

Grundlagen der Datensicherheit für Lehrerinnen und Lehrer

Dr. Lutz Hellmig

Universität Rostock

Didaktik der Informatik am Institut für Informatik

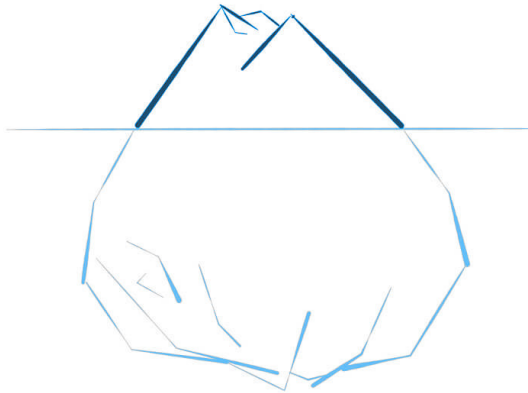
<http://pidi.informatik.uni-rostock.de>

A-Level-Grades in Großbritannien



<https://www.bbc.com/news/education-53787203>

Digitalisierung: Der Medienbildung-Informatik-Eisberg



Datensicherheit und Öffentlichkeit

Datensicherheit

Öffentlichkeit und Geheimhaltung

Daten speichern

Daten gegen Verlust schützen

Symmetrische Verschlüsselung

Datenübertragung

Asymmetrische Verschlüsselung

Integrität und Authentizität von Nachrichten

Datensicherheit

ist ein technisches Ziel.

- ▶ Bewahrung von Daten jeglicher Art vor Manipulation, Verlust, unberechtigter Kenntnisnahme und anderen Bedrohungen
- ▶ Die Rechtmäßigkeit der Datenerhebung, -speicherung und -verarbeitung ist zunächst irrelevant.

Schutzziele der Informationssicherheit

Daten

- ▶ Vertraulichkeit
- ▶ Integrität
- ▶ Verfügbarkeit

Urheberschaft

- ▶ Authentizität
- ▶ Verbindlichkeit/Nichtabstreitbarkeit
- ▶ Zurechenbarkeit $\Leftrightarrow$ Anonymität

Schutzziele der Informationssicherheit

Daten

- ▶ Vertraulichkeit
- ▶ Integrität
- ▶ Verfügbarkeit

Urheberschaft

- ▶ Authentizität
- ▶ Verbindlichkeit/Nichtabstreitbarkeit
- ▶ Zurechenbarkeit $\Leftrightarrow$ Anonymität

Datenschutz

- ▶ Gewährung der Persönlichkeitsrechte bei der Erhebung, Speicherung, Verarbeitung und Verbreitung von Daten.
- ▶ Datensicherheit ist eine der Voraussetzungen hierfür.

Datensicherheit in der Schule – Konkretisierung¹

- ▶ Sicherung der Geräte gegen unbefugten Zugriff
- ▶ Automatische Aktualisierung des Betriebssystems
- ▶ Nutzung einer sich automatisch aktualisierenden Firewall/Antivirensoftware
- ▶ Verschlüsselung auf privatem Endgerät und mobilen Datenträgern
- ▶ Nutzung einer Transport- und ggf. einer Dateiverschlüsselung beim Versand
- ▶ Verschlüsselung des privaten WLAN
- ▶ Keine Nutzung privater Cloudspeicher von Drittanbietern für die Speicherung personenbezogener Daten

¹Schuldatenschutzverordnung (SchulDSVO M-V) 2020 

Fragen zur Datensicherheit

- ▶ Welche Daten müssen gesichert werden?
- ▶ Welchen Gefahren sind diese Daten ausgesetzt?
- ▶ Welche Maßnahmen dienen der Datensicherheit?

Datensicherheit und Öffentlichkeit

Datensicherheit

Öffentlichkeit und Geheimhaltung

Daten speichern

Daten gegen Verlust schützen

Symmetrische Verschlüsselung

Datenübertragung

Asymmetrische Verschlüsselung

Integrität und Authentizität von Nachrichten

Anforderungen an sichere Kryptosysteme²

Vertraulichkeit der Inhalte bei

- ▶ öffentlichen Ressourcen und Kommunikationswegen
- ▶ öffentlich bekanntem Verfahren

aber

- ▶ geheimem Schlüssel.

Daten, deren „Sicherheit“ auf der Geheimhaltung eines Verfahrens beruht, sind nicht sicher.

²Prinzip von Kerkhoffs (1883)

Open Source Software

Die Barmer möchte eine elektronische Patientenakte einführen.

