Sicherheit von Informationen

\\//_

18. Dezember 2020

Gliederung

Anforderungen an die Informationssicherheit

Als **Informationssicherheit**

. . . bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden Systemen, die die

Anforderungen an die Informationssicherheit

Als **Informationssicherheit**

. . . bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden Systemen, die die

- Vertraulichkeit,

Anforderungen an die Informationssicherheit

Als **Informationssicherheit**

. . . bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden Systemen, die die

- Vertraulichkeit,
- Verfügbarkeit und

Anforderungen an die Informationssicherheit

Als **Informationssicherheit**

. . . bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden Systemen, die die

- Vertraulichkeit,
- Verfügbarkeit und
- Integrität sicherstellen.

Anforderungen an die Informationssicherheit

Als **Informationssicherheit**

. . . bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden Systemen, die die

- Vertraulichkeit,
- Verfügbarkeit und
- Integrität sicherstellen.

Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten Informationen.

Vertraulichkeit

. . . ist die Eigenschaft einer Nachricht, nur für einen beschränkten Empfängerkreis vorgesehen zu sein.

Vertraulichkeit

. . . ist die Eigenschaft einer Nachricht, nur für einen beschränkten Empfängerkreis vorgesehen zu sein.

. . . wird in Deutschland durch Rechtsnormen geschützt:

Vertraulichkeit

. . . ist die Eigenschaft einer Nachricht, nur für einen beschränkten Empfängerkreis vorgesehen zu sein.

. . . wird in Deutschland durch Rechtsnormen geschützt:

- **Schutz der Vertraulichkeit des Wortes**

Vertraulichkeit

. . . ist die Eigenschaft einer Nachricht, nur für einen beschränkten Empfängerkreis vorgesehen zu sein.

. . . wird in Deutschland durch Rechtsnormen geschützt:

- **Schutz der Vertraulichkeit des Wortes** ➠ nicht öffentliche Äußerungen dürfen ohne Einverständnis des Sprechers nicht aufgezeichnet werden

Vertraulichkeit

. . . ist die Eigenschaft einer Nachricht, nur für einen beschränkten Empfängerkreis vorgesehen zu sein.

. . . wird in Deutschland durch Rechtsnormen geschützt:

- **Schutz der Vertraulichkeit des Wortes** ➠ nicht öffentliche Äußerungen dürfen ohne Einverständnis des Sprechers nicht aufgezeichnet werden
- **Brief- und Fernmeldegeheimnis**

Vertraulichkeit

. . . ist die Eigenschaft einer Nachricht, nur für einen beschränkten Empfängerkreis vorgesehen zu sein.

. . . wird in Deutschland durch Rechtsnormen geschützt:

- **Schutz der Vertraulichkeit des Wortes** ➠ nicht öffentliche Äußerungen dürfen ohne Einverständnis des Sprechers nicht aufgezeichnet werden
- **Brief- und Fernmeldegeheimnis** ➠ gelten für Postsendungen, Telefongespräche und elektronische Übermittlungen

Vertraulichkeit

. . . ist die Eigenschaft einer Nachricht, nur für einen beschränkten Empfängerkreis vorgesehen zu sein.

. . . wird in Deutschland durch Rechtsnormen geschützt:

- **Schutz der Vertraulichkeit des Wortes** ➠ nicht öffentliche Äußerungen dürfen ohne Einverständnis des Sprechers nicht aufgezeichnet werden
- **Brief- und Fernmeldegeheimnis** ➠ gelten für Postsendungen, Telefongespräche und elektronische Übermittlungen
- **Schweigepflicht, Beichtgeheimnis und Verschwiegenheitspflicht**

Vertraulichkeit

. . . ist die Eigenschaft einer Nachricht, nur für einen beschränkten Empfängerkreis vorgesehen zu sein.

. . . wird in Deutschland durch Rechtsnormen geschützt:

- **Schutz der Vertraulichkeit des Wortes** ➠ nicht öffentliche Äußerungen dürfen ohne Einverständnis des Sprechers nicht aufgezeichnet werden
- **Brief- und Fernmeldegeheimnis** ➠ gelten für Postsendungen, Telefongespräche und elektronische Übermittlungen
- **Schweigepflicht, Beichtgeheimnis und Verschwiegenheitspflicht** ➠ schützen Kommunikation mit bestimmten Berufsgruppen (Ärzte, Geistliche, Anwälte, Journalisten, Banken)

Vertraulichkeit

Die Vertraulichkeit von Informationen kann durch **technische Maßnahmen** gewährleistet werden:

Vertraulichkeit

Die Vertraulichkeit von Informationen kann durch **technische Maßnahmen** gewährleistet werden:

- Verschlüsselung (➠ Kryptographie), z. B.:

Vertraulichkeit

Die Vertraulichkeit von Informationen kann durch **technische Maßnahmen** gewährleistet werden:

- Verschlüsselung (➠ Kryptographie), z. B.:
  - Webseiten mit HTTPS (➠ Online-Banking)

Vertraulichkeit

Die Vertraulichkeit von Informationen kann durch **technische Maßnahmen** gewährleistet werden:

- Verschlüsselung (➠ Kryptographie), z. B.:
  - Webseiten mit HTTPS (➠ Online-Banking)
  - E-Mail mit PGP (**P**retty **G**ood **P**rivacy ➠ Programm zur Verschlüsselung und zum Unterschreiben von Daten)

Vertraulichkeit

Die Vertraulichkeit von Informationen kann durch **technische Maßnahmen** gewährleistet werden:

- Verschlüsselung (➠ Kryptographie), z. B.:
  - Webseiten mit HTTPS (➠ Online-Banking)
  - E-Mail mit PGP (**P**retty **G**ood **P**rivacy ➠ Programm zur Verschlüsselung und zum Unterschreiben von Daten)
- Verstecken (➠ Steganographie), z. B.:

Vertraulichkeit

Die Vertraulichkeit von Informationen kann durch **technische Maßnahmen** gewährleistet werden:

- Verschlüsselung (➠ Kryptographie), z. B.:
  - Webseiten mit HTTPS (➠ Online-Banking)
  - E-Mail mit PGP (**P**retty **G**ood **P**rivacy ➠ Programm zur Verschlüsselung und zum Unterschreiben von Daten)
- Verstecken (➠ Steganographie), z. B.:
  - Mikropunkte: Verstecken von mikroskopisch kleinen Informationen (bis A4-Seite) in Satzzeichen oder i-Punkten (2. Weltkrieg)

Vertraulichkeit

Die Vertraulichkeit von Informationen kann durch **technische Maßnahmen** gewährleistet werden:

- Verschlüsselung (➠ Kryptographie), z. B.:
  - Webseiten mit HTTPS (➠ Online-Banking)
  - E-Mail mit PGP (**P**retty **G**ood **P**rivacy ➠ Programm zur Verschlüsselung und zum Unterschreiben von Daten)
- Verstecken (➠ Steganographie), z. B.:
  - Mikropunkte: Verstecken von mikroskopisch kleinen Informationen (bis A4-Seite) in Satzzeichen oder i-Punkten (2. Weltkrieg)
  - Verstecken von Daten in Trägerdaten, wie Bild- und Audiodaten (➠ enthalten Rauschen)

Verfügbarkeit

. . . ist die Wahrscheinlichkeit, mit der ein technisches System bestimmte Anforderungen innerhalb eines vereinbarten Zeitrahmens erfüllt. Sie ist ein Qualitätskriterium eines technischen Systems.

