Aufgaben in Kapitel 2

T1 Richtig oder falsch?

a richtig

b Falsch: Mit vier Bit lassen sich $2 \cdot 2 \cdot 2 \cdot 2 = 16$ verschiedene Werte darstellen.

c richtig

d Falsch: Allerdings muss zunächst die Schlüssellänge bestimmt werden, ehe sich mehrere voneinander unabhängige Häufigkeitsanalysen einsetzen lassen.

e Falsch: Der Schlüsselaustausch kann auch mit asymmetrischen Verschlüsselungsverfahren erfolgen.

f Falsch: Die Quersumme einer gegebenen Zahl lässt sich leicht bilden, allerdings ist es schlichtweg unmöglich, aus einer gegebenen Quersumme die ursprüngliche Zahl zu rekonstruieren, auch nicht unter großem Aufwand. Die Quersumme 4 könnte beispielsweise sowohl für die Zahl 13 als auch für die Zahl 22 stehen.

g Falsch: Wenn man eine Nachricht verschicken möchte, muss man diese mit dem öffentlichen Schlüssel des Empfängers verschlüsseln.

h Falsch: Mittels einer digitalen Signatur kann die Integrität einer Nachricht gesichert werden.

T2 Cäsar und Vigenère anwenden

a PUALYULA

b AOAYOGEYANEJACIAFZRZAEIXECIA

T3 Mögliche Schlüssel

Länge	Anzahl möglicher Schlüssel beim Vigenère-Verfahren bei 26 Zeichen	Dauer*	Anzahl möglicher Schlüssel beim Vigenère-Verfahren bei 80 Zeichen	Dauer
6	$26^6 = 308\,915\,776$	7 min.	80^6	4,3 d
8	$26^8 = 208\,827\,064\,576$	3,4 d	80^8	76 a
10	$26^{10} = 141\,167\,095\,653\,376$	6 a	80^{10}	486 401 a

* Dauer eines Brute-Force-Angriffs für das Durchprobieren aller Möglichkeiten, wenn sich 700 000 Schlüssel pro Sekunde ausprobieren lassen

T4 Symmetrische und asymmetrische Verschlüsselung

	Symmetrische Verschlüsselung	Asymmetrische Verschlüsselung
Anzahl der notwendigen Schlüssel bei Nachrichtenaustausch unter mehreren Personen	n(n–1) bei n Teilnehmenden	n bei n Teilnehmenden
Notwendige Vorbereitung, um Kommunikation durchführen zu können	persönliches Treffen oder Schlüsseltausch auf andere Weise	Erzeugung eines persönlichen Schlüsselpaars und Veröffentlichen des öffentlichen Schlüssels
Berechnungsaufwand	abhängig von Verfahren: im Allgemeinen deutlich geringer als bei asymmetrischen Verfahren	erhöht gegenüber symmetrischer Verschlüsselung, aber abhängig von der Schlüssellänge

T5 Digitale Signaturen

Alice:

- Nachricht verfassen
- kryptografischen Hashwert der Nachricht berechnen
- Hashwert mit privatem Schlüssel von Alice verschlüsseln
- Nachricht und verschlüsselten Hashwert (Signatur) an Bob senden

Bob:

- empfangene Signatur mit öffentlichem Schlüssel von Alice entschlüsseln
- kryptografischen Hashwert der empfangenen Nachricht berechnen
- berechneten Hashwert mit dem entschlüsselten Hashwert vergleichen
  → bei Übereinstimmung ist die Nachricht unverfälscht

Aufgaben in Kapitel 3

T1 Richtig oder falsch?

a Falsch: Die Kommunikation im Internet erfolgt oft nach dem Client/Server-Prinzip.

b Falsch: Ein Switch kann zwar theoretisch mehrere Netze miteinander verbinden. Um eine sinnvolle Kommunikation zwischen den Netzen zu ermöglichen, sollte jedoch ein Router die Netze verbinden. Ein Switch kann innerhalb eines Netzes eingesetzt werden, um mehrere Geräte miteinander zu verbinden.

c Falsch: DNS steht für Domain Name System, welches Domains IP-Adressen zuordnet.

d Falsch: Das Schichtenmodell teilt die Kommunikation im Internet in mehrere Schichten wie Anwendungs-, Transport-, Internet- und Netzzugangsschicht auf.

e richtig

f Falsch: Cookies dienen dazu, Nutzer über einzelne Anfragen hinweg zu identifizieren

T2 Ich check's, dank deiner Hilfe!

Die Kommunikation zwischen Maschinen erfolgt oft nach dem **Client/Server-Prinzip**. Dabei initiiert der Client die Kommunikation, während der Server als Dienstanbieter zunächst passiv auf eingehende Anfragen von Clients wartet. Ein Client kann beispielsweise bei einem Webserver eine Webseite anfragen. Dieser antwortet mit der passenden Seite.

