Wirtschaftsinformatik 1

Informationssicherheit

Prof. Dr. Christian Bockermann, Prof. Dr. Volker Klingspor

Hochschule Bochum

Wintersemester 2025/2026

Inhalt

Motiviation

Sneaker Shop

Hochschule Bochum
Bochum University
of Applied Sciences

Warenkorb: 0 Artikel, 0,00 €

Kategorien

- child
- infant
- men
- preschool
- toddler
- women
- youth

Nike | men

Nike SB Dunk Low April Skateboards

Preis: 186,00 €

adidas | men

Pharrell x NMD_S1 Mahbs 'Earth Strata'

Preis: 300,00 €

Jordan | youth

Air Jordan 1 Mid SS GS 'Championships'

Preis: 120,00 €

Jordan | infant

Air Jordan 1 Mid SS TD 'Championships'

Preis: 149,00 €

Jordan | men

Jordan 8 Retro Winterized Gunsmoke

Preis: 238,00 €

adidas | men

Pharrell x NMD_S1 Mahbs 'Pink'

Preis: 400,00 €

Jordan | youth

Air Jordan 1 Mid SS PS 'Championships'

Preis: 183,00 €

Jordan | child

Jordan 8 Retro Winterized Gunsmoke (GS)

Preis: 226,00 €

Sneaker Shop

Hochschule Bochum
Bochum University
of Applied Sciences

Warenkorb: 0 Artikel, 0,00 €

Kategorien

- child
- infant
- men
- preschool
- toddler
- women
- youth

Nike | men

Nike SB Dunk Low April Skateboards

Preis: 186,00 €

adidas | men

Pharrell x NMD_S1 Mahbs 'Earth Strata'

Preis: 300,00 €

Jordan | youth

Air Jordan 1 Mid SS GS 'Championships'

Preis: 120,00 €

Jordan | infant

Air Jordan 1 Mid SS TD 'Championships'

Preis: 149,00 €

Jordan | men

Jordan 8 Retro Winterized Gunsmoke

Preis: 238,00 €

adidas | men

Pharrell x NMD_S1 Mahbs 'Pink'

Preis: 400,00 €

Jordan | youth

Air Jordan 1 Mid SS PS 'Championships'

Preis: 183,00 €

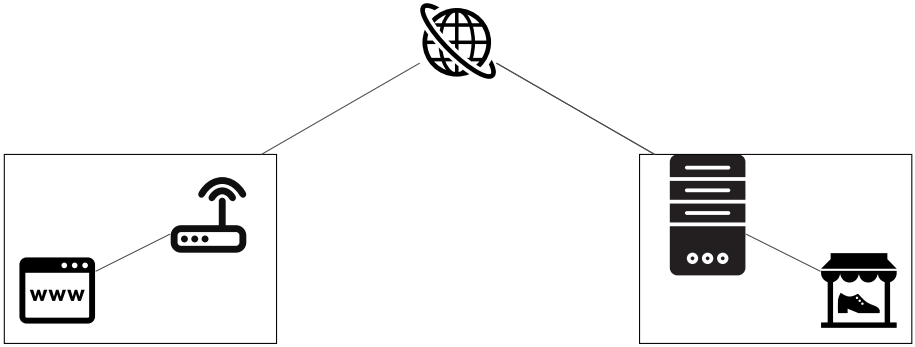
Jordan | child

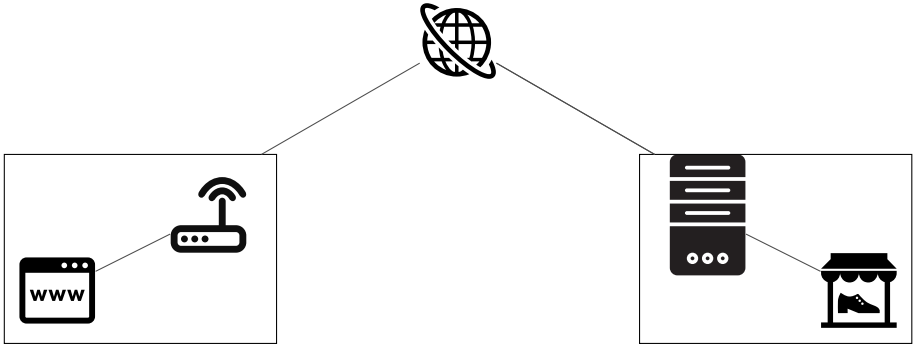
Jordan 8 Retro Winterized Gunsmoke (GS)

Preis: 226,00 €

Wie können wir Informationen sicher übertragen?

