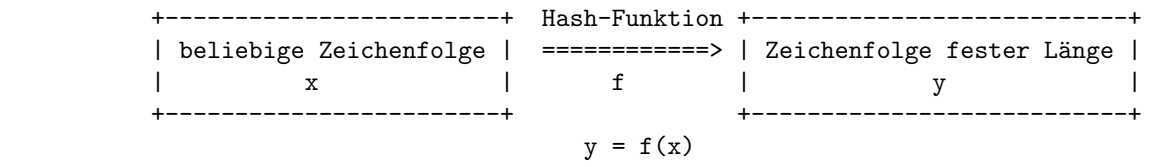
Kryptologie

1 Hash-Funktionen



Einwegfunktion

Praktisch unmöglich, zu gegebenem y ein x zu finden, sodass y = f(x)

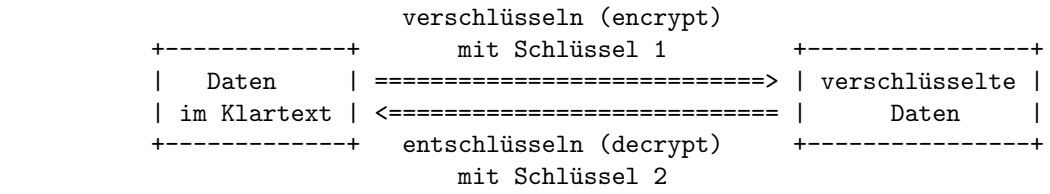
Kollisionsresistenz

Praktisch unmöglich, zwei verschiedene x und x' zu finden, sodass f(x) = f(x')

Algorithmen und Programme

- MD5 (Message-Digest Algorithm 5): `md5sum`
- SHA-2 (Secure Hash Algorithm): `sha224sum, sha256sum, sha384sum, sha512sum`

2 Verschlüsselung



2.1 Symmetrische Verschlüsselung

Eigenschaften

- Zum Ver- und Entschlüsseln wird der gleiche Schlüssel verwendet (Schlüssel 1 = Schlüssel 2).
- schnell, es können große Datenmengen verschlüsselt werden

Algorithmen und Programme

- DES (Data Encryption Standard)
- 3DES (Triple-DES)
- AES (Advanced Encryption Standard): `openssl, gpg`

2.2 Asymmetrische Verschlüsselung

Eigenschaften

- Zum Ver- und Entschlüsseln werden zwei verschiedene Schlüssel verwendet (Private-Key und Public-Key).
- langsam, es können nur kleine Datenmengen verschlüsselt werden

Algorithmus

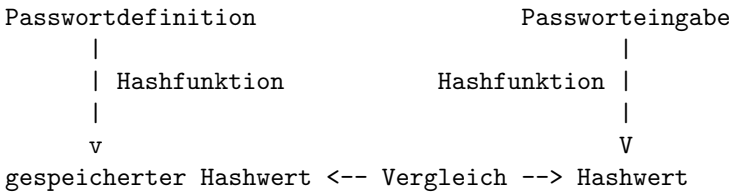
- RSA (Rivest, Shamir und Adleman): `openssl, gpg`

3 Anwendungen

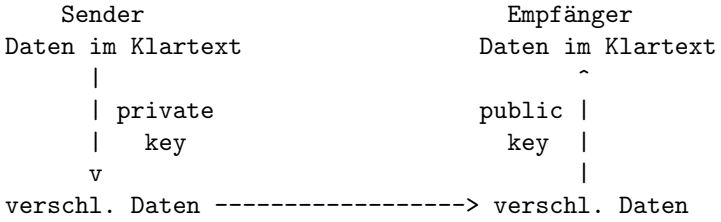
Begriffe

- Authentication (Authentifizierung): Nachweis, dass man diejenige ist, die man behauptet zu sein
- Confidentiality (Vertraulichkeit): Informationen kann nur diejenige lesen, für die sie bestimmt sind
- Integrity (Integrität): Daten wurden nicht verändert

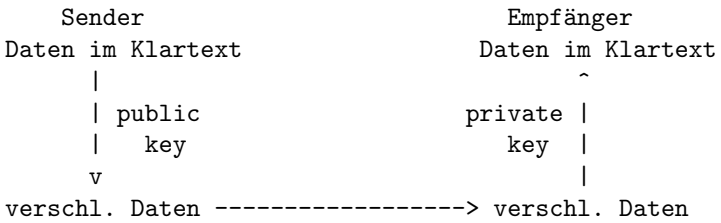
Nur Hashwerte von Passwörten speichern



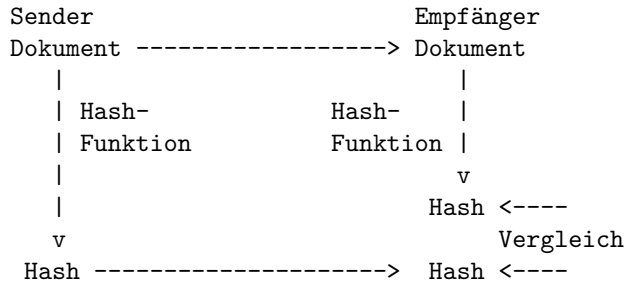
Authentifizierung



Vertraulichkeit



Integrität eines Dokuments



Signatur eines Dokuments

Beweis für die Integrität und die Herkunft eines Dokuments