BARMER

Hauptverwaltung

Ausschreibung

0014-ePatienten-2019

Justizariat

Vergabestelle

§ 28 Verwendung von Open Source Software

1. Die Verwendung von Open Source Software ist grundsätzlich nicht erlaubt. Sollte im Laufe der Entwicklung die Verwendung von Open Source Software zwingend geboten erscheinen, hat der Auftragnehmer dies dem Auftraggeber in Textform anzuzeigen, unter Angabe der relevanten Lizenzbestimmungen, unter welche die Open Source Software fällt. Der Auftraggeber wird sodann über die Verwendung der Open Source Software innerhalb angemessener Frist nach freiem Ermessen entscheiden und dem Auftragnehmer seine Entscheidung in Textform mitteilen. Falls

Lizenzmodelle für Software

proprietär Quellcode ist nicht offen.
Gestattet ist die Nutzung,
nicht aber die Modifikation der Software.

Open Source ist kostenfrei.
Der Code ist öffentlich.
Jeder kann sich an der Weiterentwicklung beteiligen.

Open Source Programme

Betriebssystem Linux

Office-Paket Libreoffice
Open Office

Browser Firefox

E-Mail-Client Thunderbird

Ver- und Entpacken 7-Zip

Verschlüsseln Veracrypt

Bildbearbeitung Gimp

Bildbetrachter Inkscape

DTP Scribus

Medienwiedergabe VLC-Player

Audiobearbeitung Audacity

Videobearbeitung OBS Studio

Cloud Nextcloud

Datensicherheit und Öffentlichkeit

Datensicherheit

Öffentlichkeit und Geheimhaltung

Daten speichern

Daten gegen Verlust schützen

Symmetrische Verschlüsselung

Datenübertragung

Asymmetrische Verschlüsselung

Integrität und Authentizität von Nachrichten

Techniken

- ▶ Welche Möglichkeiten nutzen Sie, um Daten gegen Verlust zu schützen?
- ▶ Wie schätzen Sie die Sicherheit dieser Methoden ein?
- ▶ Welche Nachteile haben diese Methoden?

Manuelle Versionskontrolle

Schlecht

Dokument 02-05-2018.txt
Dokument 02-07-2021.txt
Dokument 04-04-2020.txt
Dokument 05-03-2018.txt
Dokument 08-06-2018.txt
Dokument 08-07-2019.txt
Dokument 11-05-2018.txt
Dokument 17-05-2019.txt
Dokument 24-10-2018.txt
Dokument 26-03-2021.txt

Gut

Dokument 2018-03-05.txt
Dokument 2018-05-02.txt
Dokument 2018-05-11.txt
Dokument 2018-06-08.txt
Dokument 2018-10-24.txt
Dokument 2019-05-17.txt
Dokument 2019-07-08.txt
Dokument 2020-04-04.txt
Dokument 2021-03-26.txt
Dokument 2021-07-02.txt

Sehr gut

Dokument 2021-07-02.txt
Dokument 2021-03-26.txt
Dokument 2020-04-04.txt
Dokument 2019-07-08.txt
Dokument 2019-05-17.txt
Dokument 2018-10-24.txt
Dokument 2018-06-08.txt
Dokument 2018-05-11.txt
Dokument 2018-05-02.txt
Dokument 2018-03-05.txt

Manuelle Versionskontrolle

Schlecht

Dokument 02-05-2018.txt
 Dokument 02-07-2021.txt
 Dokument 04-04-2020.txt
 Dokument 05-03-2018.txt
 Dokument 08-06-2018.txt
 Dokument 08-07-2019.txt
 Dokument 11-05-2018.txt
 Dokument 17-05-2019.txt
 Dokument 24-10-2018.txt
 Dokument 26-03-2021.txt

Gut

Dokument 2018-03-05.txt
 Dokument 2018-05-02.txt
 Dokument 2018-05-11.txt
 Dokument 2018-06-08.txt
 Dokument 2018-10-24.txt
 Dokument 2019-05-17.txt
 Dokument 2019-07-08.txt
 Dokument 2020-04-04.txt
 Dokument 2021-03-26.txt
 Dokument 2021-07-02.txt

Sehr gut

Dokument 2021-07-02.txt
 Dokument 2021-03-26.txt
 Dokument 2020-04-04.txt
 Dokument 2019-07-08.txt
 Dokument 2019-05-17.txt
 Dokument 2018-10-24.txt
 Dokument 2018-06-08.txt
 Dokument 2018-05-11.txt
 Dokument 2018-05-02.txt
 Dokument 2018-03-05.txt

Manuelle Versionskontrolle

Schlecht

Dokument 02-05-2018.txt
Dokument 02-07-2021.txt
Dokument 04-04-2020.txt
Dokument 05-03-2018.txt
Dokument 08-06-2018.txt
Dokument 08-07-2019.txt
Dokument 11-05-2018.txt
Dokument 17-05-2019.txt
Dokument 24-10-2018.txt
Dokument 26-03-2021.txt

Gut

Dokument 2018-03-05.txt
Dokument 2018-05-02.txt
Dokument 2018-05-11.txt
Dokument 2018-06-08.txt
Dokument 2018-10-24.txt
Dokument 2019-05-17.txt
Dokument 2019-07-08.txt
Dokument 2020-04-04.txt
Dokument 2021-03-26.txt
Dokument 2021-07-02.txt

Sehr gut

Dokument 2021-07-02.txt
Dokument 2021-03-26.txt
Dokument 2020-04-04.txt
Dokument 2019-07-08.txt
Dokument 2019-05-17.txt
Dokument 2018-10-24.txt
Dokument 2018-06-08.txt
Dokument 2018-05-11.txt
Dokument 2018-05-02.txt
Dokument 2018-03-05.txt

Automatische Versionskontrolle lokal

Dateiversionsverlauf

← → ↕ ↶ ⌂ << System und Sicherheit > Dateiversionsverlauf ↕ ↻

Startseite der Systemsteuerung

Persönliche Dateien wiederherstellen

Laufwerk auswählen

Ordner ausschließen

Erweiterte Einstellungen

Siehe auch

Wiederherstellung

Systemabbildsicherung

Bewahren Sie eine Kopie Ihrer Dateien auf

Mit dem Dateiversionsverlauf werden Kopien der Dateien gespeichert, sodass Sie sie wiederherstellen können, falls sie verloren gehen oder beschädigt werden.

i Es wurde kein verwendbares Laufwerk gefunden. Es wird empfohlen, ein externes Laufwerk für den Dateiversionsverlauf zu verwenden. Verbinden Sie ein Laufwerk, und aktualisieren Sie diese Seite, oder verwenden Sie eine Netzwerkadresse.

[Netzwerkadresse auswählen](#)

Dateiversionsverlauf ist ausgeschaltet

Dateien kopieren von: Bibliotheken, Desktop, Kontakte und Favoriten

Dateien kopieren nach: *Es wurden keine verwendbaren Laufwerke gefunden.*

Einschalten

Automatische Versionskontrolle in der Cloud

testtext.odt Versionsverlauf

Heute

	testtext.odt 10:19	Bearbeitet von Lutz Hellmig Desktop	23,08 KB	Aktuelle Version
	testtext.odt 10:19	Bearbeitet von Lutz Hellmig Desktop	16,71 KB	Wiederherstellen
	Lutz Hellmig hat die Datei von OpenDocument Text (neu).odt in testtext.odt umbenannt. 10:18 • Desktop		7,74 KB	
	OpenDocument Text (neu).odt 10:18	Hinzugefügt von Lutz Hellmig Desktop	7,74 KB	

Wiederherstellen von Dateien in der Cloud

Gelöschte Dateien

Name

Gelöscht

Eine beliebige Datei wiederherstellen, die vor maximal 30 Tag gelöscht wurde

[Gelöschte Dateien wiederherstellen](#)

Suchen Sie etwas anderes?

[Eine ältere Version eines Ordners](#)[Eine ältere Version einer Datei](#)

testtext.odt

Test

vor 5 Sek.



Sie haben 30 Tage lang Zeit, eine gelöschte Datei wiederherzustellen.

Datensicherheit und Öffentlichkeit

Datensicherheit

Öffentlichkeit und Geheimhaltung

Daten speichern

Daten gegen Verlust schützen

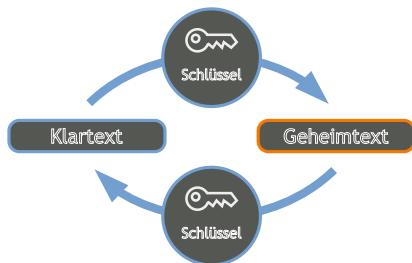
Symmetrische Verschlüsselung

Datenübertragung

Asymmetrische Verschlüsselung

Integrität und Authentizität von Nachrichten

Symmetrische Kryptosysteme

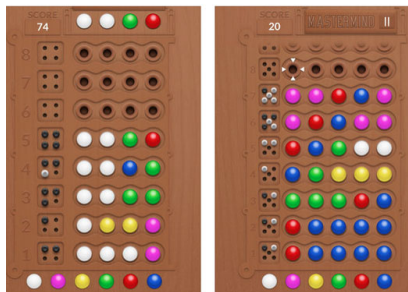


- ▶ Ein Schlüssel (= Passwort) zum Ver- und Entschlüsseln
- ▶ Schlüssel nicht universell nutzbar.
- ▶ Beispiele:
Caesar, Enigma, AES

Schlüssellänge und Sicherheit

Die Sicherheit eines Schlüssels (Passwortes) ist abhängig

- ▶ von der Länge
- ▶ vom Zeichenvorrat



Schlüssellänge und Sicherheit

Werden die Zeichen des Passwortes binär (0/1) codiert, verbleibt die Schlüssellänge als einzig relevante Größe.

- ▶ Beispiel AES-Verfahren: 192 und 256 Bit gelten derzeit als sicher.

Verschlüsselung beim Speichern von Dokumenten

Dateiname:

Dateityp:

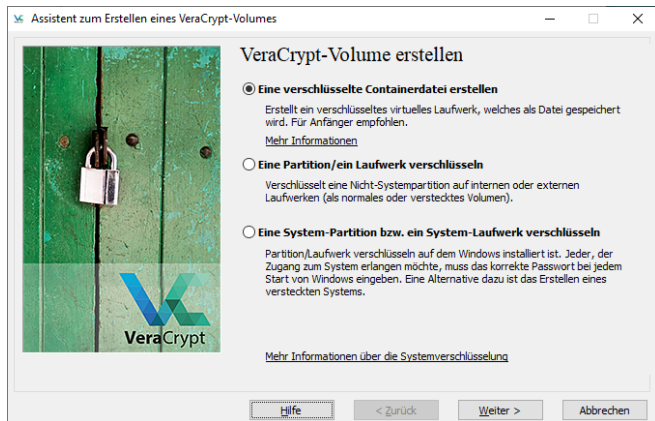
☒ Automatische
Dateiendung

☐ Mit Kennwort
speichern

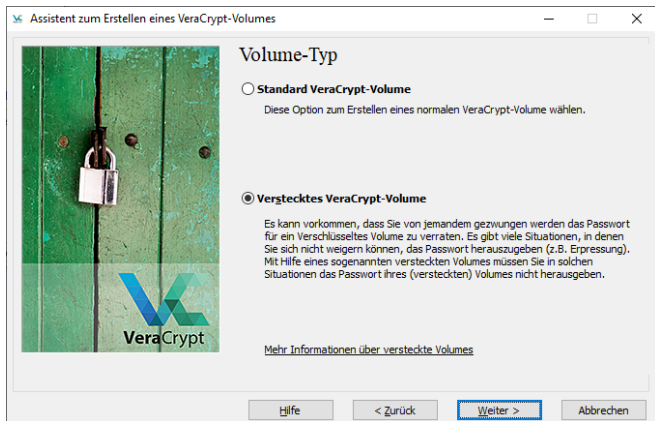
☐ Mit GPG-Schlüssel
verschlüsseln

☐ Filtereinstellungen
bearbeiten

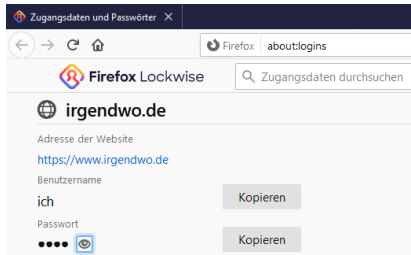
Verschlüsselung von Datenträgern mit Veracrypt



Glaubhafte Abstreitbarkeit mit Veracrypt



Warum man Passwörter nicht im Browser speichern sollte...



Passwortmanager (z. B. Kee Pass 2)



Bild von kalhh auf Pixabay (Pixabay Licence)

Datensicherheit und Öffentlichkeit

Datensicherheit

Öffentlichkeit und Geheimhaltung

Daten speichern

Daten gegen Verlust schützen

Symmetrische Verschlüsselung

Datenübertragung

Asymmetrische Verschlüsselung

Integrität und Authentizität von Nachrichten

Das Hauptproblem der symmetrischen Verschlüsselung

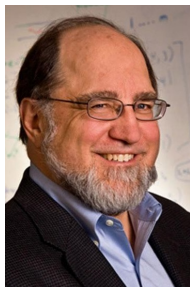


https://commons.wikimedia.org/wiki/File:JWPcon_2016_Schlüsselübergabe.jpg CC BY-SA 3.0

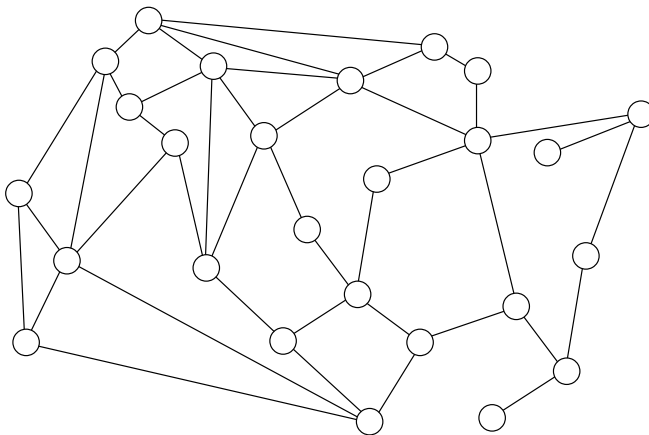
Rivest–Shamir–Adleman

RSA-Kryptosystem (1977):