Mehrere Netze können mit **Routern** miteinander verbunden werden. Die Router sorgen dafür, dass die Datenpakete über die Netze hinweg schrittweise ans Ziel gelangen. Anhand von Routing-Tabellen treffen sie Entscheidungen, über welchen Weg die Daten weitergeleitet werden.

In einem lokalen Netz können mehrere Geräte über einen **Switch** verbunden werden.

Die Kommunikation in Netzen verläuft im **Schichtenmodell**. Ein wichtiger Vorteil bei diesem Schichtenmodell ist die einfache Austauschbarkeit der konkreten Umsetzung einzelner Schichten. Ein weiterer Vorteil ist die Wiederverwendbarkeit bereits existierender Schichten für andere Zwecke. Die Kommunikation zwischen Rechnern kann durch das TCP/IP-Modell als Stapel aus insgesamt vier Schichten dargestellt werden: Anwendungs-, Transport-, Internet- und Netzzugangsschicht.

Auf der Transportschicht verwenden Server **Ports**, um bestimmte Dienste anzubieten. Die Ports sind dabei durchnummeriert. Für häufig verwendete Dienste sind einheitliche Portnummern festgelegt (z. B. 80 für HTTP). Auch von Clients versendete Daten haben eine (oft zufällig gewählte) Portnummer als Teil der Absenderadresse. Auf diese Weise können Ports dazu verwendet werden, mehrere Kommunikationsstränge zwischen gleichen Partnern auseinanderzuhalten. Ein Client-Rechner kann beispielsweise mit einer Webserver- und einer Mailserver-Anwendung auf dem gleichen Server-Rechner kommunizieren, ohne, dass dabei z. B. versehentlich Webseitenanfragen den Mailserver erreichen.

IP-Adressen werden verwendet, um Geräte auf der Internetschicht eindeutig zu identifizieren. Sie kommen in den Versionen IPv4 und IPv6 zum Einsatz. In lokalen Netzen werden bisher IPv4 Adressen häufiger genutzt. Diese sind 32 Bit lang und werden zur besseren Lesbarkeit in vier Dezimalblöcken geschrieben (z. B. 192.168.1.2). Der sogenannte Netzanteil einer IP-Adresse gibt an, in welchem Netz sich ein Gerät befindet. Der sogenannte Hostanteil der Adresse ist in diesem Netz einmalig für ein Gerät vergeben.

Auf der Netzzugangsschicht werden Geräte mithilfe **der MAC-Adresse** identifiziert. Sie ist 48 Bit lang und wird üblicherweise hexadezimal geschrieben (z. B. 12:34:DE:AD:BE:EF).

Damit Maschinen erfolgreich Informationen austauschen können, müssen die Regeln für die Kommunikation in **Protokollen** eindeutig festgelegt werden. Typische Bestandteile eines Protokolls sind das Ablaufschema der Kommunikation, die Codierung der zu übertragenden Daten und die Reaktion auf Fehler bei der Übertragung.

Ein Cookie ist eine kleine Textdatei, die vom Server generiert, an den Client übermittelt und dort gespeichert wird. Bei späteren Anfragen wird der Client dann aufgefordert, den Inhalt dieser Textdatei als Teil der Anfrage mitzusenden. So kann der Server den Client erneut identifizieren. **Cookies** sorgen dafür, dass Zugangsdaten oder Einstellungen nicht bei jeder Anfrage erneut eingegeben werden müssen. Sie werden aber auch eingesetzt, um die Aktivität von Nutzern im Internet zu verfolgen (Tracking-Cookies).

T3 Kommunikation im Schichtenmodell

a Anwendungs-, Transport-, Internet-, Netzzugangsschicht

b Die Endnutzer interagieren mit der Anwendungsschicht. Diese entspricht in der Regel dem jeweils genutzten Dienst (z. B. WWW, E-Mail, …). Die Transportschicht stellt der eigentlichen Anwendung einen Ende-zu-Ende-Kommunikationskanal bereit, sodass die Client- und die Serveranwendung direkt Daten austauschen können. Die zentrale Aufgabe der Internetschicht ist die Wegewahl (engl. routing). Insbesondere in großen Netzen wie dem Internet erreichen die Datensegmente der Transportschicht ihr Ziel in der Regel nicht direkt, sondern werden von Vermittlungsrechnern (Routern) bis ins Zielnetz weitergeleitet. Die Netzzugangsschicht sorgt für einen möglichst störungsfreien Kommunikationspfad zwischen den verschiedenen Stationen.

c Jede Schicht verwendet unterschiedliche Protokolle. Auf der Senderseite durchlaufen die zu versendenden Daten alle Schichten. Alle verwendeten Protokolle ergeben den Protokollstapel. Ein Beispiel für einen solchen Stapel wäre HTTP auf der Anwendungsschicht, TCP auf der Transportschicht, IP auf der Internetschicht und 1000Base-T auf der Netzzugangsschicht.

d Auf der Anwendungsschicht werden beispielsweise URLs verwendet, um einen Webserver zu kontaktieren. Auf der Transportschicht verwenden Server Ports, um bestimmte Dienste anzubieten. Die Internetschicht nutzt IP-Adressen zur eindeutigen Identifikation von Geräten. Auf der Netzzugangsschicht werden in der Regel sogenannte MAC-Adressen verwendet.

