Asymmetrische Verschlüsselung

Public-Key-Verfahren, digitale Signatur und Zertifikate

Wiederholung zur Prüfungsvorbereitung AP1 · Einrichten eines IT-gestützten Arbeitsplatzes

Wer ist eigentlich Alice?

- Seit dem RSA-Aufsatz von 1978 stehen in fast jeder Veröffentlichung zur Kryptografie dieselben Namen. Der Grund ist praktisch: „A sendet an B" verwechselt man ständig, „Alice sendet an Bob" nicht.

NAME	ROLLE	WAS SIE ODER ER TUT
Alice	Senderin	will eine Nachricht sicher loswerden
Bob	Empfänger	soll sie lesen können — und sonst niemand
Eve	Lauscherin (passiv)	hört mit, verändert aber nichts. Von englisch eavesdropper
Mallory	Angreifer (aktiv)	fängt ab, verändert, schiebt eigene Nachrichten unter

Prüfungsrelevant: Gegen **Eve** hilft Verschlüsselung. Gegen **Mallory** braucht es zusätzlich Signatur und Zertifikate — sonst merkt niemand, dass etwas ausgetauscht wurde.

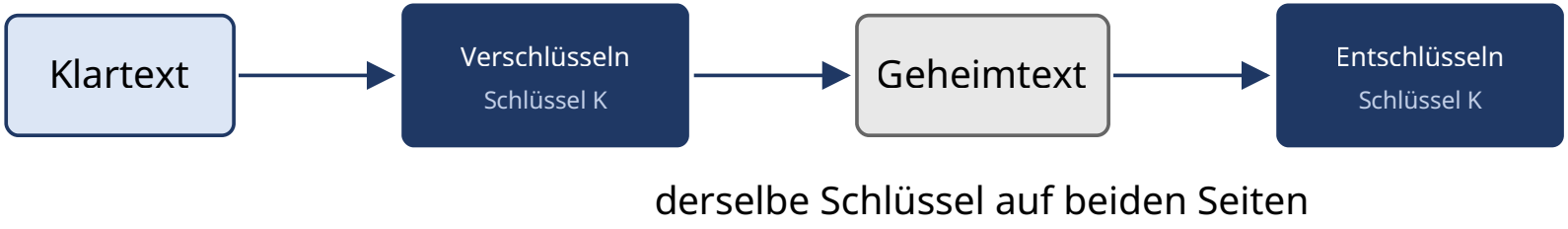
Wo wir stehen: die Schutzziele

SCHUTZZIEL	BEDEUTUNG	TYPISCHE MASSNAHME
Vertraulichkeit	Nur Befugte können die Daten lesen	Verschlüsselung, Zugriffsrechte
Integrität	Daten sind unverändert und vollständig	Hashwerte, Prüfsummen, Signatur
Authentizität	Der Absender ist der, der er zu sein vorgibt	Digitale Signatur, Zertifikate
Verfügbarkeit	Daten sind nutzbar, wenn sie gebraucht werden	Backup, Redundanz, USV

Für die Prüfung: Fragen lauten selten „was ist RSA". Sie lauten „welches Schutzziel wird verletzt" oder „welche Maßnahme schlagen Sie vor". Ordnen Sie jedes Verfahren einem Schutzziel zu — dann haben Sie die Antwort.

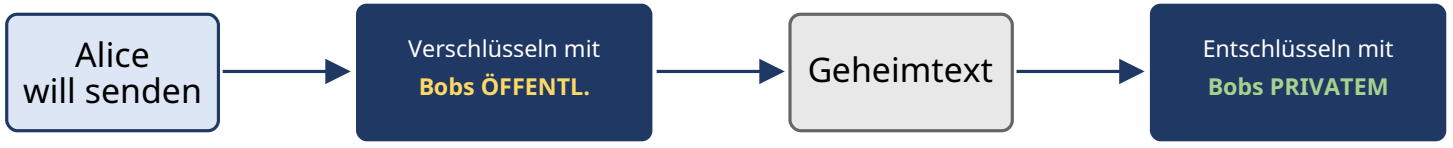
Symmetrische Verschlüsselung — und ihr Problem

- **Ein einziger Schlüssel** für Ver- und Entschlüsseln — beide Seiten besitzen denselben. Verfahren: AES, ChaCha20 (veraltet: DES, 3DES)
- **Die offene Frage:** Wie kommt dieser Schlüssel zum Partner? Über dieselbe Leitung wie die Nachricht? Dann liest Eve beides mit.



