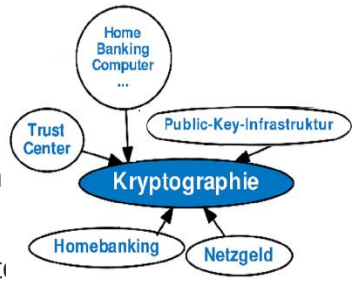
# 12. Kryptographie und Steganographie


Nach *https://www.security-insider.de* ist die *Kryptographie* eine Wissenschaft zur Entwicklung von Kryptosystemen und neben der Kryptoanalyse ein Teilgebiet der Kryptologie. Mit Hilfe kryptographischer Verfahren wie Verschlüsselung sollen Daten vor unbefugtem Zugriff geschützt und sicher ausgetauscht werden. Die Bezeichnung Kryptographie setzt sich aus den beiden Worten altgriechischen Ursprungs 'kryptos' und 'graphein' zusammen. Sie bedeuten 'verborgen' und 'schreiben'. Die Kryptographie und die Kryptoanalyse sind die beiden Teilgebiete der Kryptologie. Es handelt sich bei der Kryptographie um die Wissenschaft, Methoden, Werkzeuge und Algorithmen zu entwickeln, mit deren Hilfe sich Daten chiffrieren und für Unbefugte unkenntlich machen lassen. Diese sollen den unberechtigtem Zugriff auf Informationen verhindern und einen sicheren Datenaustausch ermöglichen. Nur derjenige, für den die Informationen bestimmt sind, kann die Daten lesen und verarbeiten.

Eine dieser Methoden stellt die ***Verschlüsselung*** und die Entschlüsselung von Daten dar. Neben der Verschlüsselung existieren noch weitere kryptographische Verfahren wie das versteckte Einbetten von Informationen in bestimmte Datenformate (versteckte Texte in Bildern). Die Kryptographie befasst sich im IT-Umfeld darüber hinaus mit weiteren Themen der ***Informationssicherheit***. Sie entwickelt Kryptosysteme, die gegen Manipulationen widerstandsfähig sind, und wendet mathematische Verfahren und Algorithmen an. Elementare Ziele sind die Integrität, Authentizität und Vertraulichkeit der Daten. Kryptographie ist auch ein Teilgebiet der Informatik.




**Was sind die Ziele der Kryptographie?**

Die moderne Kryptographie hat im Wesentlichen die vier folgenden Ziele:

- die Daten lassen sich bei der Übermittlung oder beim Speichern nicht verändern, ohne dass dies bemerkbar ist
- die Daten sind vertraulich und können nur von Berechtigten gelesen werden
- sowohl der Sender als auch der Empfänger können sich gegenseitig als Urheber oder Ziel der Informationen bestätigen
- im Nachhinein lässt sich die Urheberschaft der Nachricht nicht mehr bestreit

Je nach kryptographischem System müssen nicht alle Ziele gleichzeitig unterstützt werden. Bestimmte Anwendungsfälle können unter Umständen nur einzelne dieser Ziele erfordern.

**Symmetrische und asymmetrische Kryptographieverfahren**

Während klassische Kryptographieverfahren die Veränderung von Zeichenreihenfolgen (Transposition) und/oder das Ersetzen von Zeichen (Substitution) nutzten, verwenden moderne Verfahren digitale Schlüssel zur Umrechnung von Bitfolgen. Grundsätzlich kann zwischen symmetrischen und asymmetrischen Kryptographieverfahren unterschieden werden.

Bei symmetrischen Verfahren kommt für die Ver- und Entschlüsselung jeweils der gleiche digitale Schlüssel zum Einsatz. Sowohl der Sender als auch der Empfänger verwenden diesen Schlüssel. Damit das kryptographische Verfahren sicher ist, sind die Schlüssel streng geheim zu halten und zu schützen. Beispiele für symmetrische Verschlüsselungsalgorithmen sind:

- RC4 (Ron's Cipher 4),
- DES (Data Encryption Standard),
- Blowfish, Twofish,
- 3DES (Triple Data Encryption Standard) oder
- AES (Advanced Encryption Standard).

Asymmetrische Verfahren benutzen so genannte öffentliche und private Schlüssel. Es handelt sich um ein asymmetrisches Schlüsselpaar. Der private Schlüssel ist geheim zu halten, der öffentliche Schlüssel kann frei bekannt gemacht werden. Lediglich die ***Identität*** des öffentlichen Schlüssels ist sicherzustellen. Dies ist durch gegenseitige Verifizierung oder mit Hilfe einer Public Key Infrastructure möglich. Beispiele für asymmetrische Verschlüsselungsalgorithmen sind Diffie-Hellman oder RSA (Rivest, Shamir, Adleman).

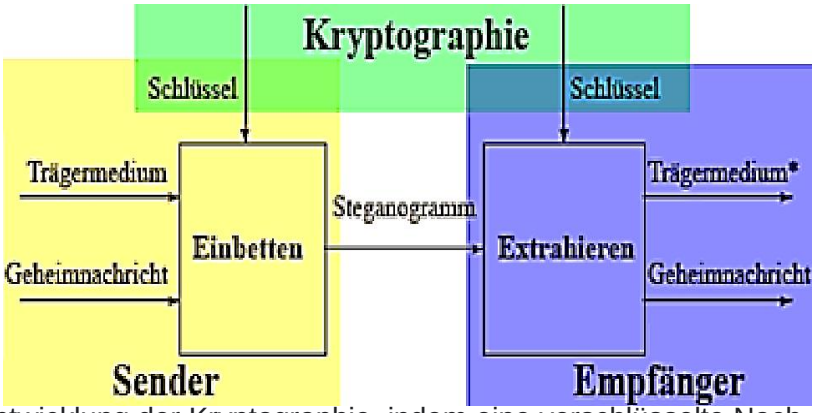
Die Besonderheit der asymmetrischen Kryptographie ist, dass mit einem öffentlichen Schlüssel chiffrierte Daten nur mit einem privaten Schlüssel wieder entschlüsselt werden können. Umgekehrt gilt, dass für die Entschlüsselung von mit einem privaten Schlüssel verschlüsselten Daten ein öffentlicher Schlüssel benötigt wird. Die asymmetrische Kryptographie lässt sich auch einsetzen, um digitale Signaturen zu realisieren. Hierbei verschlüsselt der Urheber mit Hilfe seines privaten Schlüssels einen berechneten Extrakt der Nachricht. Der Empfänger kann den verschlüsselten Wert mit dem öffentlichen Schlüssel des Senders entschlüsseln und mit dem von ihm auf die gleiche Art berechneten Extrakt der Nachricht vergleichen. Stimmen beide Extrakte überein, stammt die Signatur von der vorgegebenen Quelle.

**Doch wie funktioniert moderne digitale Kryptographie konkret?**

Doch wie funktioniert moderne digitale Kryptographie konkret? Ein zu übermittelnder Klartext wird durch einen geheimen Schlüssel, der über einen sicheren Schlüsselkanal transportiert wird, verschlüsselt. Wenn das passiert ist, wird die Nachricht über einen unsicheren Übertragungskanal zum Empfänger weitergeleitet.

**Steganorahie**

Nach Wikipedia ist **Steganographie** (auch **Steganografie**) aus den griechischen Wörtern ‚verborgen' und ‚Schrift' gebildet und bezeichnet die Kunst oder Wissenschaft der verborgenen Speicherung oder Übermittlung von Informationen in einem Trägermedium (Container). Das Wort lässt sich auf die griechischen Bestandteile 'bedeckt (steganos)' und ‚schreiben' zurückführen, bedeutet wörtlich „bedeckt schreiben" bzw. „geheimes Schreiben". Das modifizierte Medium wird als *Steganogramm* bezeichnet.




Steganographie ist eine damit eine Weiterentwicklung der Kryptographie, indem eine verschlüsselte Nachricht so versteckt wird, dass niemand vermuten kann, dass sie überhaupt existiert. Im Idealfall merkt also niemand, der fremde Daten überprüft, dass sich darin noch weitere, verschlüsselte Informationen verbergen.

Darum macht die Steganografie mit vorhergehender Kryptografie Sinn, indem Daten zuerst per Kryptografie verschlüsselt und dann per Steganografie versteckt werden, z. B. durch Verstecken des Chiffrates in leichten Farbveränderungen eines Digital-Fotos. Selbst, wenn der Angreifer die Tarnung aufdecken würde, könnte er das dann gefundene Chiffrat immer noch nicht entziffern können. Die nachgestellte Steganografie ist also besonders sinnvoll, wenn Transportwege genutzt werden, bei denen die Botschaft einem Angreifer in die Hände fallen könnte.

## Fragen zu **Kryptographie und Steganographie**

**1.** Was ist Kryptographie?

**2.** Was bedeutet Verschlüsselung?

**3.** Beschreiben Sie mit einem gewählten Beispiel die Kryptographie?

**4.** Warum ist Kryptografie wichtig?

**5.** Was sind die 4 Ziele der Kryptographie?

**6.** Welche Kryptographie Verfahren gibt es?

**7.** Was ist der Unterschied zwischen Kryptographie und Kryptologie?

**8.** Wo kommt Kryptographie zum Einsatz?

**9.** Was ist das Ziel von Kryptographie?

Antworten in word --> Block12 Ordner

**10.** Wie sicher ist Kryptographie?

**11.** Wie entstand und woher kommt der Name 'Kryptographie' genau?

**12.** Wie entschlüsselt man Kryptographie?

**13.** Wie entstand die Kryptographie?

**14.** Was ist ein Schlüssel in der Kryptographie?

**15.** Was ist das sicherste Verschlüsselungsverfahren?

**16.** Welche Verschlüsselungsverfahren werden aktuell genutzt?

**17.** Wie sicher ist 256 Bit Sicherheit?

**18.** In welchem Fall muss Kryptographie angewendet werden?

**19.** Was ist der Unterschied zwischen Steganographie und Kryptographie?

**20.** Was sind private und öffentliche Schlüssel?

**21.** Wie viele Verschlüsselungen gibt es?

**22.** Wie geht verschlüsseln?

**23.** Wie kann man den Cäsar Code knacken?

**24.** Wie Länge dauert es ein 256 Bit Passwort zu Knacken?

**25.** Was ist ein 128 Bit Schlüssel?

**26.** Wie lange dauert es eine 128 Bit-Verschlüsselung zu knacken und was genau ist AES-Verschlüsselung?

**27.** Wie viele Zeichen sind 256 Bit?

**28.** Sollte man E-Mails verschlüsseln?

**29.** Was ist die stärkste Verschlüsselung?

**30.** Wie verschlüsselt AES?

**31.** Was sind die 4 Ziele der Kryptographie?

**32.** Wie kann ich mein Handy verschlüsseln?

**33.** Was versteht man unter Steganographie?