Verfügbarkeit

. . . ist die Wahrscheinlichkeit, mit der ein technisches System bestimmte Anforderungen innerhalb eines vereinbarten Zeitrahmens erfüllt. Sie ist ein Qualitätskriterium eines technischen Systems.

Definition anhand der Zeit, in der ein System verfügbar ist:

$$\text{Verfügbarkeit} = \frac{\text{Gesamtzeit} - \text{Gesamtausfallzeit}}{\text{Gesamtzeit}} (\cdot 100\,\%)$$

Verfügbarkeit

. . . ist die Wahrscheinlichkeit, mit der ein technisches System bestimmte Anforderungen innerhalb eines vereinbarten Zeitrahmens erfüllt. Sie ist ein Qualitätskriterium eines technischen Systems.

Definition anhand der Zeit, in der ein System verfügbar ist:

$$\text{Verfügbarkeit} = \frac{\text{Gesamtzeit} - \text{Gesamtausfallzeit}}{\text{Gesamtzeit}} (\cdot 100\,\%)$$

Systeme, die mit einer hohen Verfügbarkeit (99,99 % oder besser) laufen müssen, bezeichnet man als **hochverfügbare Systeme**.

Verfügbarkeit

Wie kann man die Verfügbarkeit des eigenen Rechners und der eigenen Daten erhöhen?

Verfügbarkeit

Wie kann man die Verfügbarkeit des eigenen Rechners und der eigenen Daten erhöhen?

Hier einige **Vorschläge:**

Verfügbarkeit

Wie kann man die Verfügbarkeit des eigenen Rechners und der eigenen Daten erhöhen?

Hier einige **Vorschläge:**

- Einsatz von Qualitätshardware (➠ teuer ☹)

Verfügbarkeit

Wie kann man die Verfügbarkeit des eigenen Rechners und der eigenen Daten erhöhen?

Hier einige **Vorschläge:**

- Einsatz von Qualitätshardware (➠ teuer ☹)
- Zuverlässiges Betriebssystem ➠ z. B. GNU/Linux ☺

Verfügbarkeit

Wie kann man die Verfügbarkeit des eigenen Rechners und der eigenen Daten erhöhen?

Hier einige **Vorschläge:**

- Einsatz von Qualitätshardware (➠ teuer ☹)
- Zuverlässiges Betriebssystem ➠ z. B. GNU/Linux ☺
- **R**edundant **A**rray of **I**ndependent **D**isks (RAID)

Verfügbarkeit

Wie kann man die Verfügbarkeit des eigenen Rechners und der eigenen Daten erhöhen?

Hier einige **Vorschläge:**

- Einsatz von Qualitätshardware (➠ teuer ☹)
- Zuverlässiges Betriebssystem ➠ z. B. GNU/Linux ☺
- **R**edundant **A**rray of **I**ndependent **D**isks (RAID)
- regelmäßige Sicherheitskopien ☺

Verfügbarkeit

Wie kann man die Verfügbarkeit des eigenen Rechners und der eigenen Daten erhöhen?

Hier einige **Vorschläge:**

- Einsatz von Qualitätshardware (➠ teuer ☹)
- Zuverlässiges Betriebssystem ➠ z. B. GNU/Linux ☺
- **R**edundant **A**rray of **I**ndependent **D**isks (RAID)
- regelmäßige Sicherheitskopien ☺
- Einsatz von modernen Journaling-Dateisystemen, z. B. ext4, XFS (Linux) oder NTFS (Windows)

Verfügbarkeit

Wie kann man die Verfügbarkeit des eigenen Rechners und der eigenen Daten erhöhen?

Hier einige **Vorschläge:**

- Einsatz von Qualitätshardware (➠ teuer ☹)
- Zuverlässiges Betriebssystem ➠ z. B. GNU/Linux ☺
- **R**edundant **A**rray of **I**ndependent **D**isks (RAID)
- regelmäßige Sicherheitskopien ☺
- Einsatz von modernen Journaling-Dateisystemen, z. B. ext4, XFS (Linux) oder NTFS (Windows)
- Einsatz offener Standards beim Speichern von Daten (z. B. OASIS Open Document Format for Office Applications – ODF)

Integrität

. . . (von lat. *integritas* „Unversehrtheit“) ist die Korrektheit (Unversehrtheit) von Daten und die korrekte Funktionsweise von Systemen.

Integrität

. . . (von lat. *integritas* „Unversehrtheit“) ist die Korrektheit (Unversehrtheit) von Daten und die korrekte Funktionsweise von Systemen.

Um die Integrität von übertragenen Daten zu überprüfen, kann man z. B. **Hashfunktionen** *(bilden große Eingabemengen auf kleinere Zielmengen ab)* benutzen:

Integrität

> . . . (von lat. *integritas* „Unversehrtheit“) ist die Korrektheit (Unversehrtheit) von Daten und die korrekte Funktionsweise von Systemen.

Um die Integrität von übertragenen Daten zu überprüfen, kann man z. B. **Hashfunktionen** *(bilden große Eingabemengen auf kleinere Zielmengen ab)* benutzen:

- Zyklische Redundanzprüfung (CRC), 1961 entwickelt
  - ➠ im Terminal eingeben: `crc32 Dateiname` ↵

Integrität

. . . (von lat. *integritas* „Unversehrtheit“) ist die Korrektheit (Unversehrtheit) von Daten und die korrekte Funktionsweise von Systemen.

Um die Integrität von übertragenen Daten zu überprüfen, kann man z. B. **Hashfunktionen** *(bilden große Eingabemengen auf kleinere Zielmengen ab)* benutzen:

- Zyklische Redundanzprüfung (CRC), 1961 entwickelt
  ➠ im Terminal eingeben: `crc32 Dateiname` ↵
- Message-Digest Algorithm 5 (MD5), 1991 entwickelt
  ➠ im Terminal eingeben: `md5sum Dateiname` ↵

Integrität

. . . (von lat. *integritas* „Unversehrtheit“) ist die Korrektheit (Unversehrtheit) von Daten und die korrekte Funktionsweise von Systemen.

Um die Integrität von übertragenen Daten zu überprüfen, kann man z. B. **Hashfunktionen** *(bilden große Eingabemengen auf kleinere Zielmengen ab)* benutzen:

- Zyklische Redundanzprüfung (CRC), 1961 entwickelt
  ➠ im Terminal eingeben: `crc32 Dateiname` ↵
- Message-Digest Algorithm 5 (MD5), 1991 entwickelt
  ➠ im Terminal eingeben: `md5sum Dateiname` ↵
- Secure Hash Algorithm (SHA), SHA-1 wurde 1994 veröffentlicht ➠ Terminal: `sha1sum Dateiname` ↵

Praktisches Beispiel: Überprüfen eines Downloads

Integrität

Praktisches Beispiel: Überprüfen eines Downloads

1. Datei herunterladen

Integrität

Praktisches Beispiel: Überprüfen eines Downloads

1. Datei herunterladen
2. Ermitteln des Hashwertes der heruntergeladenen Datei

Integrität

Praktisches Beispiel: Überprüfen eines Downloads

1. Datei herunterladen
2. Ermitteln des Hashwertes der heruntergeladenen Datei
3. Vergleichen des ermittelten Hashwertes mit dem auf der Webseite veröffentlichten Hashwert (müssen übereinstimmen!)