Das Schlüsselpaar

- Jede Person besitzt **zwei** zusammengehörige Schlüssel: den **öffentlichen** darf jeder kennen, der **private** muss geheim bleiben.
- Bei sicherem Verfahren lässt sich der private aus dem öffentlichen praktisch nicht berechnen. Verfahren: RSA, ECC; Diffie-Hellman zum Aushandeln.
- **Kerckhoffssches Prinzip:** Das Verfahren darf vollständig bekannt sein — geheim bleiben müssen allein die geheimen Schlüssel. Sicherheit durch Verschweigen ist keine.



Nur Bob besitzt den privaten Schlüssel — nur er kann lesen.
Der öffentliche Schlüssel darf offen im Netz stehen.

Symmetrisch oder asymmetrisch?

	SYMMETRISCH (AES)	ASYMMETRISCH (RSA, ECC)
Schlüssel	ein gemeinsamer, geheimer	Paar aus öffentlich und privat
Geschwindigkeit	sehr schnell, auch bei großen Dateien	deutlich langsamer
Schlüsselaustausch	**das Problem** — muss geheim erfolgen	**kein geheimer Vorabaustausch** — Echtheit bleibt zu klären
Anzahl bei n Personen	n·(n−1)/2 gemeinsame Schlüssel — bei 12 sind das 66	n Schlüsselpaare
Signatur möglich	nein	ja
Typischer Einsatz	die eigentlichen Nutzdaten	Schlüsselaustausch, Signatur

Beide ergänzen sich, sie konkurrieren nicht — daraus entsteht das **hybride Verfahren**.

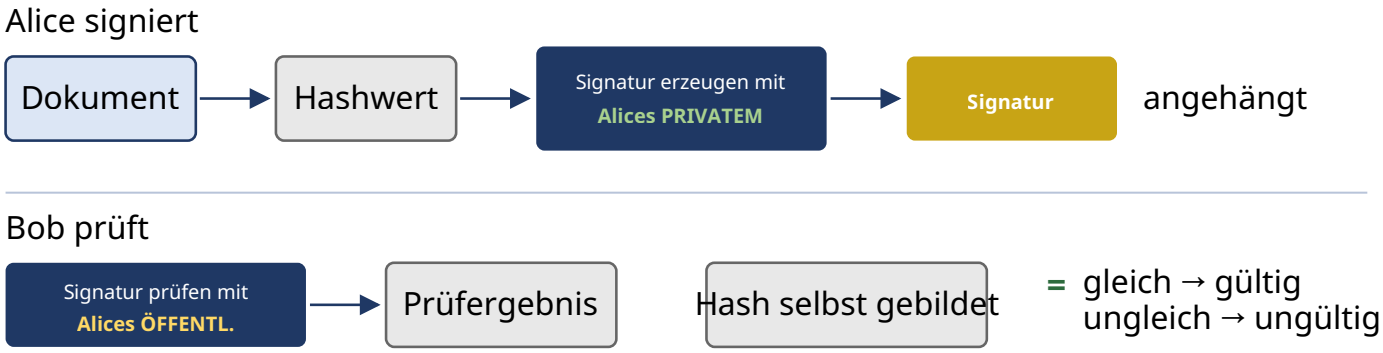
Wer verschlüsselt womit?

ZIEL	SENDER BENUTZT	EMPFÄNGER BENUTZT
Vertraulichkeit niemand sonst soll mitlesen	**öffentlichen** Schlüssel des **Empfängers**	**privaten** Schlüssel des **Empfängers**
Authentizität + Integrität Nachweis der Herkunft	**privaten** Schlüssel des **Senders** (Signatur)	**öffentlichen** Schlüssel des **Senders**
Beides zugleich	erst signieren mit eigenem privaten, dann verschlüsseln mit öffentlichem des Empfängers	

Eselsbrücke: Verschlüsseln richtet sich an den **Empfänger** — also nimmt man dessen Schlüssel. Signieren spricht über den **Sender** — also nimmt man den eigenen. Wer das sicher hat, löst die meisten Aufgaben.

