ITS Teil 3: Kryptografie

Einführung

- Themen der Kryptografie sind u.a. Vertraulichkeit von Daten & Identifizierung von Personen in Rechnernetzen (z.B. Passwort, Fingerabdruck, PIN, TAN)
- Das Wort kommt aus dem grieschischen von „geheim schreiben“, es geht also nicht darum, das z.B. das Senden einer Nachricht unkenntlich gemacht wird (→ Stegenografie), sondern darum, den Text zu verändern und dadurch unleserlich zu machen
- Bsp. Nachricht in Bildpunkte verpacken → man muss wissen, welche Bildpunkte dazu verwendet worden sind
- Anwendungen im Internet: Emails, WWW, Client-Server-Programme (Authentifizierung), VPN, Online-Banking, Remote Access

Symmetrische Verschlüsselung

- Mathematisches Verfahren (Chiffre), um eine Nachricht (Klartext) in ein zufälliges Muster (Chiffretext) umzuwandeln
- Zusätzlich: Verwendung von Schlüsseln
- Gute Verschlüsselungsalgorithmen sind öffentlich bekannt: Sicherheit basiert auf geheimem Schlüssel
- Kryptoanalyse:
    - Ciphertext-Only (nur der Chiffretext bekannt)
    - Known-Plaintext (Klar- und Chiffretext sind bekannt → Schlüssel herausfinden)
    - Chosen-Plaintext (Chiffretext ist bekannt, Chiffrierversuche mit verschiedenen Klartexten)
- Kodewörter:
    - Jede Nachricht entspricht einem Kodewort
    - Vorteil: sehr einfach und bis zum ersten Einsatz absolut sicher
    - Nachteil: nur wenige Nachrichten können kodiert werden, leichtes Erraten beim wiederholten Einsatz
    - Codierung bezeichnet die Substitution auf Basis von Wörtern oder Sätzen
- Caesar-Chiffre:
    - Einfache Form einer Substitutionschiffre
    - Ersetzen oder Vertauschen der Buchstaben
    - Mathematisch ausgedrückt →diese Operation ist die Addition Modulo der Mächtigkeit des Alphabets (n = 26)
    - Analyse: Brute-Force oder Häufigkeitsanalyse
    - Beispiel:

      $Klartext: \quad A \quad B \quad C \quad D \quad E \quad F \quad G$

      $Chiffretext: \quad D \quad E \quad F \quad G \quad H \quad I \quad J$

      $GABE \Rightarrow JDEH$
    - Mathematisch:

      $C = (K + S) \bmod 26 \qquad (im\ Beispiel\ s = 3)$

      $K = (C - S) \bmod 26$

- Häufigkeitsanalyse → den häufigsten Buchstaben suchen → anhand von Sprachmodell einsetzen und Caesarfolge fortsetzen
- Weitere Substitutionschiffre → Freimaurer-Chiffre
- Allgemeine Substitution:
    - Beliebiges (nicht arithmetisch beschreibbares) Vertauschen der Symbole
    - Vorteil: Schlüsselraum gleich $n!$
    - Eine Häufigkeitsanalyse muss für jeden Buchstaben des Chiffretextes erfolgen
- Kryptoanalyse einfacher Substitution:
    - Brute-Force nur bei arithmetischen Verfahren
    - Ausnutzung der Bedeutung einer Sprache:
        - Relative Buchstabenhäufigkeit
        - Bigramme, Trigramme
    - Bekannte Wortgrenzen bzw. häufige Wortendungen
    - Mögliche Nachbarzeichen von Vokalen und Konsonanten
- Permutationschiffren:
    - Buchstaben werden nicht ersetzt, sondern nur vertauscht
    - Eines der ältesten Verfahren
    - Mechanisch einfach umsetzbar, da oft geometrisch beschreibbar
    - Beispiel: Skytal
    - Prinzip → zeilenweises Eintragen des Klartextes in eine Matrix, spaltenweises Auslesen
    - Analysemöglichkeit → Suchen von Bi-/Trigrammen
    - Beispiel für Spalten-Permutation:

      Der verwendete Klartext lautet: Verschluesselungsalgorithmus

      $$\begin{bmatrix} V & E & R & S & C & H & L \\ U & E & S & S & E & L & U \\ N & G & S & A & L & G & O \\ R & I & T & H & M & U & S \end{bmatrix} \Rightarrow VUNREEGIRSSTSSAHCELMULGULUOS$$

    - Blockpermutation mit Schlüssel $(1\ 4\ 3\ 6\ 7\ 5)$ → der Schlüssel zeigt an, wie die Stellen verschoben worden sind, z.B. die 1. Stelle an die 4. Stelle
    - Beispiel für die Block-Permutation:

      Mit dem Schlüssel $(1\ 4\ 3\ 6\ 7\ 5)$ wird aus dem Text der Matrixzeilen

      $CESVLRH—EESUUSL—LGANOSG—MIHRSTU$

      Analyse:
      Die Blocklänge ist zunächst unbekannt → es wird mit dem Trigramm SCH angesetzt

Test mit Blockgröße 5

$CESVL—RHEES—UUSLL—GANOS—GMIHR—STU$

➔ SCH ergibt sich mit folgender Verschiebung: 3 → 4, 1 → 5, 2 → 1

→ $E\_\_C—H\_\_ER$

➔ Die übrigen Buchstaben können keine sinnvolle Lösung herbeiführen

Test mit Blockgröße 6

$CESVLR—HEESUU—SLLGAN—OSGMIH—RSTU$

➔ Das C müsste verschoben werden, dadurch würde auch das H verschoben, was dazu führt, das SCH nicht hergestellt werden kann

➔ Diese Blockgröße funktioniert nicht

Test mit Blockgröße 7

$CESVLRH—EESUUSL—LGANOSG—MIHRSTU$

➔ SCH ergibt sich in Kombination mit EVLR → sinnvoll ist VERSCHL

- Homophone Substitutions-Chiffren:
  - Nachteil einfacher Substitutionen → statistische Eigenschaften des Klartextes sind im Chiffretext enthalten
  - Vermeidung durch unterschiedliche Chiffrezeichen für Klartextzeichen
  - Nachteil → Expansion des Chiffretextes
  - Historisches Beispiel → Beale-Chiffre
  - Sehr sicher aber auch sehr unhandlich
- Polyalphabetische Substitution:
  - Verwendung mehrerer einfacher Substitutionen
  - Reihenfolge und Auswahl der Substitutionen hängen vom Schlüssel ab
  - Nachteile einfacher oder homophoner Substitutionen werden vermieden
- Vigenère-Chiffre:
  - Die Substitution erfolgt addiert mittels eines Schlüsselwortes
  - Die Buchstabenposition des Schlüsselwortes wird auf den Klartext addiert
  - Prinzip → mehrere Caesar-Chiffren
  - Analyse → finden der Schlüssellänge und brechen der entsprechenden Anzahl von Caesar-Chiffren
  - Beispiel:

$$\begin{array}{lcccccccccc} Klartext: & H & O & C & H & S & C & H & U & L & E \\ Schlüssel: & +S & T & U & D & S & T & U & D & S & T \\ Chiffretext: & Z & H & W & K & K & V & B & X & D & X \end{array}$$

Rechenbeispiel:

$H = 7, S = 18 \rightarrow (18+7) \bmod 26 = 25 \rightarrow 25 = Z$

➔ Bei 0 beginnen, weil die Modulorechnung auch dieses Ergebnis haben kann

    - Gleiche Buchstaben entsprechen nicht mehr gleichen Buchstaben im Chiffretext
    - Ist die Schlüssellänge 1, entspricht die Vigenère-Chiffre der Caesar-Chiffre
    - Analyse und Bearbeitung anhand von Vigenère-Quadrat (s. Arbeitsblatt)
- Vernom-Chiffre:
    - Je länger der Schlüssel einer Vigenère-Chiffre, desto schwieriger die Analyse
    - Bei der Vernom-Chiffre ist der Schlüssel genauso lang wie der Klartext
    - Analyse → sehr schwierig
    - Besteht der Schlüssel aus einem sinnvollen Wort, kann eine Häufigkeitsanalyse erfolgreich sein
- One Time Pad:
    - Ist der Schlüssel eines Vernom-Chiffre vollkommen zufällig gewählt, ist keine Analyse mehr möglich
    - Wird der Schlüssel nur einmal (one time) verwendet, besteht absolute Sicherheit
    - Bei Binärdaten → die Addition entspricht einer XOR-Verknüpfung
    - Nachteile: Schlüssellänge, Zufallszahlen