Integrität

Praktisches Beispiel: Überprüfen eines Downloads

1. Datei herunterladen
2. Ermitteln des Hashwertes der heruntergeladenen Datei
3. Vergleichen des ermittelten Hashwertes mit dem auf der Webseite veröffentlichten Hashwert (müssen übereinstimmen!)

Beispiele für Downloadquellen mit Hashwerten:

- https://www.virtualbox.org/wiki/Downloads (SHA256 und MD5)
- ftp://ftp5.gwdg.de/pub/opensuse/distribution/12.3/iso/ (SHA1 und MD5)

Integrität

Sicherheit des Secure Hash Algorithm – Aktueller Stand:

Integrität

Sicherheit des Secure Hash Algorithm – Aktueller Stand:

- SHA-1 von 1994 gilt seit 2005 als unsicher

Integrität

Sicherheit des Secure Hash Algorithm – Aktueller Stand:

- SHA-1 von 1994 gilt seit 2005 als unsicher
- als moderne Alternative kann die SHA-2-Familie (SHA-224, SHA-256, SHA-384, SHA-512) genutzt werden, z. B.: (`sha512sum Dateiname` ↵)

Integrität

Sicherheit des Secure Hash Algorithm – Aktueller Stand:

- SHA-1 von 1994 gilt seit 2005 als unsicher
- als moderne Alternative kann die SHA-2-Familie (SHA-224, SHA-256, SHA-384, SHA-512) genutzt werden, z. B.: (`sha512sum Dateiname` ↵)
- SHA-3 (Keccak) wurde 2012 vom US-amerikanischen NIST (**N**ational **I**nstitute of **S**tandards and **T**echnology) als Gewinner der SHA-3-Wettbewerbs bekannt gegeben und wird als Alternative zu SHA-2 standardisiert

Kryptologie

. . . ist eine Wissenschaft, die sich mit Informationssicherheit beschäftigt. Im engeren Sinne geht es dabei um Verschlüsselungsverfahren.

Kryptologie

. . . ist eine Wissenschaft, die sich mit Informationssicherheit beschäftigt. Im engeren Sinne geht es dabei um Verschlüsselungsverfahren.

Begriffe:

Kryptologie

. . . ist eine Wissenschaft, die sich mit Informationssicherheit beschäftigt. Im engeren Sinne geht es dabei um Verschlüsselungsverfahren.

Begriffe:

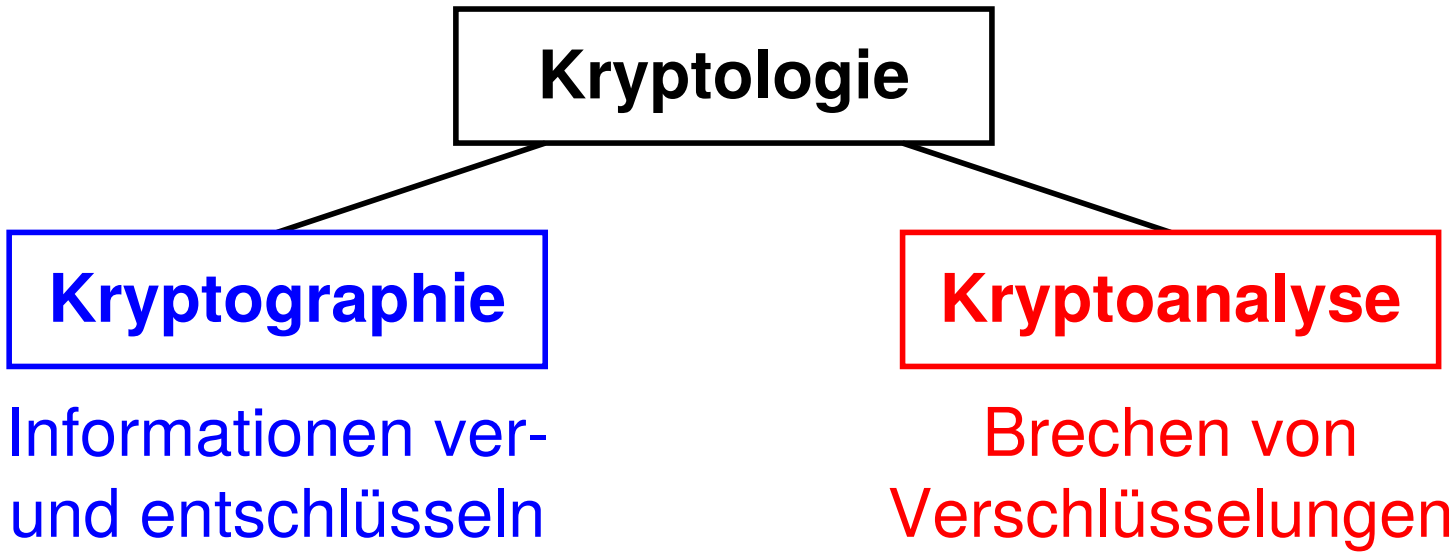
κρυπτός (griech.) „versteckt, verborgen, geheim“

Kryptologie

. . . ist eine Wissenschaft, die sich mit Informationssicherheit beschäftigt. Im engeren Sinne geht es dabei um Verschlüsselungsverfahren.

Begriffe:

κρυπτός (griech.) „versteckt, verborgen, geheim“



Kryptographie – Ziele

1. **Vertraulichkeit/Zugriffsschutz**

Kryptographie – Ziele

1. **Vertraulichkeit/Zugriffsschutz** ➠ Zugriff auf Information nur durch berechtigte Personen

Kryptographie – Ziele

1. **Vertraulichkeit/Zugriffsschutz** ➠ Zugriff auf Information nur durch berechtigte Personen
2. **Integrität/Änderungsschutz**

Kryptographie – Ziele

1. **Vertraulichkeit/Zugriffsschutz** ➠ Zugriff auf Information nur durch berechtigte Personen
2. **Integrität/Änderungsschutz** ➠ Daten müssen nachweislich vollständig und unverändert sein

Kryptographie – Ziele

1. **Vertraulichkeit/Zugriffsschutz** ➠ Zugriff auf Information nur durch berechtigte Personen
2. **Integrität/Änderungsschutz** ➠ Daten müssen nachweislich vollständig und unverändert sein
3. **Authentizität/Fälschungsschutz**