T4 Protokolle

a Das HTTP-Protokoll legt auf der Anwendungsschicht die Regeln zum Abrufen einer Webseite fest. Die Variante HTTPS ermöglicht eine verschlüsselte Kommunikation. E-Mails können beispielsweise mit dem SMTP- oder POP-Protokoll versendet werden.

b Sind Protokolle in frei zugänglichen Dokumenten standardisiert und beschrieben, können alle diese Spezifikationen einsehen. Bei der Entwicklung von Software (z. B. einem E-Mail-Client) kann das Protokoll passend umgesetzt werden. Sollten sich Änderungen im Protokoll ergeben, können alle Produkte, welche das Protokoll verwenden, angepasst werden. Die Kommunikation in Netzen kann unabhängig von Betriebssystemen, Sprachen und Hardware umgesetzt werden.

c Lösungsbeispiel: Die Kommunikation wird mit fünf schnellen Klopfzeichen begonnen, woraufhin das Gegenüber innerhalb von 10 Sekunden ebenfalls mit fünf schnellen Klopfzeichen antworten muss, um den Verbindungsaufbau zu bestätigen.
Der eigentliche Datenaustausch erfolgt anschließend nach den Regeln des Morsealphabets. Der Initiator der Kommunikation darf dabei als erstes „senden". Danach wird jeweils abwechselnd „gesendet", wobei jede empfangene Nachricht mindestens mit „OK" bestätigt werden muss. Eine Pause von mindestens 10 Sekunden signalisiert das Ende einer Nachricht.
Die Verbindung kann abgebaut werden, indem die Nachricht „ENDE ENDE ENDE" gemorst wird. Alternativ wird auch eine Pause von mindestens 60 Sekunden als Verbindungsabbruch interpretiert.

T5 Firewalls

a Eine Firewall kann am Verbindungspunkt eines lokalen Netzes mit dem Internet oder auf individuellen Geräten verwendet werden, um die Angriffsmöglichkeiten aus dem Internet zu reduzieren. Es handelt sich bei einer Firewall um eine spezielle Software, welche den Datenverkehr vom und ins Internet überwacht und nach zuvor festgelegten Regeln filtert. Der Datenverkehr kann so auf bestimmte Protokolle oder festgelegte Adressen beschränkt werden.

b Das Öffnen eines Ports bedeutet, eine Regel zur Firewall hinzuzufügen, welche die Kommunikation auf dem geöffneten Port erlaubt.

c individuell

Aufgaben in Kapitel 4

T1 Richtig oder falsch?

a Falsch: Verbreitete Anwendungen wie Bilderkennungssysteme, Sprachassistenten oder Textgeneratoren sind Vertreter schwacher KI-Systeme. Starke KI wurden in den 2010er Jahren jedenfalls nicht entwickelt.

b Falsch: Bei unüberwachtem Lernen müssen die Daten über kein Label verfügen.

c richtig

d Falsch: Zur linearen Separation genügt ein einzelnes künstliches Neuron

e Falsch: Die Neuronen der Eingabeschicht leiten die Werte unverändert an die Neuronen der nachfolgenden Schicht weiter.

f Bei der Nachvollziehbarkeit eines KI-Systems unterscheidet man zwischen Erklärbarkeit und Transparenz. Beschränkt man sich auf die Erklärbarkeit, ist die Antwort falsch, weil nur wesentliche Argumente für eine Entscheidung benannt werden müssen. Legt man den Schwerpunkt auf Transparenz, ist die Antwort richtig.

T2 Ich check's, dank deiner Hilfe!

Starke und schwache KI: Schwache KI beschreibt Systeme, die nur eine bestimmte Aufgabe lösen können, z. B. virtuelle persönliche Assistenten. Eine starke KI hingegen würde über eine dem Menschen ebenbürtige Intelligenz verfügen oder diese sogar noch übertreffen. Solche Systeme gibt es aktuell nicht.
Überwachtes Lernen hat als Ziel jedem Datum ein (bekanntes) Label zuzuordnen, z. B. „Hund" bzw. „Katze" in der Abbildung oben auf S. 159. Als Eingabe erhält die KI Datensätze, denen bereits Label korrekt zugeordnet sind.
Maschinelles Lernen ordnet man KIs mit datenbasierten Ansätzen zu.
Bei **wissensbasierten Ansätzen** werden (Experten-)Wissen, Regeln oder Strategien z. B. in Tabellen und Entscheidungsbäumen gespeichert und angewendet bzw. durchsucht.
Datenbasierte Ansätze nutzen hingegen Datenbestände, um selbst z. B. Regeln für Label, Gruppierungen in den Daten oder vorteilhafte Aktionen zu finden (siehe verstärkendes, überwachtes und unüberwachtes Lernen S. 158/159).