D_KRYPTOGRAFIE_SYM

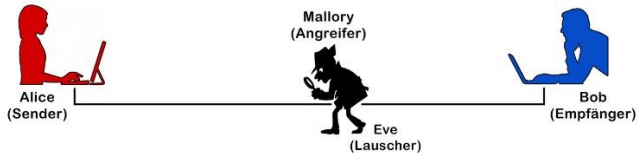
Wir werden uns mit den folgenden Teilbereichen der Kryptografie beschäftigen:

- Symmetrische Verschlüsselung *(Vorzugsweise Klassische Verfahren)*
- Asymmetrische Verschlüsselung
- Digitale Signatur *(Hashwertbildung)*
- Public Key Infrastruktur
- Internet und Zertifikate *(HTTPS, TLS)*
- PGP und OpenPGP *(gpg4win, Kleopatra)*
- Sichere E-Mails *(OpenPGP, S-MIME, Thunderbird)*

Grundlagen zu Verschlüsselungsverfahren

Mit **Kryptografie** war ursprünglich die **Wissenschaft der Verschlüsselung** gemeint. Heute umfasst sie allgemein die Informationssicherheit und die Widerstandsfähigkeit gegen Manipulation und unbefugtes Lesen.

- **Kryptologie**: Wissenschaft vom Entwurf, der Anwendung und der Analyse von kryptografischen Verfahren
- **Kryptografie**: Wie kann eine Nachricht ver- und wieder entschlüsselt werden?
- **Kryptoanalyse**: Wie sicher ist ein Verschlüsselungsverfahren?
- **Akteure** in der Literatur:



- **Symmetrische Verschlüsselung**: Symmetrische Verschlüsselungsverfahren zeichnen sich dadurch aus, dass der Absender die Botschaft mit demselben Schlüssel verschlüsselt, wie der Empfänger, der die Botschaft wieder entschlüsselt. Man unterscheidet zwischen historischen und heutzutage unsicheren Verfahren wie ROT etc. und aktuellen sicheren Verfahren wie AES.
- **Asymmetrische Verschlüsselung**: Asymmetrische Verschlüsselungsverfahren zeichnen sich dadurch aus, dass jeder Teilnehmer ein Schlüsselpaar Public/Privat-Key besitzt. Dies erleichtert den Schlüsseltausch und verringert die Schlüsselanzahl.
- **Digital signieren**: Hier geht es nicht darum, einen Inhalt vor fremden Personen zu verbergen, sondern Authentizität, Integrität und Verbindlichkeit einer Nachricht zu gewährleisten. Es kommt dabei dieselbe Technik zur Anwendung, wie bei der asymmetrischen Verschlüsselung.

Geheimhaltung bedeutet:
Nachrichten unter Verschluss

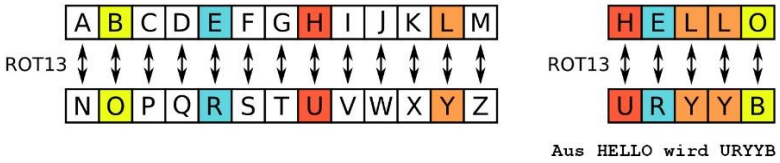
Verschluss bedeutet:
Abgeschlossen mit Schlüssel

Schlüssel bedeutet:
Muss sicher verschickt werden

Symmetrische Verschlüsselung

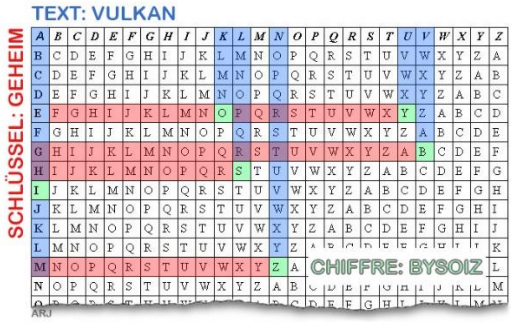
Symmetrische Verschlüsselungsverfahren zeichnen sich dadurch aus, dass der Absender die Botschaft mit demselben Schlüssel verschlüsselt, wie der Empfänger, der die Botschaft wieder entschlüsselt. Schon der römische Feldherr und spätere Kaiser Julius Cäsar kannte einen der folgenden Verschlüsselungstrick und nutzte ihn bei seinen geheimen Botschaften.

