Verschlüsselung

Lara Quitte, Tino Jeromin

1 Begriffe

- Verschlüsselung: Die von einem Schlüssel abhängige Umwandlung von Klartext in einen Schlüsseltext, so dass der Klartext aus dem Schlüsseltext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann.
- Kryptographie: Wissenschaft des Verschlüsselns
- Codierung: relativ einfache Art der Verschlüsselung, bei der nicht einzelne Zeichen, sondern ganze Worte verschlüsselt werden. Meist als tabellarische Liste, z.B mit Codebüchern
- Überschlüsselung: Wendet man für mehr Sicherheit die Codierung mehrfach an, so nennt man dies Überschlüsselung
- Schlüssel: entscheidender Parameter bei der Verschlüsselung
- Entschlüsselung: umgekehrter Schritt zur Verschlüsselung
- symmetrische Verschlüsselung: Schlüssel zur Entschlüsselung ist der gleiche, wie schon zur Verschlüsselung
- asymmetrische Verschlüsselung: Schlüssel zur Entschlüsselung ist ungleich dem der Verschlüsselung. Geht hier der Schlüssel verloren, so lässt sich Objekt nicht mehr entschlüsseln
- Entzifferung: verschlüsselten Text lesen, ohne den Schlüssel zu kennen
- Leitungsverschlüsselung: Nachrichten werden nur jeweils für den Nachbarrechner verschlüsselt. Dieser entschlüsselt die Nachricht, verschlüsselt sie erneut und schickt sie an seinen Nachbarn. So geht es weiter bis zum Zielrechner. Vorteil: nur Nachbarn müssen sich auf Verschlüsselung einigen und es kann auf niedriger Protokollebene stattfinden. Nachteil: jeder einzelne Rechner muss vertrauenswürdig und sicher sein.
- Ende-zu-Ende-Verschlüsselung: Nachricht wird vom Absender verschlüsselt und in dieser Form unverändert über mehrere Rechner hinweg zum Empfänger übertragen. Keiner der Rechner hat Einsicht in Klartextnachricht. Nachteil: Absender muss sich mit jedem Beteiligten auf Verfahren einigen.

2 Grundlagen

- außer Text lassen sich auch alle anderen Arten von Informationen verschlüsseln, z.B. Sprachnachrichten, Bilder, Quellcode
- neben geheimem Code gibt es auch offene Verschlüsselung, wie ASCII und Morsecode ¿ zählen nicht zur Verschlüsselung
- Wahl und Geheimhaltung des Schlüssels sind wichtige Vorraussetzungen für Erfolg ¿ z.B. Codebuch, Passwort oder auch E-Mail-Verschlüsselung (hier automatische Generierung des Schlüssels)

- zur Entschlüsselung wird der Schlüssel benötigt
- modernes, aktuell als unbrechbar geltendes Verschlüsselungsverfahren: Advanced Encryption Standard (AES)

3 Klassifizierung

3.1 Symmetrische Verschlüsselung

Symmetrische Verschlüsselungsverfahren verwenden zur Ver- und Entschlüsselung den gleichen Schlüssel.Man unterscheidet zwischen mehreren Klassen:

3.1.1 Substitutionsverfahren

Ein Beispiel ist hier die Caesar-Verschlüsselung. Bei dieser werden Buchstaben des Klartextes durch andere Buchstaben ersetzt.

3.1.2 Transposition

Jeder Buchstabe bleibt hier wie er ist, aber nicht wo er ist. Der Platz im Text wird verändert. Die Revertierung ist eine Methode, bei der die Buchstaben des Wortes umgekehrt werden, z.B. GEHEIMNIS = SINMIEHEG.

3.1.3 Stromverschlüsselung

Die Zeichen des Klartextes werden jeweils einzeln und nacheinander verschlüsselt.

3.1.4 Blockverschlüsselung

Der Klartext wird vor der Verschlüsselung in Blöcker einer bestimmten Größe aufgeteilt. Danach können unterschiedliche Verfahren zur Verschlüsselung angewandt werden.

3.2 Asymmetrische Verschlüsselung

Kennzeichen dieser Verschlüsselung ist, dass zur Verschlüsselung ein völlig anderer Schlüssel verwendet wird, als zur Entschlüsselung. Es wird zwischen öffentlichen und privaten Schlüsseln unterschieden. Der private Schlüssel wird niemals weiter gegeben, wohingegen der öffentliche Schlüssel an einen Partner übergeben werden kann. Dieser benötigt zur Entschlüsselung des Codes jedoch zusätzlich noch einen privaten Schlüssel. Daher ist noch nicht einmal der Verschlüssler selbst in der Lage seine eigene Nachricht, die er mit dem öffentlichen Schlüssel der anderen Person verschlüsselt hat, zu entschlüsseln. Umgekehrt kann eine Person ihren privaten Schlüssel nutzen, um damit Nachrichten zu Verschlüsseln. Dann ist jedermann mit Zugang zum öffentlichen schlüssel in der Lage die Nachricht zu entschlüsseln. Dies dient z.B. zur Authentifizierung.

3.3 Hybridverfahren

Da asymmetrische Verfahren algorithmisch aufwendiger sind als symmetrische, werden in der Praxis oft Kombinationen aus beiden verwendet. Hier wird ein zufällig generierter, individueller Schlüssel mithilfe eines asymmetrischen Verfahrens ausgetauscht und dann gemeinsam als Schlüssel für ein symmetrisches Verfahren genutzt.

4 Anwendung

- Nachrichtenübertragung in Netzwerken, wo Nachricht über mehrere Stationen übertragen wird (Leitungsverschlüsselung Ende-zu-Ende-Verschlüsselung)
- Verschlüsselung von Daten auf Datenträgern

5 Quellen

- https://de.wikipedia.org/wiki/Verschlüsselung