Schlüsselpaar aus privatem und öffentlichem Schlüssel

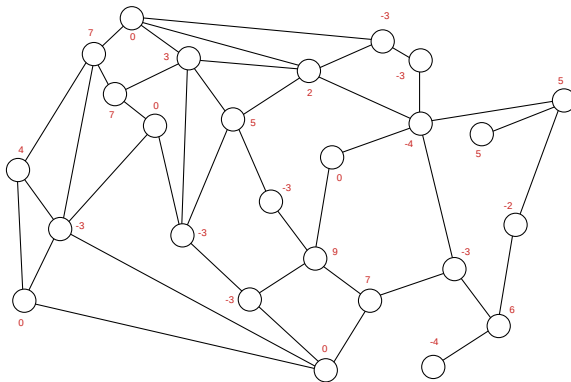


Prinzip der asymmetrischen Verschlüsselung



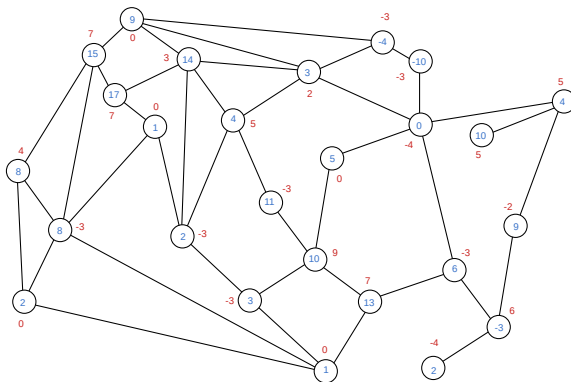
Asymmetrische Verschlüsselung einer Zahl

$$29 = 0 + -3 + -3 + 5 + 9 + 4 + 5 + 7 + -4 + -3 + 7 + -3 + 0 \\ + -3 + -3 + 0 + 6 + -3 + 7 + 0 + -4 + 5 + 2 + -2 + 3 + 0$$



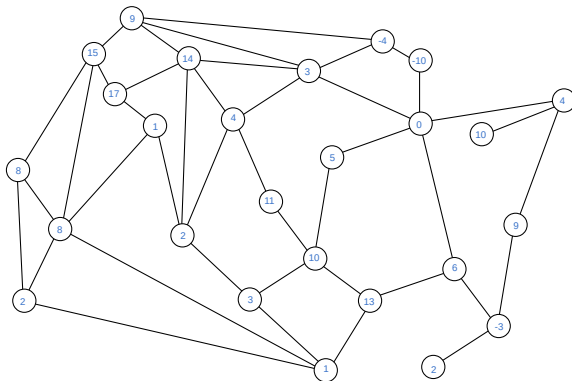
Asymmetrische Verschlüsselung einer Zahl

$$29 = 0 + -3 + -3 + 5 + 9 + 4 + 5 + 7 + -4 + -3 + 7 + -3 + 0 \\ + -3 + -3 + 0 + 6 + -3 + 7 + 0 + -4 + 5 + 2 + -2 + 3 + 0$$



Asymmetrische Verschlüsselung einer Zahl

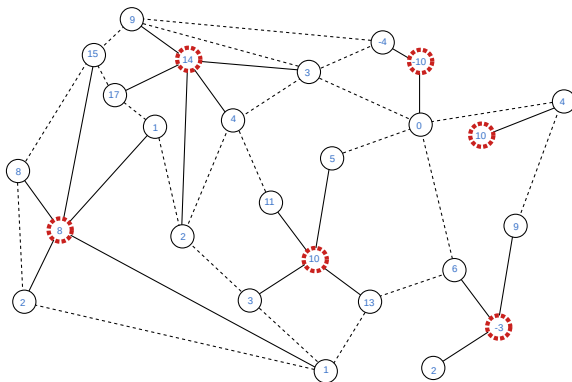
29 = ?



The graph consists of 20 nodes, each represented by a light blue circle with a black border and a black number inside. The nodes are labeled with the following values: 9, 15, 17, 14, 1, 4, 3, -4, -10, 0, 10, 4, 8, 8, 2, 11, 5, 10, 3, 13, 6, 9, -3, 2, 1. The edges are categorized into two types: solid black lines and dashed grey lines. A specific path is highlighted with a red line connecting nodes 14 and 3.

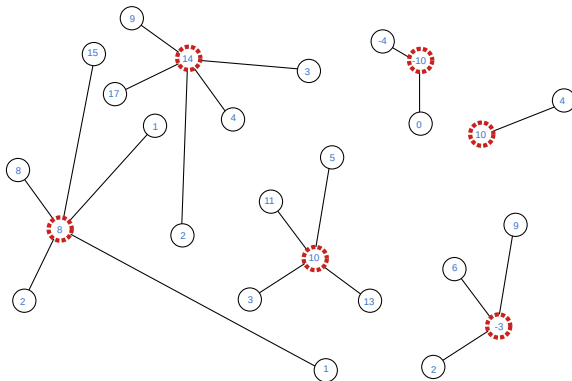
Asymmetrische Verschlüsselung einer Zahl

29 = ?