Kryptographie – Ziele

1. **Vertraulichkeit/Zugriffsschutz** ➠ Zugriff auf Information nur durch berechtigte Personen
2. **Integrität/Änderungsschutz** ➠ Daten müssen nachweislich vollständig und unverändert sein
3. **Authentizität/Fälschungsschutz** ➠ Urheber/Absender der Nachricht soll eindeutig identifizierbar sein

Kryptographie – Ziele

1. **Vertraulichkeit/Zugriffsschutz** ➠ Zugriff auf Information nur durch berechtigte Personen
2. **Integrität/Änderungsschutz** ➠ Daten müssen nachweislich vollständig und unverändert sein
3. **Authentizität/Fälschungsschutz** ➠ Urheber/Absender der Nachricht soll eindeutig identifizierbar sein
4. **Verbindlichkeit/Nichtabstreitbarkeit**

Kryptographie – Ziele

1. **Vertraulichkeit/Zugriffsschutz** ➠ Zugriff auf Information nur durch berechtigte Personen
2. **Integrität/Änderungsschutz** ➠ Daten müssen nachweislich vollständig und unverändert sein
3. **Authentizität/Fälschungsschutz** ➠ Urheber/Absender der Nachricht soll eindeutig identifizierbar sein
4. **Verbindlichkeit/Nichtabstreitbarkeit** ➠ Urheberschaft soll sich gegenüber Dritten nachweisen lassen (d.h. Urheber kann Urheberschaft nicht bestreiten)

Kryptographie – Verfahren

(klassische) symmetrische Verfahren

Kryptographie – Verfahren

(klassische) symmetrische Verfahren ➠ verwenden den gleichen Schlüssel für Ver- und Entschlüsselung, z. B.:

Kryptographie – Verfahren

(klassische) symmetrische Verfahren ➠ verwenden den gleichen Schlüssel für Ver- und Entschlüsselung, z. B.:

- Caesar-Verschiebechiffre (Gaius Julius Caesar, 100 v. Chr. – 44 v. Chr.)

Kryptographie – Verfahren

(klassische) symmetrische Verfahren ➠ verwenden den gleichen Schlüssel für Ver- und Entschlüsselung, z. B.:

- Caesar-Verschiebechiffre (Gaius Julius Caesar, 100 v. Chr. – 44 v. Chr.)
- Vigenère-Verschlüsselung (Blaise de Vigenère, 1523 – 1596)

Kryptographie – Verfahren

(klassische) symmetrische Verfahren ➠ verwenden den gleichen Schlüssel für Ver- und Entschlüsselung, z. B.:

- Caesar-Verschiebechiffre (Gaius Julius Caesar, 100 v. Chr. – 44 v. Chr.)
- Vigenère-Verschlüsselung (Blaise de Vigenère, 1523 – 1596)
- Vernam-Chiffre (Gilbert Sandford Vernam, 1890 – 1960), Spezialfall der Vigenère-Chiffre, bei echt zufälligem Schlüssel perfekt sicher (➠ Einmal-verschlüsselung, One-Time-Pad)

Kryptographie – Verfahren

(klassische) symmetrische Verfahren ➠ verwenden den gleichen Schlüssel für Ver- und Entschlüsselung, z. B.:

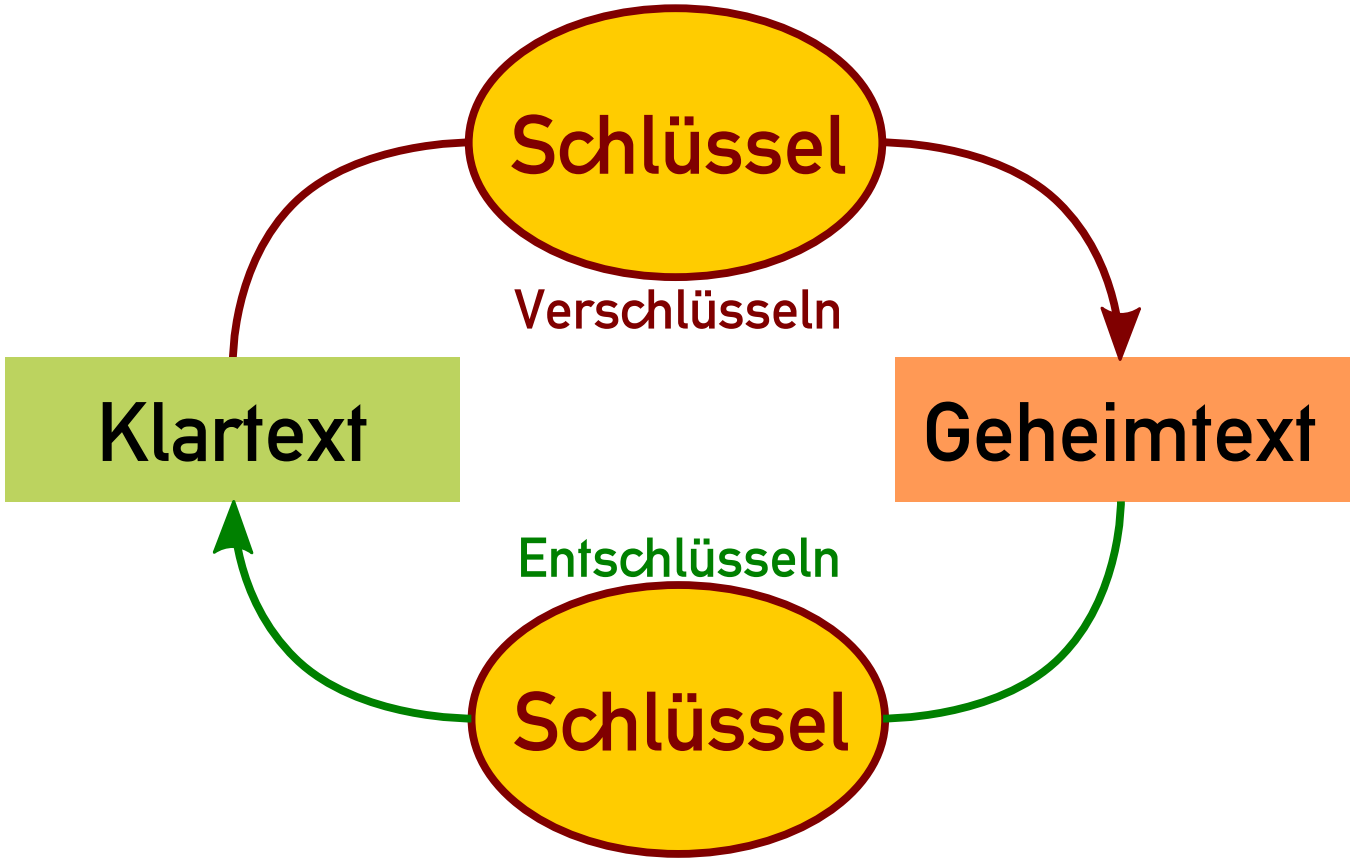
- Caesar-Verschiebechiffre (Gaius Julius Caesar, 100 v. Chr. – 44 v. Chr.)
- Vigenère-Verschlüsselung (Blaise de Vigenère, 1523 – 1596)
- Vernam-Chiffre (Gilbert Sandford Vernam, 1890 – 1960), Spezialfall der Vigenère-Chiffre, bei echt zufälligem Schlüssel perfekt sicher (➠ Einmal-verschlüsselung, One-Time-Pad)
- moderne Verfahren wie z. B. DES, AES, IDEA, Blowfish, CAST und RC6

symmetrische Verfahren – Prinzip

Verschlüsselung und **Entschlüsselung** erfolgen mit dem gleichen geheimen Schlüssel:

symmetrische Verfahren – Prinzip

Verschlüsselung und **Entschlüsselung** erfolgen mit dem gleichen geheimen Schlüssel:



Kryptographie – Verfahren

(moderne) asymmetrische Verfahren

Kryptographie – Verfahren

(moderne) asymmetrische Verfahren ➠ verwenden unterschiedliche Schlüssel für Ver- und Entschlüsselung (öffentlicher und privater Schlüssel), z. B.:

Kryptographie – Verfahren

(moderne) asymmetrische Verfahren ➠ verwenden unterschiedliche Schlüssel für Ver- und Entschlüsselung (öffentlicher und privater Schlüssel), z. B.:

- Diffie-Hellman-Merkle-Schlüsselaustausch (1976 von Martin Hellman, Whitfield Diffie und Ralph Merkle an der Stanford-Universität entwickeltes Protokoll)

Kryptographie – Verfahren

(moderne) asymmetrische Verfahren ➠ verwenden unterschiedliche Schlüssel für Ver- und Entschlüsselung (öffentlicher und privater Schlüssel), z. B.:

- Diffie-Hellman-Merkle-Schlüsselaustausch (1976 von Martin Hellman, Whitfield Diffie und Ralph Merkle an der Stanford-Universität entwickeltes Protokoll)
- RSA-Verfahren (1977 von Ronald L. **R**ivest, Adi **S**hamir und Leonard M. **A**dleman entwickelt)

Kryptographie – Verfahren

(moderne) asymmetrische Verfahren ➠ verwenden unterschiedliche Schlüssel für Ver- und Entschlüsselung (öffentlicher und privater Schlüssel), z. B.:

- Diffie-Hellman-Merkle-Schlüsselaustausch (1976 von Martin Hellman, Whitfield Diffie und Ralph Merkle an der Stanford-Universität entwickeltes Protokoll)
- RSA-Verfahren (1977 von Ronald L. **R**ivest, Adi **S**hamir und Leonard M. **A**dleman entwickelt)
- moderne Public-Key-Verschlüsselungsverfahren bei z. B. OpenPGP, S/MIME, SSH, SSL/TLS und HTTPS

asymmetrische Verfahren – Prinzip (1)

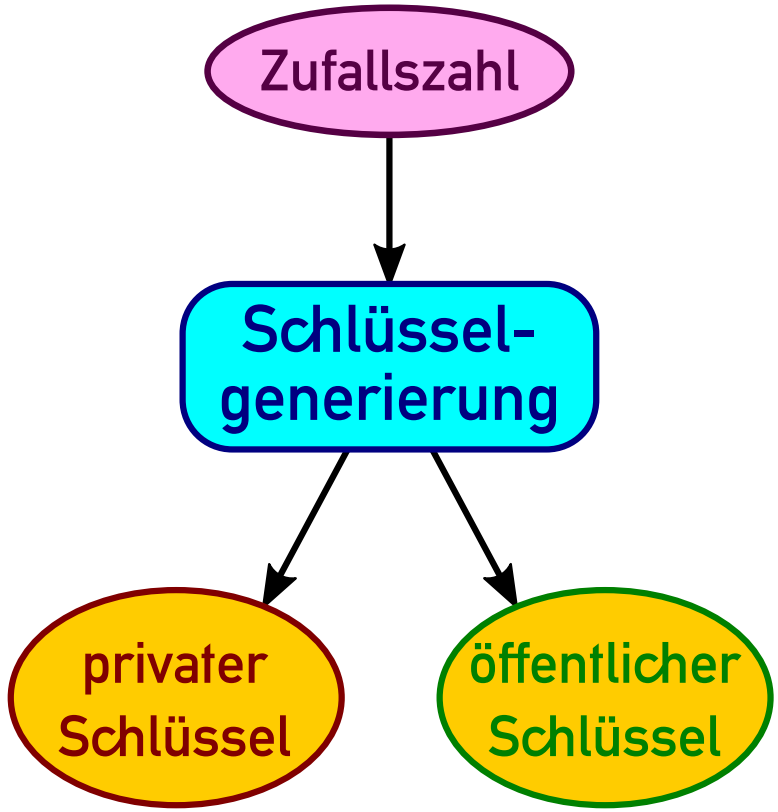
Die **Schlüsselgenerierung** beruht auf „Falltürfunktionen“, also Funktionen, die leicht zu berechnen, aber ohne ein Geheimnis (die „Falltür“) praktisch unmöglich zu invertieren sind.

asymmetrische Verfahren – Prinzip (1)

Die **Schlüsselgenerierung** beruht auf „Falltürfunktionen“, also Funktionen, die leicht zu berechnen, aber ohne ein Geheimnis (die „Falltür“) praktisch unmöglich zu invertieren sind.
Der öffentliche Schlüssel ist dann eine Beschreibung der Funktion, der private Schlüssel ist die Falltür.

asymmetrische Verfahren – Prinzip (1)

Die **Schlüsselgenerierung** beruht auf „Falltürfunktionen“, also Funktionen, die leicht zu berechnen, aber ohne ein Geheimnis (die „Falltür“) praktisch unmöglich zu invertieren sind.
Der öffentliche Schlüssel ist dann eine Beschreibung der Funktion, der private Schlüssel ist die Falltür.

