LU05c - Verschlüsselungsverfahren

Mehr Verfahren zum Nachlesen und Ausprobieren https://www.cryptool.org/de/cryptool-online

Dieses Kapitel enthält eine Auswahl an Verschlüsselungsverfahren aus verschiedenen Zeitaltern. Wir beginnen mit den einfachsten Verfahren und steigern uns langsam. Jedem Verfahren werden die jeweiligen Begriffe (siehe LU05a - Verschlüsselung: Einführung zugeordnet.

Caesar-Chiffre

- Kryptographie
- Substitutionsverfahren
- Symmetrische Verschlüsselung

Angeblich soll Julius Caesar dieses Verfahren für seine militärischen Nachrichten eingesetzt haben. Er schrieb seine Nachrichten so, dass er jeden Buchstaben im Alphabet um 3 Positionen verschoben hat. Also wurde „A“ zu „D“, „B“ zu „E“, … bis schliesslich „Z“ zu „C“ wurde. Der Empfänger musste das Verfahren lediglich umkehren um die ursprüngliche Nachricht zu lesen.

Bei diesem Verfahren wird die Anzahl Positionen der Verschiebung als Schlüssel verwendet. Caesar nutzte also den Schlüssel = 3.

Weitere Informationen finden Sie unter https://www.cryptool.org/de/cto/caesar

Vigenère

- Kryptographie
- Substitutionsverfahren
- Symmetrische Verschlüsselung

Wie bei der Caesar-Chiffre werden die Buchstaben ersetzt. Anstatt jeden Buchstaben um die gleiche Anzahl Stellen zu verschieben, bestimmt ein Schlüsselwort die Verschiebung im Alphabet.

Beispiel

```
Klartext:  DIESES VERFAHREN GALT DREIHUNDERT JAHRE LANG ALS NICHT KNACKBAR
Schlüssel: GEHEIM GEHEIMGEH EIMG EHEIMGEHEIM GEHEI MGEH EIM GEHEI MGEHEIMG
```

Zum ersten Buchstaben **D** gehört der Schlüssel **G**. **G** ist im Alphabet der 6. Buchstabe nach dem A. Also wird **D** um 6 Stellen verschoben und wir erhalten **J**.

```
JMLWME BIYJITXIU KIXZ HYIQTARKIZF PEOVM XGRN ETE TMJLB WTEJOJMX
```

Genauere Angaben finden Sie unter https://www.cryptool.org/de/cto/vigenere und im Kapitel LU05d - Vigenère erklärt.

Gartenzaun

- Kryptographie
- Transpositionsverfahren
- Symmetrische Verschlüsselung

Dieses Verfahren wird im separaten Kapitel LU05e - Gartenzaun erklärt.

Tätowierter Bote

- Steganographie

Bei diesem antiken Verfahren wurde die Nachricht durch einen Sklaven überbracht. Eine Drittperson sollte nicht merken, dass eine Nachricht versandt wurde.

1. Rasiere den Kopf eines Sklaven.
2. Tätowiere die Nachricht auf die Kopfhaut des Sklaven.
3. Warte bis die Haare des Sklaven nachgewachsen sind.
4. Sende den Sklaven an den Empfänger der Nachricht.
5. Rasiere den Kopf des Sklaven und lies die Botschaft.

Dieses Verfahren benötigte sehr viel Zeit um die Nachricht zu senden.

Enigma

- Kryptographie
- Substitutionsverfahren
- Symmetrische Verschlüsselung

Die Enigma war eine mechanische Schlüsselmaschine des deutschen Militärs im 2. Weltkrieg.

Die Klartext-Nachricht wird über die Tastatur eingegeben. Dabei leuchtet für jeden Tastenanschlag im Lampenfeld ein Buchstabe auf. Diesen Buchstaben notierte man als chiffrierte Nachricht.

Die Verschlüsselung basierte auf drei drehbaren Walzen, die nach jedem Buchstaben weiter drehten. Dadurch wurde für einen Buchstabe (z.B. A) jedes mal in einen andere chiffrierten Buchstaben übersetzt. Damit der Empfänger die Nachricht wieder entschlüsseln konnte, wurden die Walzen zu Beginn jeder Nachricht in eine vorgegebene Position gebracht. Diese Position war für jeden Tag anders.

Die Sicherheit der Enigma basierte auf drei Faktoren:

- Die Konstruktion der einzelnen Walzen war geheim.
- Je nach Kombination der Walzen entstand ein anderer Chiffre-Text.
- Durch die Startposition der Walzen entstand ein anderer Chiffre-Text.

www.101computing.net - Enigma Simulator

One-time-pad

- Kryptographie
- Substitutionsverfahren
- Symmetrische Verschlüsselung

Beim One Time Pad wird für jede einzelne Nachricht ein neuer Schlüssel verwendet. Da die Beschreibung des Verfahrens recht umfangreich ist, finden Sie diese in einem separaten Kapitel.