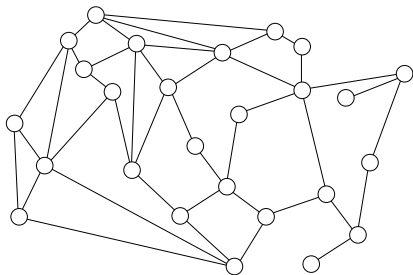
Asymmetrische Verschlüsselung einer Zahl

$$29 = 8 + 14 + 10 - 10 + 10 - 3$$

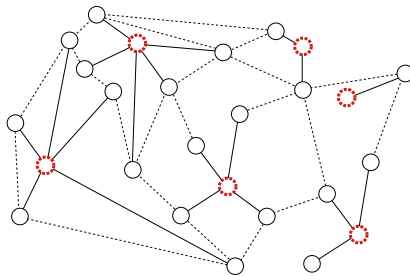


Schlüsselpaar der asymmetrischen Verschlüsselung

Öffentlicher Schlüssel



Privater Schlüssel



Ein-Weg-Funktionen



Zerlegung in Primfaktoren – eine Einweg-Funktion

$$\begin{array}{r} 4286536187 \\ \times 2021031973 \\ \hline \end{array}$$

Zerlegung in Primfaktoren – eine Einweg-Funktion

$$\begin{array}{r} 4286536187 \\ \times 2021031973 \\ \hline 8663226687348506951 \end{array}$$

Zerlegung in Primfaktoren – eine Einweg-Funktion

$$\begin{array}{r}
 4286536187 \\
 \times 2021031973 \\
 \hline
 8663226687348506951
 \end{array}$$

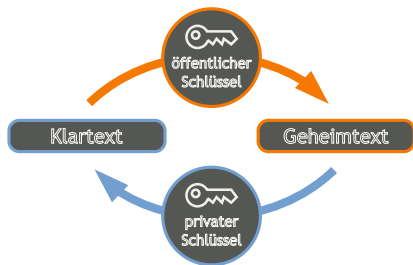
$$\begin{array}{r}
 \hline
 7529938666291482431
 \end{array}$$

Zerlegung in Primfaktoren – eine Einweg-Funktion

$$\begin{array}{r}
 4286536187 \\
 \times 2021031973 \\
 \hline
 8663226687348506951
 \end{array}$$

$$\begin{array}{r}
 3133098593 \\
 \times 2403351967 \\
 \hline
 7529938666291482431
 \end{array}$$

Asymmetrische Kryptosysteme



- ▶ Erzeugung eines Paares von öffentlichem und geheimem Schlüssel per *Einwegfunktion*
- ▶ Ver- und Entschlüsselung zeitaufwendiger als bei symmetrischen Verfahren
- ▶ Beispiel:
RSA (1977)
- ▶ Passwortgeschützte, verschlüsselte Speicherung des privaten Schlüssels.

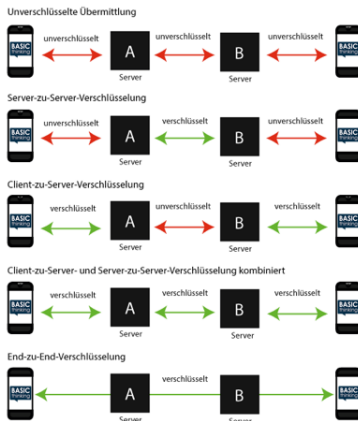
Verschlüsselte E-Mails

- ▶ Verwendung eines E-Mail-Clients (z. B. Thunderbird)
- ▶ Schlüsselverwaltung
 - ▶ Verschlüsselung mit dem öffentlichen Schlüssel des *Empfängers*
 - ▶ Entschlüsselung mit privatem Schlüssel des *Empfängers*

Hybride Kryptosysteme

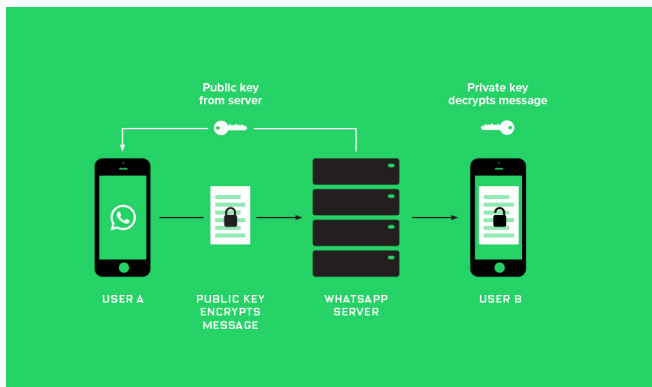
1. Schlüsseltausch mit asymmetrischer Verschlüsselung
2. Nachrichtenübertragung mit symmetrischer Verschlüsselung

Ende-zu-Ende-Verschlüsselung



<https://www.basichthinking.de/blog/wp-content/uploads/2016/04/serverclient.png>

Ende-zu-Ende-Verschlüsselung



<https://t3n.de/news/wp-content/uploads/2016/04/Whatsapp-ende-zu-ende-verschluesselung.jpg>

Datensicherheit und Öffentlichkeit

Datensicherheit

Öffentlichkeit und Geheimhaltung

Daten speichern

Daten gegen Verlust schützen

Symmetrische Verschlüsselung

Datenübertragung

Asymmetrische Verschlüsselung

Integrität und Authentizität von Nachrichten

Finde einen Unterschied! Welches Bild wurde gefälscht?



https://commons.wikimedia.org/wiki/File:00_3465_Mecklenburgische_Bäderbahn_Molli.jpg
CC-BY-SA-4.0

Fehlererkennung durch Prüfbits, Prüfziffern, Prüfsummen

ISBN 978-3-548-37623-**3**

Personalausweis T22000129**3**

EAN



IBAN DE **26** 1300 0000 0014 0015 18

Prüfsummen entstehen aus *gewichteten Quersummen* oder anderen
→ Streuwertfunktionen (Kleine Änderung – große Wirkung).

Digitale Signaturen – Schutz gegen Veränderung

Signatur erzeugen

1. Hashwert („Fingerabdruck“) der Nachricht bilden
2. mit privatem Schlüssel des Absenders verschlüsseln

- ▶ Da die Prüfung mit dem öffentlichem Schlüssel des Absenders erfolgt, kann jeder die Echtheit der Nachricht prüfen.
- ▶ Vertraulichkeit ist nicht gegeben.

Signatur prüfen

1. Hashwert mit öffentlichem Schlüssel des Absenders entschlüsseln
2. Vergleich mit eigener Berechnung des Hash-Werts.

Digitale Signaturen – Schutz gegen Veränderung

Signatur erzeugen

1. Hashwert („Fingerabdruck“) der Nachricht bilden
2. mit privatem Schlüssel des Absenders verschlüsseln

Signatur prüfen

1. Hashwert mit öffentlichem Schlüssel des Absenders entschlüsseln
2. Vergleich mit eigener Berechnung des Hash-Werts.

- ▶ Da die Prüfung mit dem öffentlichem Schlüssel des Absenders erfolgt, kann jeder die Echtheit der Nachricht prüfen.
- ▶ Vertraulichkeit ist nicht gegeben.

Digitale Signaturen – Schutz gegen Veränderung

Signatur erzeugen

1. Hashwert („Fingerabdruck“) der Nachricht bilden
2. mit privatem Schlüssel des Absenders verschlüsseln

- ▶ Da die Prüfung mit dem öffentlichem Schlüssel des Absenders erfolgt, kann jeder die Echtheit der Nachricht prüfen.
- ▶ Vertraulichkeit ist nicht gegeben.

Signatur prüfen

1. Hashwert mit öffentlichem Schlüssel des Absenders entschlüsseln
2. Vergleich mit eigener Berechnung des Hash-Werts.

Digitale Signaturen – Schutz gegen Veränderung

Signatur erzeugen

1. Hashwert („Fingerabdruck“) der Nachricht bilden
2. mit privatem Schlüssel des Absenders verschlüsseln

- ▶ Da die Prüfung mit dem öffentlichem Schlüssel des Absenders erfolgt, kann jeder die Echtheit der Nachricht prüfen.
- ▶ Vertraulichkeit ist nicht gegeben.

Signatur prüfen

1. Hashwert mit öffentlichem Schlüssel des Absenders entschlüsseln
2. Vergleich mit eigener Berechnung des Hash-Werts.

Zertifikate

Authentifizierung: Woher weiß ich, dass der öffentliche Schlüssel wirklich zu der genannten Person gehört?