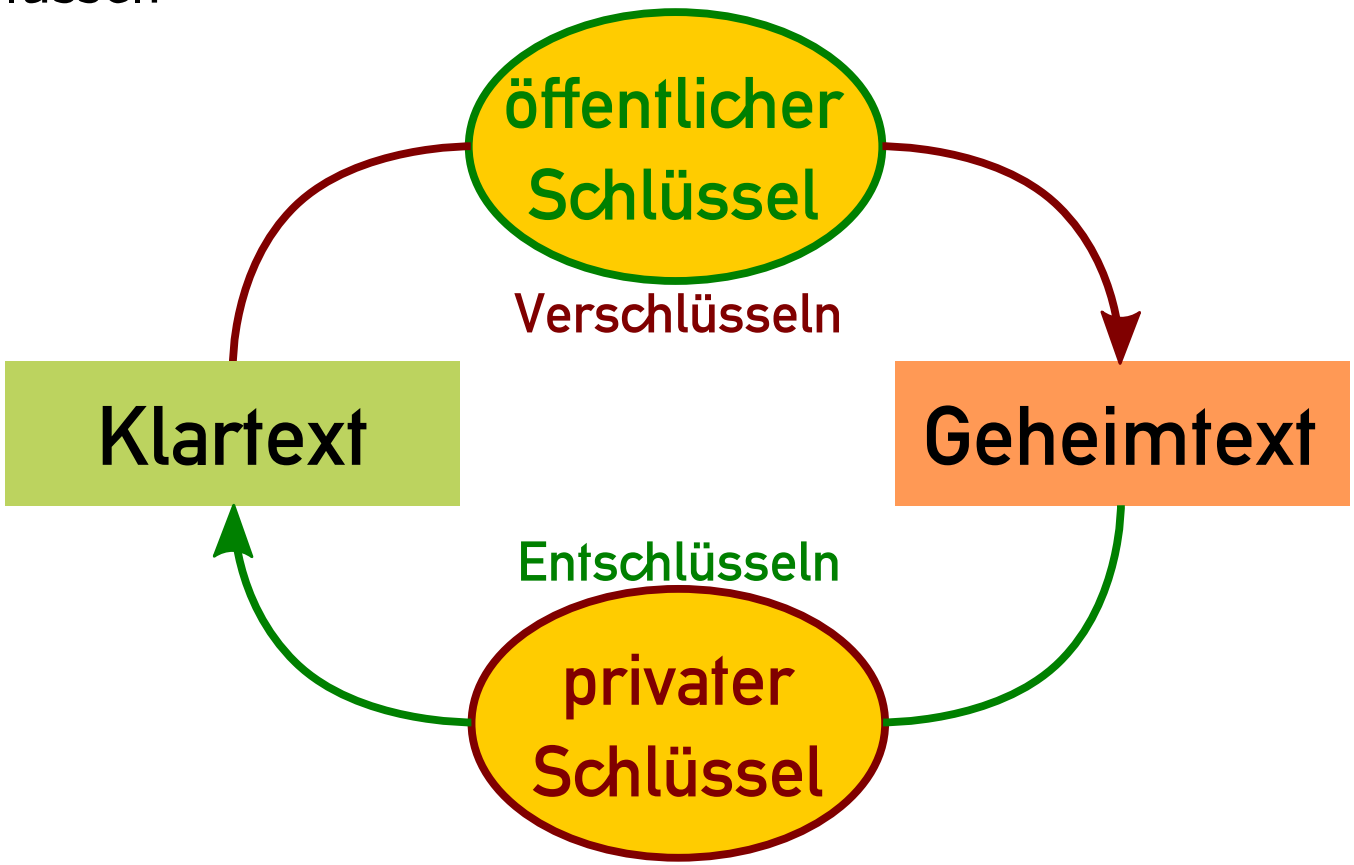


asymmetrische Verfahren – Prinzip (2a)

Die **Verschlüsselung** erfolgt dann mit dem öffentlichem Schlüssel und die **Entschlüsselung** mit dem privatem Schlüssel:

asymmetrische Verfahren – Prinzip (2a)

Die **Verschlüsselung** erfolgt dann mit dem öffentlichem Schlüssel und die **Entschlüsselung** mit dem privatem Schlüssel:

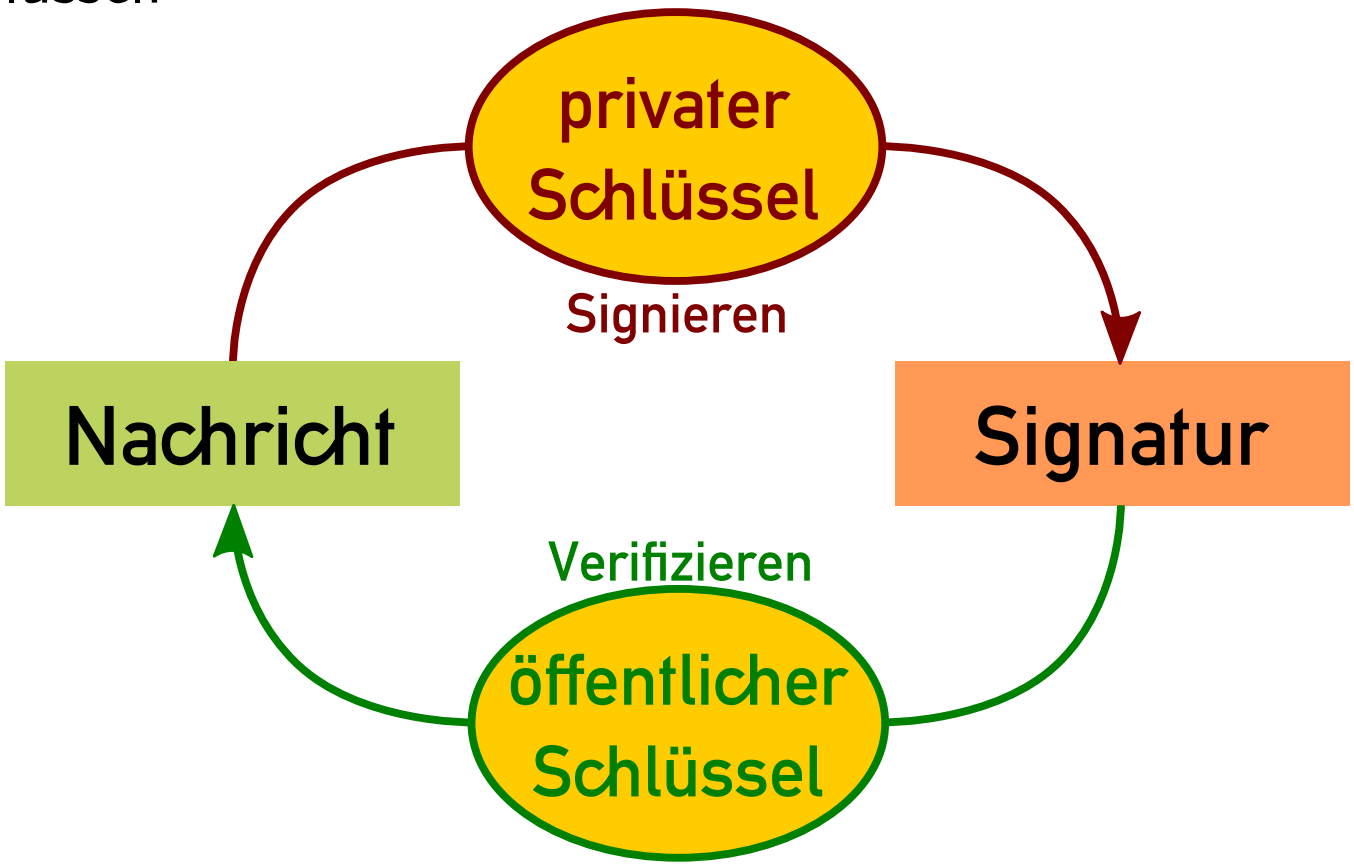


asymmetrische Verfahren – Prinzip (2b)

Das **Signieren** von Nachrichten erfolgt mit dem privaten Schlüssel und die **Verifikation** mit dem öffentlichen Schlüssel:

asymmetrische Verfahren – Prinzip (2b)

Das **Signieren** von Nachrichten erfolgt mit dem privaten Schlüssel und die **Verifikation** mit dem öffentlichen Schlüssel:



Zusammenfassung

symmetrische Verfahren

Zusammenfassung

symmetrische Verfahren

- Die Zeichenvertauschung wird vom Empfänger der verschlüsselten Nachricht Schritt für Schritt rückgängig gemacht.