Nachricht in einem Bild

Eine Nachricht kann in einer Bilddatei versteckt werden. Dazu werden einzelne Farbinformationen für die Codierung der Nachricht verwendet:

- Ein Bild mit einer Auflösung von 500*300 Pixeln besteht aus 150'000 einzelnen Bildpunkten.
- Die Farbe jedes Pixels im Bild wird durch 24 Bit beschrieben.
- In jedem zehnten Pixel wird das letzte Bit der Farbinformation durch ein Bit der binären Nachricht ersetzt.
  - Somit können 15'000 Bit bzw. 1875 Byte an Text in das Bild integriert werden.
  - Beim Betrachten des Bildes fällt diese kleine Farbabweichung nicht auf.

Ein derart präpariertes Bild können Sie auf einer öffentlichen Webseite hochladen. Niemand würde ahnen, dass eine Nachricht im Bild versteckt ist.

Pretty good privacy

- Kryptographie
- Substitutions- und Transpositionsverfahren
- Hybride Verschlüsselung (asymmetrisch **und** symmetrisch)

Dieses Programm wurde zum Verschlüsseln und Signieren von Nachrichten entwickelt. Es verwendet eine Kombination aus symmetrischer und asymmetrischer Verschlüsselung, weil

- eine asymmetrische Verschlüsselung einer Nachricht sehr rechenintensiv ist und
- für jeden Empfänger die komplette Nachricht neu verschlüsselt werden müsste.

Daher wird die Nachricht mit einem zufälligen symmetrischen Schlüssel, dem sogenannten *session key*, verschlüsselt. Dieser zufällige Schlüssel muss dem Empfänger mitgeteilt werden. Daher wird dieser mit dem öffentlichen Schlüssel des Empfängers verschlüsselt.

Funktionsweise

Verschlüsselung einer Nachricht
1. Erzeuge einen zufälligen Schlüssel (session key).
2. Verschlüssle die Nachricht/Daten mit dem *session key*.
3. Verschlüssle den *session key* mit dem öffentlichen Schlüssel des Empfängers.
4. Sende die verschlüsselte Nachricht bestehend aus Daten und *session key*.

Ursprünglich wurde ein RSA-Algorithmus (siehe RSA-Kryptosystem) zur Verschlüsselung eingesetzt. Neuere Versionen verwenden den Elgamal-Algorithmus (siehe Elgamal-Verschlüsselungsverfahren.

GNU Privacy Guard (GnuPG oder GPG)

GnuPG ist eine Open Source Software die als Ersatz von PGP entwickelt wurde. Die Verschlüsselung erfolgt mit dem gleichen, hybriden Verschlüsselungsverfahren wie PGP. Allerdings werden in GnuPG nur patentfreie Algorithmen zur Verschlüsselung eingesetzt.

Das Add-On „Enigmail“ für Thunderbird verwendet GnuPG für die Verschlüsselung und das Signieren von Nachrichten. Die Installation und der Einsatz von Enigmail ist wird in der LU06 behandelt.

Transport Layer Security (TLS)

Alte Bezeichnung: Secure Sockets Layer (SSL)

- Kryptographie
- Substitutions- und Transpositionsverfahren
- Hybride Verschlüsselung (asymmetrisch **und** symmetrisch)

Transport Layer Security wird für den sicheren Datenaustausch zwischen Webserver und Client eingesetzt. Das Verfahren wird benötigt, da die wenigsten Internetnutzer über einen Public/Private-Key verfügen. Selbst wenn der Nutzer ein solches Keypaar besitzt, wird der Server (z.B. Homebanking-Server) den Schlüssel nicht kennen.

Bei TLS wird eine asymmetrische Verschlüsselung für den Schlüsselaustausch und eine symmetrische Verschlüsselung für die Daten eingesetzt.

Vorgehen

1. Im ersten Schritt wird vom Client eine Verbindung zum Server aufgebaut.
    - Damit der Client sicher mit dem richtigen Server kommuniziert, wird sich der Server mit seinem Zertifikat (siehe zertifikat) ausweisen.
2. Anschliessend bestimmen der Client und der Server den symmetrischen Schlüssel für den weiteren Datenaustausch.
   Dafür kommen zwei Varianten in Frage:
    - Der Client bestimmt eine zufällige Geheimzahl und verschlüsselt diese mit dem öffentlichen Schlüssel des Servers.
    - Client und Server bestimmen eine Geheimzahl mittels Diffie-Hellman-Schlüsselaustausch.

3. Aus der Geheimzahl wird dann der Schlüssel für den Datenaustausch ermittelt.

Entwicklung

In der Vergangenheit basierte die Verschlüsselung immer darauf, dass das eingesetzte Verfahren und dessen Details geheim blieb. Sobald jemand weiss, dass eine Nachricht mit Caesar-Chiffre verschlüsselt ist, kann die Nachricht relativ einfach geknackt werden.

Bei der Enigma war zwar die Funktionsweise bekannt, schliesslich wurde die Erfindung zum Patent angemeldet. Nicht öffentlich bekannt war aber die Verdrahtung der Walzen und die Grundstellung der Walzen zu Beginn der Verschlüsselung.

Bei den meisten modernen Verschlüsselungsverfahren ist Algorithmen öffentlich bekannt. Dadurch können Wissenschaftler prüfen, ob das Verfahren sicher ist und allfällige Schwachstellen erkennen.

---

m114-A0G