- ▶ Einmalige persönliche Identifizierung z. B. durch PostIdent
- ▶ Gegenseitige Bewertung der Authentizität (Pretty Good Privacy)

Verschlüsselte Kommunikation mit zertifizierten Anbietern



Datensicherheit in der Schule³

- ▶ Sicherung der Geräte gegen unbefugten Zugriff
- ▶ Automatische Aktualisierung des Betriebssystems
- ▶ Nutzung einer sich automatisch aktualisierenden Firewall/Antivirensoftware
- ▶ Verschlüsselung auf privatem Endgerät und mobilen Datenträgern
- ▶ Nutzung einer Transport- und ggf. einer Dateiverschlüsselung beim Versand
- ▶ Verschlüsselung des privaten WLAN
- ▶ Keine Nutzung privater Cloudspeicher von Drittanbietern für die Speicherung personenbezogener Daten

³Schuldatenschutzverordnung (SchulDSVO M-V) 2020 

Datensicherheit in der Schule³

- ▶ Sicherung der Geräte gegen unbefugten Zugriff
- ▶ Automatische Aktualisierung des Betriebssystems
- ▶ Nutzung einer sich automatisch aktualisierenden Firewall/Antivirensoftware
- ▶ Verschlüsselung auf privatem Endgerät und mobilen Datenträgern
- ▶ Nutzung einer Transport- und ggf. einer Dateiverschlüsselung beim Versand
- ▶ Verschlüsselung des privaten WLAN
- ▶ Keine Nutzung privater Cloudspeicher von Drittanbietern für die Speicherung personenbezogener Daten

³Schuldatenschutzverordnung (SchulDSVO M-V) 2020

Datensicherheit in der Schule³

- ▶ Sicherung der Geräte gegen unbefugten Zugriff
- ▶ Automatische Aktualisierung des Betriebssystems
- ▶ Nutzung einer sich automatisch aktualisierenden Firewall/Antivirensoftware
- ▶ Verschlüsselung auf privatem Endgerät und mobilen Datenträgern
- ▶ Nutzung einer Transport- und ggf. einer Dateiverschlüsselung beim Versand
- ▶ Verschlüsselung des privaten WLAN
- ▶ Keine Nutzung privater Cloudspeicher von Drittanbietern für die Speicherung personenbezogener Daten

³Schuldatenschutzverordnung (SchulDSVO M-V) 2020

Datensicherheit in der Schule³

- ▶ Sicherung der Geräte gegen unbefugten Zugriff
- ▶ Automatische Aktualisierung des Betriebssystems
- ▶ Nutzung einer sich automatisch aktualisierenden Firewall/Antivirensoftware
- ▶ Verschlüsselung auf privatem Endgerät und mobilen Datenträgern
- ▶ Nutzung einer Transport- und ggf. einer Dateiverschlüsselung beim Versand
- ▶ Verschlüsselung des privaten WLAN
- ▶ Keine Nutzung privater Cloudspeicher von Drittanbietern für die Speicherung personenbezogener Daten

³Schuldatenschutzverordnung (SchulDSVO M-V) 2020 

Datensicherheit in der Schule³

- ▶ Sicherung der Geräte gegen unbefugten Zugriff
- ▶ Automatische Aktualisierung des Betriebssystems
- ▶ Nutzung einer sich automatisch aktualisierenden Firewall/Antivirensoftware
- ▶ Verschlüsselung auf privatem Endgerät und mobilen Datenträgern
- ▶ Nutzung einer Transport- und ggf. einer Dateiverschlüsselung beim Versand
- ▶ Verschlüsselung des privaten WLAN
- ▶ Keine Nutzung privater Cloudspeicher von Drittanbietern für die Speicherung personenbezogener Daten

³Schuldatenschutzverordnung (SchulDSVO M-V) 2020 

Datensicherheit in der Schule³

- ▶ Sicherung der Geräte gegen unbefugten Zugriff
- ▶ Automatische Aktualisierung des Betriebssystems
- ▶ Nutzung einer sich automatisch aktualisierenden Firewall/Antivirensoftware
- ▶ Verschlüsselung auf privatem Endgerät und mobilen Datenträgern
- ▶ Nutzung einer Transport- und ggf. einer Dateiverschlüsselung beim Versand
- ▶ Verschlüsselung des privaten WLAN
- ▶ Keine Nutzung privater Cloudspeicher von Drittanbietern für die Speicherung personenbezogener Daten

³Schuldatenschutzverordnung (SchulDSVO M-V) 2020 

Datensicherheit in der Schule³

- ▶ Sicherung der Geräte gegen unbefugten Zugriff
- ▶ Automatische Aktualisierung des Betriebssystems
- ▶ Nutzung einer sich automatisch aktualisierenden Firewall/Antivirensoftware
- ▶ Verschlüsselung auf privatem Endgerät und mobilen Datenträgern
- ▶ Nutzung einer Transport- und ggf. einer Dateiverschlüsselung beim Versand
- ▶ Verschlüsselung des privaten WLAN
- ▶ Keine Nutzung privater Cloudspeicher von Drittanbietern für die Speicherung personenbezogener Daten

³Schuldatenschutzverordnung (SchulDSVO M-V) 2020 

Haben Sie weitere

- ▶ Fragen
- ▶ Anregungen
- ▶ Rückmeldungen?