Digitale Signatur

Vorab, der Hashwert: eine Einwegfunktion — aus beliebig langen Daten wird ein Wert fester Länge, nicht umkehrbar. Sicher: SHA-256, SHA-3. Unsicher wegen Kollisionen: **MD5, SHA-1**.



Belegt Herkunft und Integrität — sofern der Schlüssel nachweislich zu Alice gehört

Signiert ist nicht verschlüsselt: das Dokument bleibt im Klartext. Sprachlich sauber: **Signatur erzeugen** und **prüfen** — nicht „den Hash verschlüsseln"; die Kurzform stammt aus RSA und gilt bei ECDSA nicht.

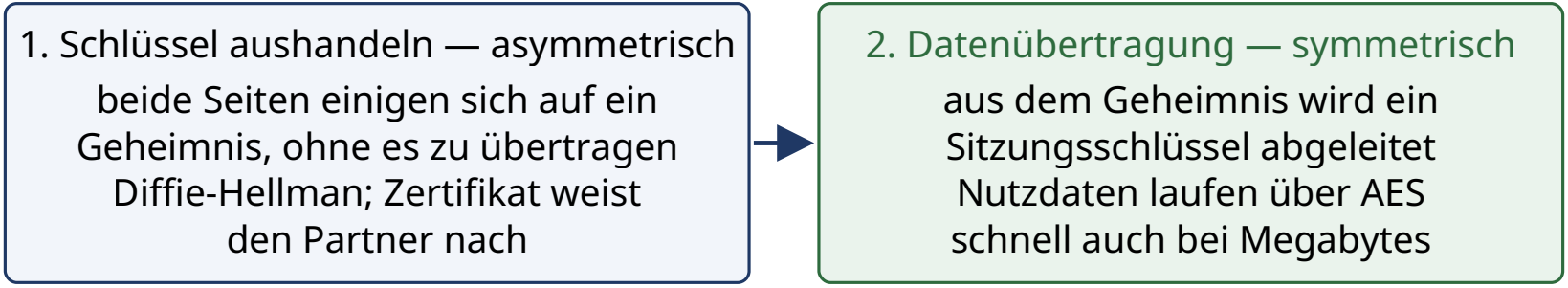
Signatur vorhanden heißt nicht Signatur geprüft

Der Titeltext des Comics lautet sinngemäß: „Wer ganz sicher gehen will, prüft, ob unten ein großer Block wirrer Zeichen steht." Genau das ist der Trugschluss. Ein Signaturblock **sieht** nach Sicherheit aus — geprüft ist er damit nicht.

Eine Signatur nützt nur, wenn sie **verifiziert** wird und der öffentliche Schlüssel **nachweislich** zum Absender gehört. Dasselbe gilt für das Schloss im Browser: sichtbar ist noch nicht geprüft.

Hybride Verschlüsselung

- **Asymmetrisch** handelt den Schlüssel aus und weist nach, wer der Partner ist — **symmetrisch** laufen dann die eigentlichen Daten.
- **PGP und S/MIME:** ein zufälliger Dateischlüssel wird mit dem öffentlichen Schlüssel des Empfängers verpackt und mitgeschickt.
- **Modernes TLS (ab Version 1.3):** kein Schlüssel wird verschickt. Beide Seiten handeln über Diffie-Hellman ein gemeinsames Geheimnis aus und leiten daraus die Sitzungsschlüssel ab; das Zertifikat dient der Authentisierung.



Zertifikate und Zertifizierungsstelle

Das offene Problem: Alice lädt „Bobs öffentlichen Schlüssel" herunter — woher weiß sie, dass er wirklich Bob gehört? Asymmetrie löst den Schlüsselaustausch, nicht die Echtheit.

BEGRIFF	BEDEUTUNG
Digitales Zertifikat (Standard X.509)	bindet einen öffentlichen Schlüssel an eine Identität — Inhaber, Schlüssel, Aussteller, Gültigkeitszeitraum
Zertifizierungsstelle (CA)	signiert das Zertifikat; nachträgliche Änderungen werden bei der Prüfung erkennbar
Vertrauenskette	Server-Zertifikat ← Zwischen-CA ← Root-CA. Nur der Root-CA vertraut Ihr Browser von sich aus; sie ist im Betriebssystem hinterlegt

Bei einem einfachen Zertifikat prüft die CA nur die **Kontrolle über den Domainnamen** — nicht die Seriosität des Betreibers.