Zusammenfassung

symmetrische Verfahren

- Die Zeichenvertauschung wird vom Empfänger der verschlüsselten Nachricht Schritt für Schritt rückgängig gemacht.
- Der Empfänger muss den Schlüssel kennen.

Zusammenfassung

symmetrische Verfahren

- Die Zeichenvertauschung wird vom Empfänger der verschlüsselten Nachricht Schritt für Schritt rückgängig gemacht.
- Der Empfänger muss den Schlüssel kennen.

asymmetrische Verfahren

Zusammenfassung

symmetrische Verfahren

- Die Zeichenvertauschung wird vom Empfänger der verschlüsselten Nachricht Schritt für Schritt rückgängig gemacht.
- Der Empfänger muss den Schlüssel kennen.

asymmetrische Verfahren

- Es gibt zwei Schlüssel, einen öffentlichen (public key) und einen privaten (private key).

Zusammenfassung

symmetrische Verfahren

- Die Zeichenvertauschung wird vom Empfänger der verschlüsselten Nachricht Schritt für Schritt rückgängig gemacht.
- Der Empfänger muss den Schlüssel kennen.

asymmetrische Verfahren

- Es gibt zwei Schlüssel, einen öffentlichen (public key) und einen privaten (private key).
- Die Dechiffrierung kann jeweils nur mit dem Gegenstück erfolgen.

Beispiel für eine asymmetrische Verschlüsselung

Beispiel für eine asymmetrische Verschlüsselung

Teil ①: Die Diffie-Hellman-Schlüsselvereinbarung

Beispiel für eine asymmetrische Verschlüsselung

Teil ①: Die Diffie-Hellman-Schlüsselvereinbarung

Zwei Kommunikationspartner (A und B) wollen einen gemeinsamen geheimen Schlüssel über einen unsicheren Kanal vereinbaren, der von einem Dritten (C) abgehört werden kann.

Beispiel für eine asymmetrische Verschlüsselung

Teil ①: Die Diffie-Hellman-Schlüsselvereinbarung

Zwei Kommunikationspartner (A und B) wollen einen gemeinsamen geheimen Schlüssel über einen unsicheren Kanal vereinbaren, der von einem Dritten (C) abgehört werden kann.

Problem: Wie kann der Schlüssel geheim bleiben, wenn die Kommunikation abgehört wird?

Beispiel für eine asymmetrische Verschlüsselung

Teil ①: Die Diffie-Hellman-Schlüsselvereinbarung

Zwei Kommunikationspartner (A und B) wollen einen gemeinsamen geheimen Schlüssel über einen unsicheren Kanal vereinbaren, der von einem Dritten (C) abgehört werden kann.

Problem: Wie kann der Schlüssel geheim bleiben, wenn die Kommunikation abgehört wird?

Lösung: Der Schlüssel wird indirekt mit Hilfe des Diffie-Hellman-Protokolls vereinbart.

Beispiel für eine asymmetrische Verschlüsselung

Teil ①: Die Diffie-Hellman-Schlüsselvereinbarung

Zwei Kommunikationspartner (A und B) wollen einen gemeinsamen geheimen Schlüssel über einen unsicheren Kanal vereinbaren, der von einem Dritten (C) abgehört werden kann.

Problem: Wie kann der Schlüssel geheim bleiben, wenn die Kommunikation abgehört wird?

Lösung: Der Schlüssel wird indirekt mit Hilfe des Diffie-Hellman-Protokolls vereinbart.

➠ Für C ist es zwar theoretisch möglich, den Schlüssel zu ermitteln. Praktisch ist aber der Rechenaufwand so hoch, dass es für C undurchführbar wird.

① Diffie-Hellmann-Schlüsselvereinbarung

① Diffie-Hellmann-Schlüsselvereinbarung

1. A und B tauschen öffentlich (➠ durch C lesbar) eine Primzahl p und eine Zahl g mit $1 < g < p - 1$ aus.

① Diffie-Hellmann-Schlüsselvereinbarung

1. A und B tauschen öffentlich (➠ durch C lesbar) eine Primzahl p und eine Zahl g mit $1 < g < p-1$ aus.
2. A wählt eine Zufallszahl u und berechnet eine Zahl a mit $a = g^u \bmod p$

① Diffie-Hellmann-Schlüsselvereinbarung

1. A und B tauschen öffentlich (➠ durch C lesbar) eine Primzahl p und eine Zahl g mit $1 < g < p-1$ aus.
2. A wählt eine Zufallszahl u und berechnet eine Zahl a mit $a = g^u \bmod p$
3. B wählt eine Zufallszahl v und berechnet eine Zahl b mit $b = g^v \bmod p$

① Diffie-Hellmann-Schlüsselvereinbarung

1. A und B tauschen öffentlich (➠ durch C lesbar) eine Primzahl p und eine Zahl g mit $1 < g < p-1$ aus.
2. A wählt eine Zufallszahl u und berechnet eine Zahl a mit $a = g^u \bmod p$
3. B wählt eine Zufallszahl v und berechnet eine Zahl b mit $b = g^v \bmod p$
4. A und B tauschen die Zahlen a und b öffentlich aus

① Diffie-Hellmann-Schlüsselvereinbarung

1. A und B tauschen öffentlich (➠ durch C lesbar) eine Primzahl p und eine Zahl g mit $1 < g < p-1$ aus.
2. A wählt eine Zufallszahl u und berechnet eine Zahl a mit $a = g^u \bmod p$
3. B wählt eine Zufallszahl v und berechnet eine Zahl b mit $b = g^v \bmod p$
4. A und B tauschen die Zahlen a und b öffentlich aus
5. A berechnet Schlüssel k aus b, der Zufallszahl u und der Primzahl p: $k = b^u \bmod p = g^{v \cdot u} \bmod p$

① Diffie-Hellmann-Schlüsselvereinbarung

1. A und B tauschen öffentlich (➠ durch C lesbar) eine Primzahl p und eine Zahl g mit $1 < g < p-1$ aus.
2. A wählt eine Zufallszahl u und berechnet eine Zahl a mit $a = g^u \bmod p$
3. B wählt eine Zufallszahl v und berechnet eine Zahl b mit $b = g^v \bmod p$
4. A und B tauschen die Zahlen a und b öffentlich aus
5. A berechnet Schlüssel k aus b, der Zufallszahl u und der Primzahl p: $k = b^u \bmod p = g^{v \cdot u} \bmod p$
6. B berechnet Schlüssel k aus a, der Zufallszahl v und der Primzahl p: $k = a^v \bmod p = g^{u \cdot v} \bmod p$

① Diffie-Hellmann-Schlüsselvereinbarung

Die von A und B unabhängig voneinander berechnete Zahl k kann jetzt als gemeinsamer Schlüssel dienen.

① Diffie-Hellmann-Schlüsselvereinbarung

Die von A und B unabhängig voneinander berechnete Zahl k kann jetzt als gemeinsamer Schlüssel dienen.