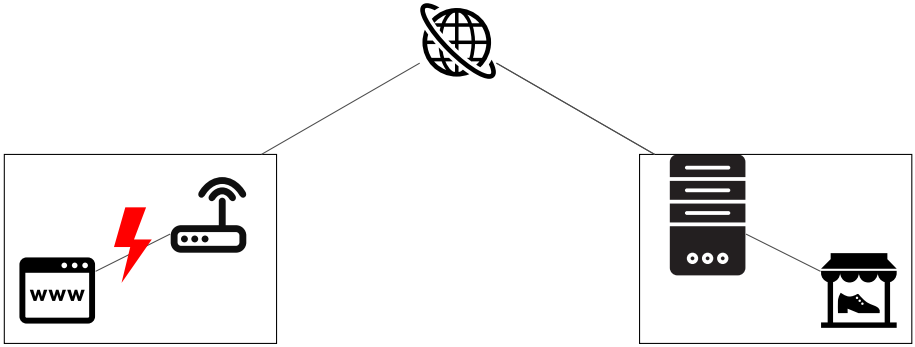
Zugriff auf Webseiten





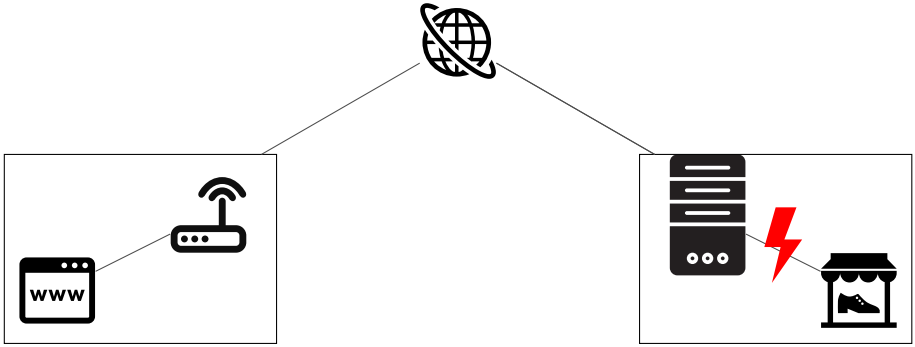
Wo können potentielle Angriffspunkte sein?

Schützen Sie Ihr WLAN!



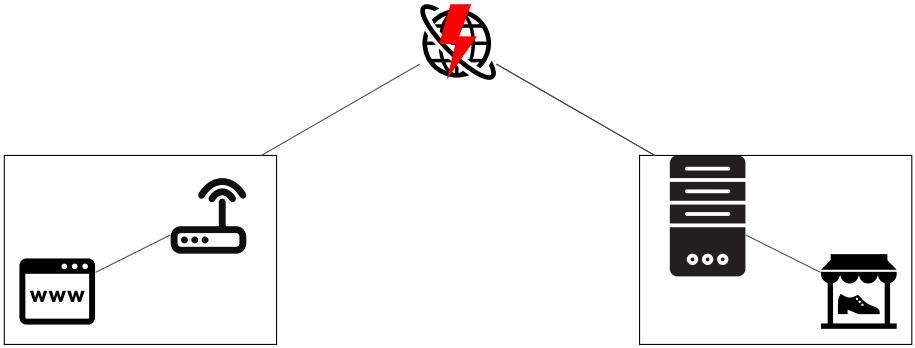
Wo können potentielle Angriffspunkte sein?

Besuchen Sie nur vertrauenswürdige Anbieter!



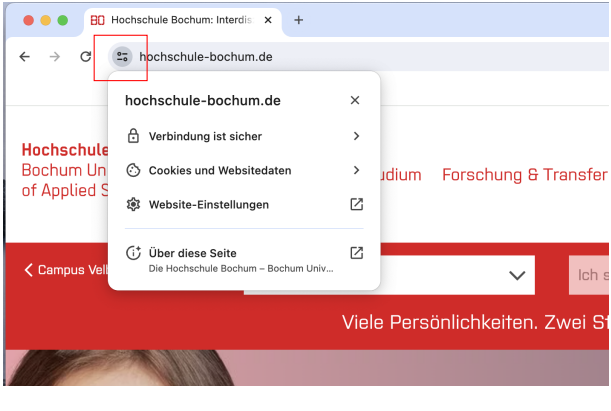
Wo können potentielle Angriffspunkte sein?

Schützen Sie die Internetverbindung!

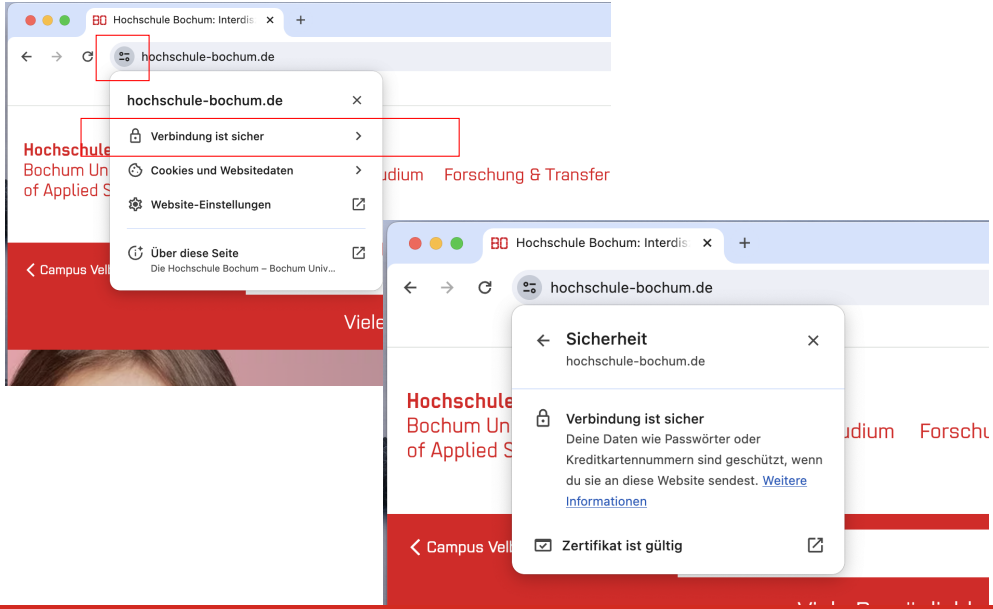


Wo können potentielle Angriffspunkte sein?

Prüfen der Verbindung



Prüfen der Verbindung



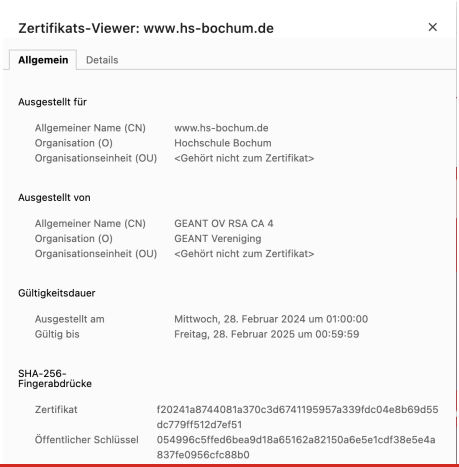
Warum ist die Verbindung zum Web-Server sicher?

Warum ist die Verbindung zum Web-Server sicher?

- Die Daten werden verschlüsselt!

Warum ist die Verbindung zum Web-Server sicher?

- Die Daten werden verschlüsselt!
- Der Server kann sich ausweisen!

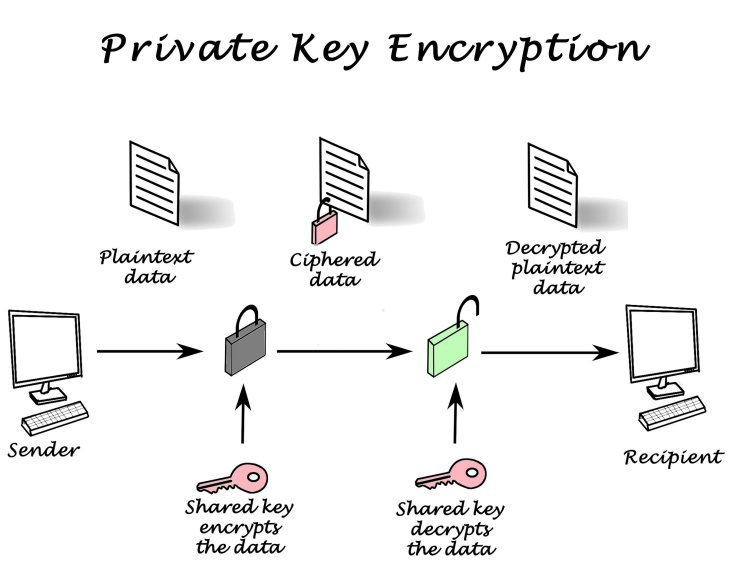


Technische Grundlagen

- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Hashfunktionen
- Zertifikate

Technische Grundlagen

Symmetrische Verschlüsselung


Private Key Encryption
Plaintext data
Ciphered data
Decrypted plaintext data
Sender
Recipient
Shared key encrypts the data
Shared key decrypts the data

Herausforderungen:

- der Schlüssel muss beiden Seiten bekannt sein
- der Schlüssel darf niemandem anderen bekannt sein

Herausforderungen:

- der Schlüssel muss beiden Seiten bekannt sein
- der Schlüssel darf niemandem anderen bekannt sein

Beispiel für (super einfache) Verschlüsselung: Caesar-Verschlüsselung
`https://www.kryptowissen.de/caesar-chiffre-praxis.php`

Herausforderungen:

- der Schlüssel muss beiden Seiten bekannt sein
- der Schlüssel darf niemandem anderen bekannt sein

Beispiel für (super einfache) Verschlüsselung: Caesar-Verschlüsselung
`https://www.kryptowissen.de/caesar-chiffre-praxis.php`

Beispiele für sichere Verschlüsselungsalgorithmen: AES, Triple-DES, Twofish
`https://de.wikipedia.org/wiki/Symmetrisches_Kryptosystem`

Wofür eignet sich symmetrische Verschlüsselung?

Wofür eignet sich symmetrische Verschlüsselung?

- Verschlüsselung von Dokumenten

Wofür eignet sich symmetrische Verschlüsselung?

- Verschlüsselung von Dokumenten
- Verschlüsselung von Festplatten

Wofür eignet sich symmetrische Verschlüsselung?

- Verschlüsselung von Dokumenten
- Verschlüsselung von Festplatten
- Verschlüsselung der WLan-Verbindung

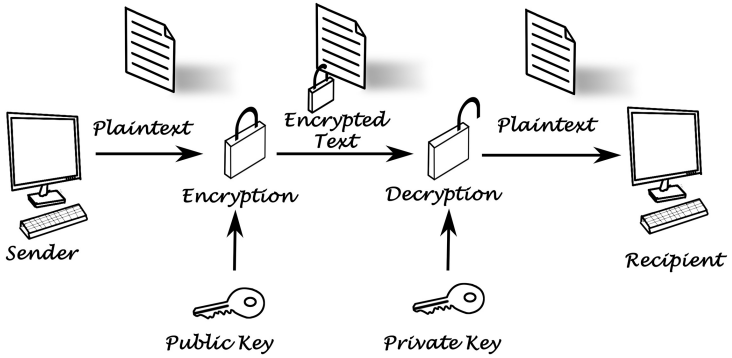
Wofür eignet sich symmetrische Verschlüsselung?

- Verschlüsselung von Dokumenten
- Verschlüsselung von Festplatten
- Verschlüsselung der WLan-Verbindung
- Immer dann sinnvoll, wenn der Schlüssel einfach und sicher geteilt werden kann.

Technische Grundlagen

Aymmetrische Verschlüsselung

Der Empfänger besitzt ein Schlüsselpaar



Herausforderungen:

- der private Schlüssel muss geheim bleiben
- der öffentliche Schlüssel muss sicher zugeordnet werden können
- die Verschlüsselung ist relativ langsam

Wofür eignet sich asymmetrische Verschlüsselung?

Wofür eignet sich asymmetrische Verschlüsselung?

- Verschlüsseltes Versenden von Emails

Wofür eignet sich asymmetrische Verschlüsselung?

- Verschlüsseltes Versenden von Emails
- Verschlüsseltes Versenden von geheimen Schlüsseln

Wofür eignet sich asymmetrische Verschlüsselung?

- Verschlüsseltes Versenden von Emails
- Verschlüsseltes Versenden von geheimen Schlüsseln
- …

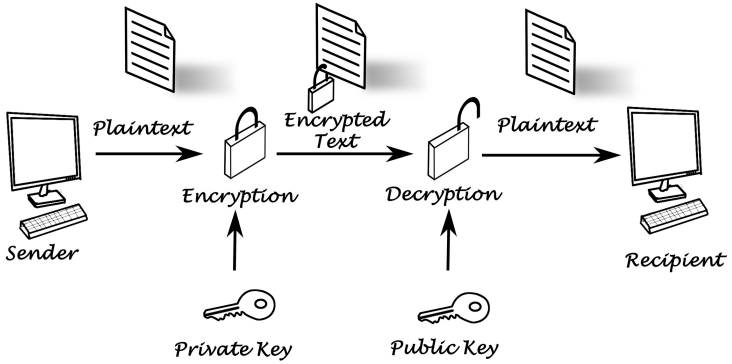
Wofür eignet sich asymmetrische Verschlüsselung?

- Verschlüsseltes Versenden von Emails
- Verschlüsseltes Versenden von geheimen Schlüsseln
- …
- Immer dann sinnvoll, wenn der Schlüssel nicht einfach und sicher geteilt werden kann.

Technische Grundlagen

Signierung

Der Sender besitzt ein Schlüsselpaar



- Der "verschlüsselte" Text ist *nicht* geheim
- Jeder kann den Text mit dem öffentlichen Schlüssel lesen
- Da nur der Besitzer des privaten Schlüssels den Text verschlüsseln konnte, kann dieser als Verfasser verifiziert werden.

- Der "verschlüsselte" Text ist *nicht* geheim
- Jeder kann den Text mit dem öffentlichen Schlüssel lesen
- Da nur der Besitzer des privaten Schlüssels den Text verschlüsseln konnte, kann dieser als Verfasser verifiziert werden.

Herausforderungen:

- der private Schlüssel muss geheim bleiben
- der öffentliche Schlüssel muss sicher zugeordnet werden können

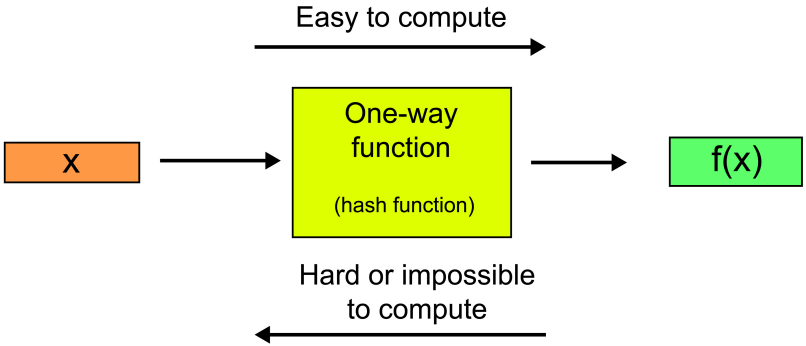
Wofür eignet sich Signierung?

Wofür eignet sich Signierung?

- Sicherstellen, dass ein Dokument von einem bestimmten Verfasser stammt
- …

Technische Grundlagen

Hash-Funktionen



- Der Hashwert $f(x)$ für ein Dokument/x ist immer gleich
- Ändert sich das Dokument/x auch nur ein wenig, ist der Hashwert $f(x)$ vollständig anders
- Zwei unterschiedliche Dokumente/x haben unterschiedliche Hashwerte $f(x)$

Wozu dienen Hash-Funktionen?

Wozu dienen Hash-Funktionen?

- Überprüfen, ob ein Dokument verändert wurde

Wozu dienen Hash-Funktionen?

- Überprüfen, ob ein Dokument verändert wurde
- Speichern von Passwörtern

Wozu dienen Hash-Funktionen?

- Überprüfen, ob ein Dokument verändert wurde
- Speichern von Passwörtern
- …

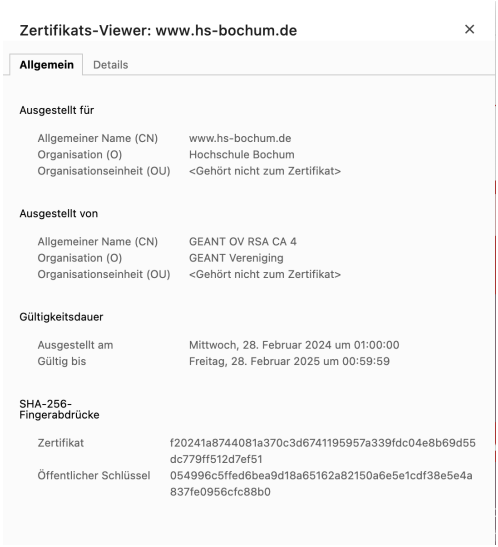
Technische Grundlagen

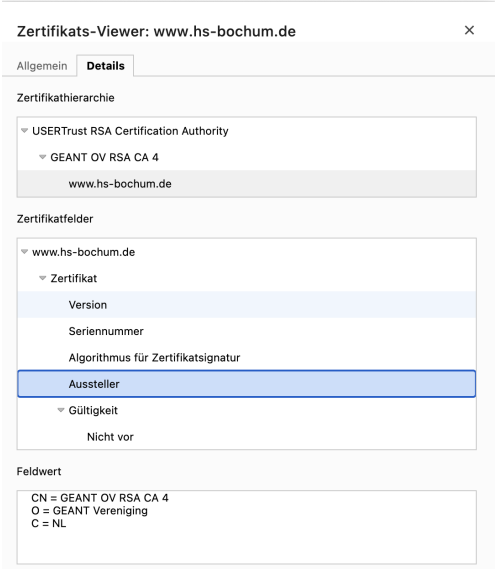
Zertifkate

Ein Zertifikat bestätigt den Eigentümer sowie weitere Eigenschaften eines öffentlichen Schlüssels.
Es beinhaltet i.d.R

- Den Namen des Ausstellers (engl. issuer) des Zertifikates
- Informationen zu den Regeln und Verfahren der Ausgabe
- Informationen zur Gültigkeitsdauer
- Den öffentlichen Schlüssel
- Den Namen des Eigentümers (engl. subject) des öffentlichen Schlüssels.
- Weitere Informationen zum Eigentümer des öffentlichen Schlüssels.
- Angaben zum zulässigen Anwendungs- und Geltungsbereich des öffentlichen Schlüssels.
- Eine digitale Signatur des Ausstellers über alle anderen Informationen.

Beispielzertifikat

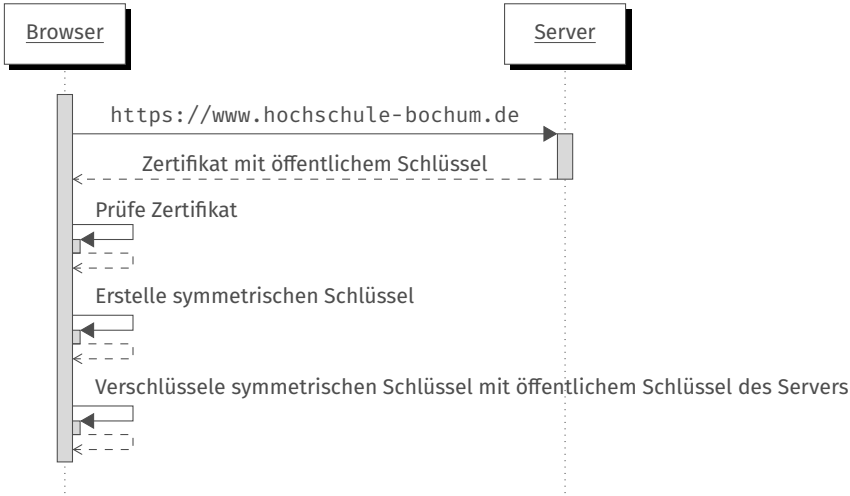


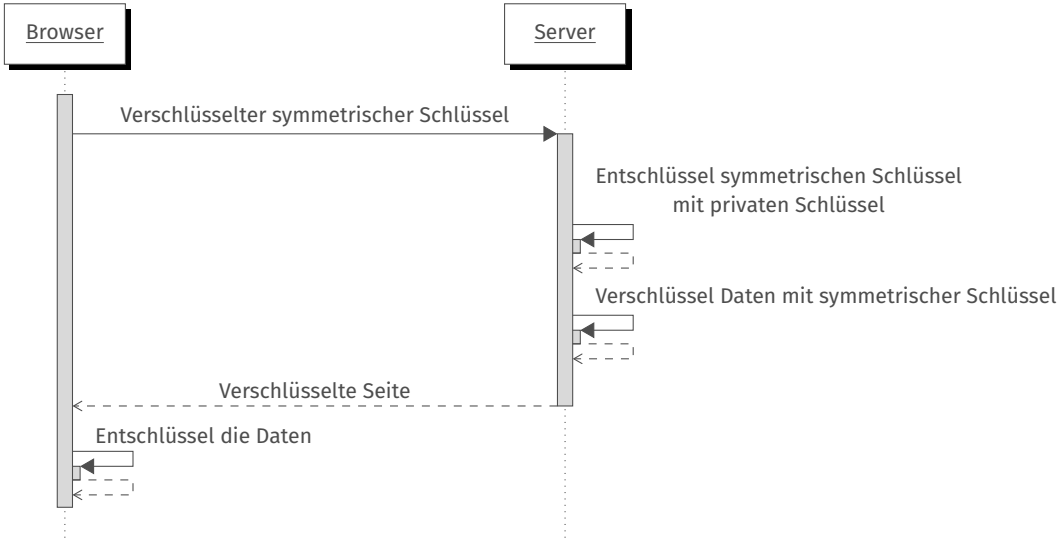


Anwendungen

HTTPS

Wie wird beim Aufruf einer Web-Seite ein Schlüssel generiert und ausgetauscht?

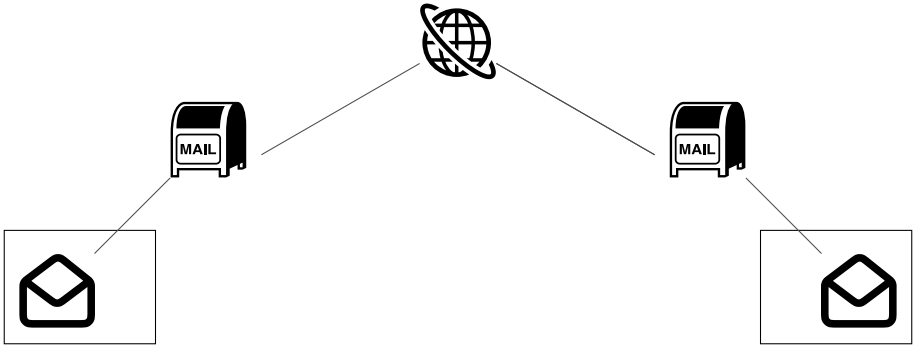

Browser
Server
https://www.hochschule-bochum.de
Zertifikat mit öffentlichem Schlüssel
Prüfe Zertifikat
Erstelle symmetrischen Schlüssel
Verschlüssele symmetrischen Schlüssel mit öffentlichem Schlüssel des Servers


Browser
Server
Verschlüsselter symmetrischer Schlüssel
Entschlüssel symmetrischen Schlüssel
mit privaten Schlüssel
Verschlüssel Daten mit symmetrischer Schlüssel
Verschlüsselte Seite
Entschlüssel die Daten

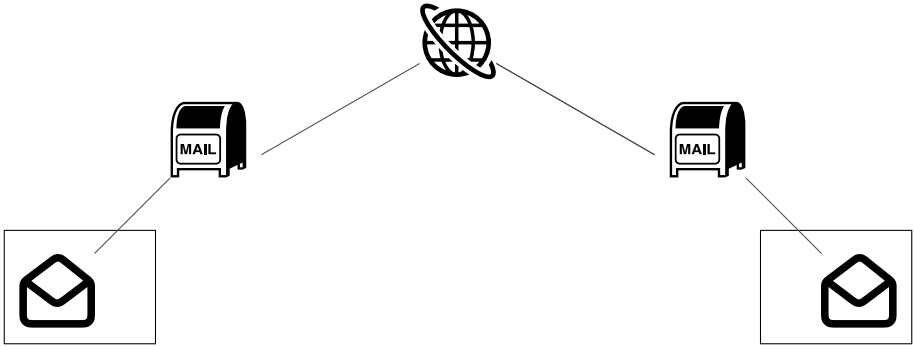
Anwendungen

Email

Emails sind wie Postkarten – für jeden lesbar

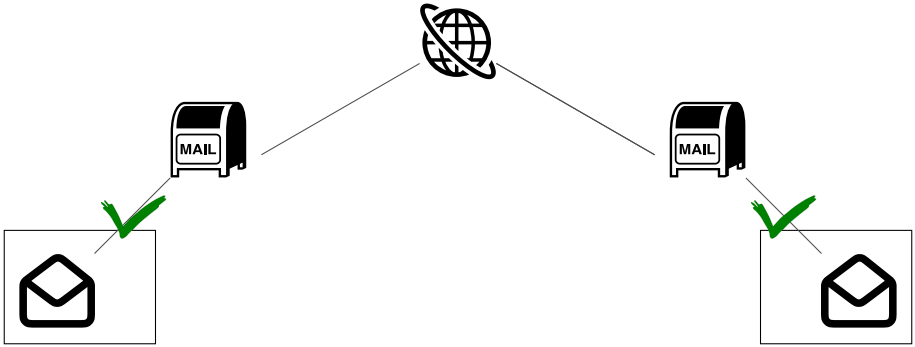


Emails sind wie Postkarten – für jeden lesbar



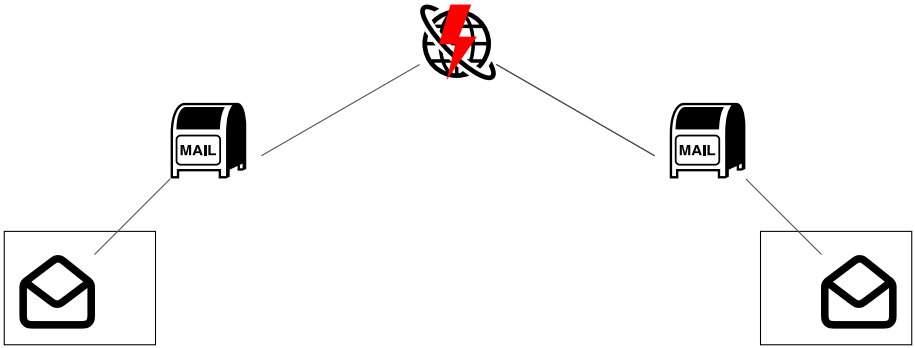
Emails sind wie Postkarten – für jeden lesbar

Die Verbindung zum Mail-Server ist i.d.R. sicher!

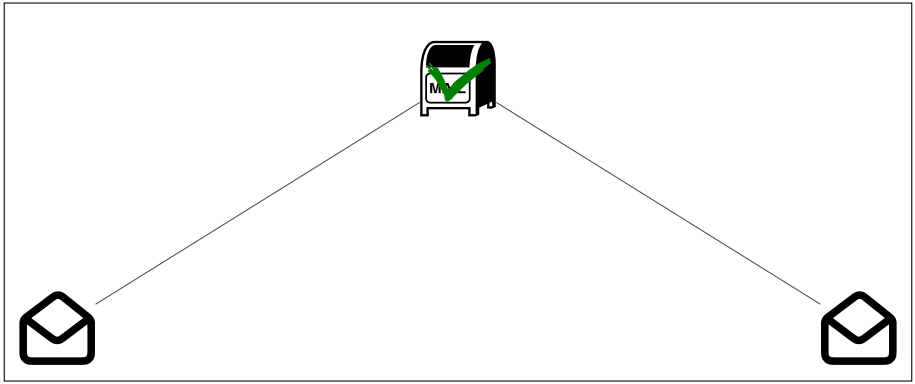


Emails sind wie Postkarten – für jeden lesbar

Im Internet wird die Mail unverschlüsselt weitergereicht!



Emails innerhalb einer Organisation sind sicher!



Alle Nachrichten, die Sie außerhalb kontrollierter Infrastruktur verschicken, sollten Ende-zu-Ende-verschlüsselt sein.

Email: OpenPGP, S/MIME
`https://www.bsi.bund.de/dok/11486410`

WhatsApp: Meta und amerikanische Geheimdienste haben vermutlich Zugriff

Signal, Threema: Server in EU, OpenSource → vermutlich sicher

Verschicken Sie als Unternehmen keine schützenswerten Informationen (Rechnungen, Verträge, Kundendaten, …) per Email.

Anwendungen

Passwörter

Die 10 häufigsten (privaten) Passwörter in Deutschland 2023 (Hasso Platter Institut):

Die 10 häufigsten (privaten) Passwörter in Deutschland 2023 (Hasso Platter Institut):

1. 123456789
2. 12345678
3. hallo
4. 1234567890
5. 1234567
6. password
7. password1
8. target123
9. iloveyou
10. gwerty123

Beruflich wird auch gerne der Firmenname verwendet (Platz 1 lt. Wikipedia in Deutschland)

Wie sollten Sie Passwörter behandeln?

- Gutes Passwort wählen
  - 8–12 Zeichen bei vier verschiedenen Zeichenarten
  - mehr als 25 Zeichen bei 2 Zeichenarten
- Individuelles Passwort pro Account
- Das Passwort sollte im Wörterbuch nicht vorkommen
- Nutzen Sie Mehr-Faktor-Authentifizierung
- Nutzen Sie Passwort-Manager
- Vermeiden Sie Namen und Geburtsdaten
- Vermeiden Sie Wiederholungs- und Tastaturmuster (*qwrtz*)
- Vermeiden Sie Ziffern und Sonderzeichen am Anfang oder Ende eines sonst einfachen Passworts (*password1*)

`https://www.bsi.bund.de/dok/6596574`

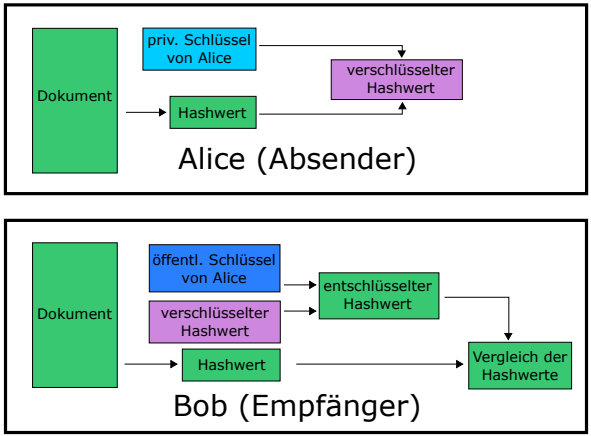
Wie werden Passwörter in den Web-Anwendungen gespeichert?

- Passwörter werden mit einer Hashfunktion "Ein-Weg-Verschlüsselt"
  - Nicht umkehrbar
  - Kollisionsfrei
- "iloveyou" $\rightarrow$ Hashfunktion (SHA-1) $\rightarrow$ "ee8d8728f435fd550f83852aabab5234ce1da528"
- Der Hashwert wird gespeichert
- Bei der Prüfung der Passworts werden die Hashwerte verglichen

Anwendungen

Digitale Signaturen

Eine Signatur (elektronische Unterschrift) stellt sicher, dass ein Dokument von einer bestimmten Person erstellt und nicht geändert wurde.



https://de.wikipedia.org/wiki/Elektronische_Signatur

Rahmenbedingungen für Signaturen

- Technisch sicher, wenn
  - der öffentliche Schlüssel eindeutig zugeordnet werden kann
  - der private Schlüssel sicher gespeichert ist
- Erfordert "Trust Service Provider" der Person verifiziert und Zertifikat ausstellt
- Für Deutschland aktuell unter `https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tl/DE` zu finden
- Gesetzlich geregelt in: Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) und Vertrauensdienstegesetz (VDG)

Informationssicherheit

Sicherstellung der Schutzziele

Vertraulichkeit: Informationen sind nur für den vorgesehen Empfängerkreis einsehbar

Verfügbarkeit: Informationen stehen mit einer hoher Wahrscheinlichkeit zur Verfügung

Integrität: Informationen können nicht unautorisiert verändert werden

- Schutz vor unbefugter Preisgabe von Informationen
  - Eigenschaft einer Information, nur für einen beschränkten Empfängerkreis vorgesehen zu sein.
  - Weitergabe und Veröffentlichung sind nicht erwünscht.
- Schutzmaßnahmen
  - Zugangskontrolle (Bsp.: Tresor, Passwörter, etc.)
  - Verschlüsselung (Bsp.: HTTPS)

Verfügbarkeit

- Gewährleistung, dass die Daten/das System
  - zugänglich und
  - funktionsfähig sind/ist.
- Schutz vor
  - Ausfällen (Schutz gegen Stromausfall, Brand, Wasser, …)
  - Datenverlust (Erstellen von Sicherungen)
  - Diebstahl / Ransomware
  - Denial-of-Service-Attacken

- Gewährleistung, dass die Daten nur von befugten Personen geändert werden
- Schutz vor unbefugtem
  - Löschen
  - Ändern
  - Hinzufügen

Abgeleitete Anforderungen

- Zurechenbarkeit
  - Es kann jederzeit nachgewiesen werden, wer welche Änderungen durchgeführt hat
- Verbindlichkeit/Nichtabstreitbarkeit (engl. non-repudiation)
  - Es ist kein unzulässiges Abstreiten durchgeführter Handlungen
- Rechtssicherheit
  - Die Informationen können rechtskräftig nachgewiesen werden
    - Ein Vertragsabschluss muss z.B. nachgewiesen werden können

- Gesetzliche Anforderungen
  - Datenschutzgrundverordnung (DSGVO)
  - BSI-Gesetz §8a: Sicherheit in der Informationstechnik Kritischer Infrastrukturen
  - BSI-Gesetz §8c: Anforderungen an Anbieter digitaler Dienste
  - Basel II, SOX, Richtlinien zur Buchführung lassen Anforderungen erschließen

- Gesetzliche Anforderungen
  - Datenschutzgrundverordnung (DSGVO)
  - BSI-Gesetz §8a: Sicherheit in der Informationstechnik Kritischer Infrastrukturen
  - BSI-Gesetz §8c: Anforderungen an Anbieter digitaler Dienste
  - Basel II, SOX, Richtlinien zur Buchführung lassen Anforderungen erschließen
- Externe Anforderungen
  - Geschäftspartner erwarten die vertrauliche/sichere Verwendung von Daten
    - BP: Teilefertigung für Automobile erfordern genaue Kenntnisse über Automobil-Design

- Gesetzliche Anforderungen
  - Datenschutzgrundverordnung (DSGVO)
  - BSI-Gesetz §8a: Sicherheit in der Informationstechnik Kritischer Infrastrukturen
  - BSI-Gesetz §8c: Anforderungen an Anbieter digitaler Dienste
  - Basel II, SOX, Richtlinien zur Buchführung lassen Anforderungen erschließen
- Externe Anforderungen
  - Geschäftspartner erwarten die vertrauliche/sichere Verwendung von Daten
    - BP: Teilefertigung für Automobile erfordern genaue Kenntnisse über Automobil-Design
- Interne Anforderungen
  - Daten stellen wirtschaftlichen Wert dar
    - Personaldaten sind für Headhunter interessant
    - Produktdaten für Konkurrenzunternehmen/Plagiierer
    - Verlust von vertraulichen Daten kann zu Vertrauensverlust führen (weniger Kunden, Kursverluste, …)

Kein System kann 100% die Anforderungen erfüllen

- schon früher nicht → Panzerknackerbande
- Risiken:
  - analysieren
  - bewerten (Schaden im Eintrittsfall vs. Eintrittswahrscheinlichkeit vs. Kosten der Schutzmaßnahmen
  - dokumentieren
  - Schutzmaßnahmen ergreifen

Die Sicherstellung der Informationssicherheit ist ein fortlaufenden Prozess

- IT-Grundschutz-Katalog des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Sie liegt in der Verantwortung der Geschäftsleitung, diese kann nicht delegiert werden.

Besonderheit: Datenschutz

Grundrecht auf informationelle Selbstbestimmung

- Jeder kann selbst darüber entscheiden, wem er welche persönlichen Informationen zur Verfügung stellt
- *Volkszählungsurteil* (BVerfG, vom 15. Dezember 1983)
- Verordnung (EU) 2016/679: Datenschutz-Grundverordnung (DSGVO)

Datenschutz-Grundverordnung (DSGVO)

- Unternehmen dürfen Daten nur speichern, wenn
  - es eine gesetzliche Verpflichtung dazu gibt (z.B. Vertragsdaten, Abrechnungsdaten, …), oder
  - der Betroffene seine explizite Einwilligung dazu gegeben hat

Datenschutz-Grundverordnung (DSGVO)

- Unternehmen dürfen Daten nur speichern, wenn
  - es eine gesetzliche Verpflichtung dazu gibt (z.B. Vertragsdaten, Abrechnungsdaten, …), oder
  - der Betroffene seine explizite Einwilligung dazu gegeben hat
- Minimalitätsprinzip: Nur die Daten speichern, die unbedingt erforderlich sind

Datenschutz-Grundverordnung (DSGVO)

- Unternehmen dürfen Daten nur speichern, wenn
  - es eine gesetzliche Verpflichtung dazu gibt (z.B. Vertragsdaten, Abrechnungsdaten, …), oder
  - der Betroffene seine explizite Einwilligung dazu gegeben hat
- Minimalitätsprinzip: Nur die Daten speichern, die unbedingt erforderlich sind
- Gespeicherte Daten müssen auf Anfrage
  - herausgegeben werden
  - korrigiert werden
  - gelöscht werden (wenn rechtlich zulässig)

Datenschutz-Grundverordnung (DSGVO)

- Unternehmen dürfen Daten nur speichern, wenn
  - es eine gesetzliche Verpflichtung dazu gibt (z.B. Vertragsdaten, Abrechnungsdaten, …), oder
  - der Betroffene seine explizite Einwilligung dazu gegeben hat
- Minimalitätsprinzip: Nur die Daten speichern, die unbedingt erforderlich sind
- Gespeicherte Daten müssen auf Anfrage
  - herausgegeben werden
  - korrigiert werden
  - gelöscht werden (wenn rechtlich zulässig)
- Die Prinzipien müssen auch eingehalten werden, wenn die Daten an Dritte weitergegeben werden