HTTPS: was das Schloss bedeutet

DAS SCHLOSS SAGT	DAS SCHLOSS SAGT **NICHT**
Die Verbindung ist verschlüsselt (Vertraulichkeit)	Dass die Seite seriös ist
Das Zertifikat ist gültig und passt zur Adresse	Dass der Betreiber ehrlich ist
Eine vertrauenswürdige CA hat es ausgestellt	Dass Ihre Daten dort sicher gespeichert werden

Prüfungsrelevant: Auch eine Phishing-Seite kann ein gültiges Zertifikat besitzen. HTTPS schützt den **Transportweg**, nicht vor betrügerischen Inhalten. Ebenso: HTTPS ersetzt kein Backup und keine Zugriffskontrolle.

Typische Prüfungsfallen

FALSCH	RICHTIG
„Ich verschlüssele mit meinem privaten Schlüssel, damit nur der Empfänger liest."	Verschlüsselt wird mit dem **öffentlichen** Schlüssel des **Empfängers**.
„Eine signierte Mail kann niemand lesen."	Doch — Signatur beweist nur Herkunft und Unverändertheit.
„Asymmetrisch ist sicherer, also nimmt man es für alles."	Zu langsam für Massendaten, deshalb **hybrid**.
„Der Hashwert verschlüsselt die Datei."	Hash ist eine Einwegfunktion, keine Verschlüsselung — nicht umkehrbar.
„HTTPS bedeutet, die Seite ist vertrauenswürdig."	Nur der Transportweg ist geschützt.

Zusammenfassung

VERFAHREN	ERFÜLLT SCHUTZZIEL	TYPISCHER EINSATZ
Symmetrisch (AES)	Vertraulichkeit	Nutzdaten, Festplattenverschlüsselung
Asymmetrisch (RSA, ECC)	Vertraulichkeit	Schlüsselaustausch, Signatur
Hashwert (SHA-256)	Integrität	Dateiprüfsummen, Downloadvergleich
Digitale Signatur	Authentizität + Integrität	E-Mail, Software, Verträge
Zertifikat / PKI	Authentizität	HTTPS, VPN
Hybrid (TLS)	alle drei zusammen	HTTPS, SSH, VPN-Verbindungen
Passwort-Hashverfahren	Passwörter schützen	Argon2id, bcrypt — mit Salt, **nicht** einfaches SHA-256

> In der Prüfung zuerst fragen: **welches Schutzziel** meint die Aufgabe? Die Verfahrenswahl ergibt sich fast immer daraus.

Quellen

GRUNDLAGE	FUNDSTELLE
Ausbildungsrahmenplan	FIAusbV vom 28.02.2020, Anlage, Abschnitt A, lfd. Nr. 6 „Umsetzen, Integrieren und Prüfen von Maßnahmen zur IT-Sicherheit und zum Datenschutz" — 6 Wochen im 1. bis 18. Monat
Rahmenlehrplan	KMK-Beschluss vom 13.12.2019, Lernfeld 4 „Schutzbedarfsanalyse im eigenen Arbeitsbereich durchführen", 1. Ausbildungsjahr, 40 Stunden
Prüfungsbereich	Teil 1 der gestreckten Abschlussprüfung, 90 Minuten schriftlich (§ 9 FIAusbV). Die Aufgabenform ist dort nicht festgelegt — die Übungsaufgaben sind der gängigen Prüfungspraxis nachgebildet, es sind keine Originalaufgaben der IHK
Signatur und Hashing	NIST FIPS 186-5 (Digital Signature Standard); TLS 1.3 nach RFC 8446
Kryptobox-Übung	Dietrich / Lautebach: Kryptografie — Informatik des Vertrauens, Landesakademie für Fortbildung und Personalentwicklung an Schulen Baden-Württemberg, 01/2018
Unplugged-Ansatz	CS Unplugged: Public Key Encryption, University of Canterbury, CC BY-NC-SA 4.0
Comic	Randall Munroe: PGP, xkcd Nr. 1181, 04.03.2013, CC BY-NC 2.5