Wichtige Bedingungen:

① Diffie-Hellmann-Schlüsselvereinbarung

Die von A und B unabhängig voneinander berechnete Zahl k kann jetzt als gemeinsamer Schlüssel dienen.

Wichtige Bedingungen:

Damit C den Schlüssel nicht aus p, g, a und b berechnen kann, müssen die verwendeten Zahlen p und g groß genug sein. Außerdem muss g die Ordnung $p-1$ haben.

① Diffie-Hellmann-Schlüsselvereinbarung

Die von A und B unabhängig voneinander berechnete Zahl k kann jetzt als gemeinsamer Schlüssel dienen.

Wichtige Bedingungen:

Damit C den Schlüssel nicht aus p, g, a und b berechnen kann, müssen die verwendeten Zahlen p und g groß genug sein. Außerdem muss g die Ordnung $p-1$ haben. Dann kann C die zur Schlüsselberechnung ($k = b^u \bmod p$ oder $k = a^v \bmod p$) notwendige Zahl u bzw. v nicht mit vertretbarem Aufwand berechnen (➠ „Problem des diskreten Logarithmus“).

② ElGamal-Verschlüsselung

Das ElGamal-Verschlüsselungsverfahren wurde im Jahr 1985 vom äqyptischen Kryptologen Taher Elgamal (auch Tahir al-Dschamal) entwickelt.

② ElGamal-Verschlüsselung

Das ElGamal-Verschlüsselungsverfahren wurde im Jahr 1985 vom äqyptischen Kryptologen Taher Elgamal (auch Tahir al-Dschamal) entwickelt.
Es handelt sich um eine Public-Key-Verschlüsselung, die auf dem Diffie-Hellman-Schlüsselaustausch aufbaut.

② ElGamal-Verschlüsselung

Das ElGamal-Verschlüsselungsverfahren wurde im Jahr 1985 vom äqyptischen Kryptologen Taher Elgamal (auch Tahir al-Dschamal) entwickelt.
Es handelt sich um eine Public-Key-Verschlüsselung, die auf dem Diffie-Hellman-Schlüsselaustausch aufbaut.

Verfahren (B sendet A eine Nachricht, C hört ab):

② ElGamal-Verschlüsselung

Das ElGamal-Verschlüsselungsverfahren wurde im Jahr 1985 vom äqyptischen Kryptologen Taher Elgamal (auch Tahir al-Dschamal) entwickelt.
Es handelt sich um eine Public-Key-Verschlüsselung, die auf dem Diffie-Hellman-Schlüsselaustausch aufbaut.

Verfahren (B sendet A eine Nachricht, C hört ab):

1. Diffie-Hellman-Schlüsselaustausch (siehe ①) ➠ A und B besitzen geheimen Schlüssel k und die öffentlichen Zahlen p und g. C kennt nur p und g.

② ElGamal-Verschlüsselung

Das ElGamal-Verschlüsselungsverfahren wurde im Jahr 1985 vom äqyptischen Kryptologen Taher Elgamal (auch Tahir al-Dschamal) entwickelt.
Es handelt sich um eine Public-Key-Verschlüsselung, die auf dem Diffie-Hellman-Schlüsselaustausch aufbaut.

Verfahren (B sendet A eine Nachricht, C hört ab):

1. Diffie-Hellman-Schlüsselaustausch (siehe ①) ➠ A und B besitzen geheimen Schlüssel k und die öffentlichen Zahlen p und g. C kennt nur p und g.
2. B verschlüsselt Botschaft m mit: $c = k \cdot m \bmod p$

② ElGamal-Verschlüsselung

Das ElGamal-Verschlüsselungsverfahren wurde im Jahr 1985 vom äqyptischen Kryptologen Taher Elgamal (auch Tahir al-Dschamal) entwickelt.
Es handelt sich um eine Public-Key-Verschlüsselung, die auf dem Diffie-Hellman-Schlüsselaustausch aufbaut.

Verfahren (B sendet A eine Nachricht, C hört ab):

1. Diffie-Hellman-Schlüsselaustausch (siehe ①) ➠ A und B besitzen geheimen Schlüssel k und die öffentlichen Zahlen p und g. C kennt nur p und g.
2. B verschlüsselt Botschaft m mit: $c = k \cdot m \bmod p$
3. Übertragung des Schlüsseltextes c (sichtbar für C)

② ElGamal-Verschlüsselung

Das ElGamal-Verschlüsselungsverfahren wurde im Jahr 1985 vom äqyptischen Kryptologen Taher Elgamal (auch Tahir al-Dschamal) entwickelt.
Es handelt sich um eine Public-Key-Verschlüsselung, die auf dem Diffie-Hellman-Schlüsselaustausch aufbaut.

Verfahren (B sendet A eine Nachricht, C hört ab):

1. Diffie-Hellman-Schlüsselaustausch (siehe ①) ➠ A und B besitzen geheimen Schlüssel k und die öffentlichen Zahlen p und g. C kennt nur p und g.
2. B verschlüsselt Botschaft m mit: $c = k \cdot m \bmod p$
3. Übertragung des Schlüsseltextes c (sichtbar für C)
4. A entschlüsselt c mit: $m = k^{-1} \cdot c \bmod p$

ElGamal-Verschlüsselung – Aufgabe

Testen Sie das ElGamal-Verfahren mit Hilfe folgender Webseite:

- http://www.iti.fh-flensburg.de/lang/krypto/protokolle/elgamal.htm (Abschnitt „Beispiel“)

Hinweis:

Skriptblocker (z. B. NoScript) können die Funktionalität der Webseite beeinträchtigen!

RSA – Aufgabe

Informieren Sie sich über das RSA-Kryptosystem. Erstellen Sie ein übersichtliches PDF-Dokument mit folgenden Schwerpunkten:

- Prinzip des RSA-Verfahrens
- Schlüsselerzeugung (Überblick)
- Ver- und Entschlüsseln von Nachrichten
- Signieren von Nachrichten
- Sicherheit des RSA-Verfahrens
- Anwendungsgebiete

Drucken Sie das PDF-Dokument aus und stellen Sie es im CMS des WGK Informatik für die Mitschüler bereit.

Steganographie

Finde den Unterschied ...

- Größe: 6903632 Byte
- Originalbild

- Größe: 7144428 Byte
- enthält eine verborgene Information

Aufgaben zur Steganographie

Im Verzeichnis `~/+all/Steganographie` befinden Sich die Dateien `Originalbild.jpg`, `Geheimbild.jpg` und `Stegmusik.wav`. Auf den Computern ist das Konsolenprogramm `steghide` installiert.

1. Machen Sie sich mit der Funktionsweise von `steghide` vertraut (Konsole: `man steghide` ↵ oder `steghide` ↵ – ohne Argumente).
2. Extrahieren Sie die in `Geheimbild.jpg` und `Stegmusik.wav` verborgenen Dateien. Das Passwort lautet „`Steganographie`“.
3. Informieren Sie sich anhand der extrahierten Dateien über Steganographie.
4. Erzeugen Sie mit `steghide` eigene Steganogramme (➠ `~/+all/Steganographie/Beispiele`).