Die Rotationschiffre ROT: Dies ist ein **klassisches, historisches Verfahren**. Bei der Rotationschiffre (Verschiebechiffre) wird jeder Buchstabe des lateinischen Alphabets durch den im Alphabet um eine bestimmte Anzahl Stellen davor bzw. dahinter liegenden Buchstaben ersetzt. Bei der ROT-13 wird z.B. um 13 Buchstaben verschoben:



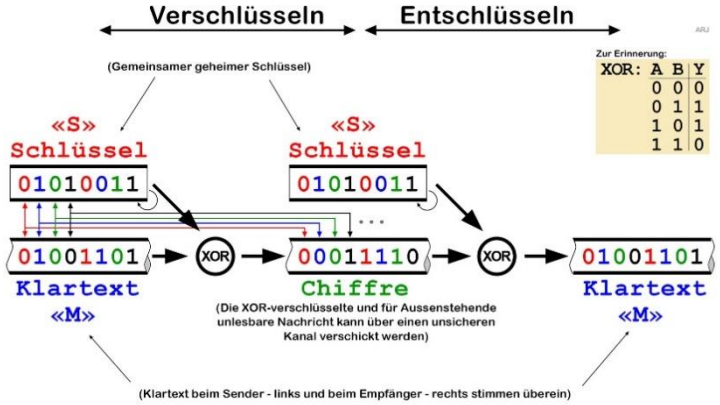
Hier folgen Aufgaben zum Thema. Siehe separates Aufgabenblatt.

Die Vigenèreverschlüsselung: Dies ist ebenfalls ein **klassisches, historisches Verfahren**. Bei monoalphabetischen Chiffrierverfahren wie der Rotationschiffre wird ein Buchstabe immer durch denselben Buchstaben ersetzt. Darum sind derart verschlüsselte Geheimtexte schnell nicht mehr geheim, weil sie mit einer einfachen Häufigkeitsanalyse leicht entschlüsselbar sind. Der nun vorgestellte Algorithmus ist ein einfaches polyalphabetisches Chiffrierverfahren. Beim polyalphabetisches Chiffrierverfahren wird ein Buchstabe in der Regel mit verschiedenen Buchstaben chiffriert. Ein einfaches polyalphabetisches Chiffrierverfahren wurde von Blaise de Vigenère (1523-1596), basierend auf den Ideen eines Benediktinermönches, entwickelt. Das nach ihm benannte Vigenère-Verfahren galt lange Zeit als unknackbar:



Hier folgen Aufgaben zum Thema. Siehe separates Aufgabenblatt.

Die XOR-Stromchiffre: Dies ist ein **klassisches Verfahren**, dass aber heute eher nicht mehr verwendet wird. Bei der Stromchiffre werden Klartext Bit für Bit bzw. Zeichen für Zeichen XOR-ver- bzw.



entschlüsselt. Sender und Empfänger benutzen denselben Schlüssel.

Vorsicht: Sind einem Angreifer Klartext und Chiffre bekannt, kann er den Schlüssel ohne Probleme rekonstruieren.

Hier folgen Aufgaben zum Thema. Siehe separates Aufgabenblatt.

AES (Advanced Encryption Standard): Im Gegensatz zu den vorangegangenen klassischen Verfahren handelt es sich bei AES um ein **aktuelles, modernes, symmetrisches Verschlüsselungsverfahren**, dass z.B. bei PGP zusammen mit dem asynchron verschlüsselten Schlüsseltauch RSA Verwendung findet. Eine ausführliche Beschreibung findet man z.B. auf Wikipedia oder im Crypttool.

Hier folgen Aufgaben zum Thema. Siehe separates Aufgabenblatt.

Schlussfolgerung zur symmetrischen Verschlüsselung: