i>Z</i> Moderator	<i>Z</i> magnificus
<i>W</i> Saluator	<i>W</i> excellentissimus
	<i>A</i>

Sicherheit

Ein steganographisches Verfahren ist sicher, wenn:

- ⦿ dritte Personen keinerlei Rückschlüsse auf nichtoffensichtliche Informationen ziehen können
- ⦿ eingebettete Informationen selbst bei Kenntnis von deren Existenz von Dritten nicht auslesbar sind

Sicherheit

- ⦿ Verschlüsselung für zusätzliche Sicherheit

Steganalyse:

- ⦿ Aufdecken steganographischer Kontaminierung
- ⦿ Analyse steganographischer Verfahren

Quellen

- <http://de.wikipedia.org/wiki/Steganographie>
- <http://svenomenal.net/>
- <https://www.datenschutzzentrum.de/selbstdatenschutz/internet/steganographie/index.htm>
- http://de.wikipedia.org/wiki/Computergestuetzte_Steganographie