### 1.1

1. Bitte grenzen Sie Kryptologie, Kryptografie und Kryptoanalyse voneinander ab.

*Kryptologie ist die Lehre und Wissenschaft der vertraulichen Nachrichtenübermittlung und umfasst die Kryptografie und die Kryptoanalyse. Kryptografie ist die Kunst des verborgenen oder geheimen Schreibens, d. h. Informationen so zu verändern, dass sie für alle anderen als die vorgesehenen Empfänger nicht mehr zu entziffern sind. Kryptoanalyse ist die Kunst, die verborgene Schrift zu entschlüsseln, also das Brechen von Chiffren, d. h. das Wiederherstellen oder Fälschen von verschlüsselten Informationen ohne Kenntnis des Schlüssels.*

1. Bitte unterscheiden Sie zwischen Kodierung und Verschlüsselung.

Sowohl bei der Verschlüsselung als auch bei der Kodierung werden Informationen in ein computerlesbares Format umgewandelt. Bei der Verschlüsselung ist diese Umwandlung jedoch ohne Kenntnis des Schlüssels nicht umkehrbar.

## 1.2

1. Bitte vervollständigen Sie den folgenden Satz: In der Praxis werden sensible Informationen durch \_\_\_\_ Fehler erlangt.
   * *menschliche* oder
   * kryptografische
2. Wofür steht CIA in der IT-Sicherheit?  
   *Confidentiality, Integrity und Availability.*
3. Bitte nennen Sie die fünf Säulen der Informationssicherheit.   
   *Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung und Nichtabstreitbarkeit von Informationen.*

## 1.3

1. Bitte nennen Sie die wichtigsten Epochen der Kryptografie.   
   *klassisches (Stift und Papier), elektromechanisches (Rotormaschine) und digitales Zeitalter.*
2. Wie viele mögliche Schlüssel gibt es bei einer Cäsar-Chiffre?   
   *26 einschließlich des trivialen Schlüssels.*
3. Bitte markieren Sie die richtige Antwort. Welches ist eine Substitutions-Chiffre?

* *Cäsar-Chiffre*
* Skytale   
  *Die Cäsar-Chiffre ist eine Substitutions-Chiffre und die Skytale ist eine Transpositions-Chiffre.*

1. Welches Manko haben alle Rotormaschinen?   
   *Da die Substitution buchstabenweise erfolgt, wird die Häufigkeit der Buchstaben beibehalten.*

## 1.4

1. Bitte nennen Sie zwei Algorithmen, die das Kerckhoffs‘sche Prinzip erfüllen.   
   *DES und AES.*
2. Was ist ein gutes Diffusionskriterium nach Shannon?   
   *Wenn sich ein Bit im Klartext oder Schlüssel ändert, ändert sich die Hälfte der Bits im Geheimtext.*

## 1.5

1. Bitte erklären Sie den Unterschied zwischen einer Prüfsumme und einer kryptografischen Hashfunktion.   
   *Bei einer kryptografischen Hashfunktion ist es nicht möglich, Kollisionen zu erzeugen.*
2. Bitte nennen Sie die typischen Einsatzzwecke für Prüfsummen.  
   *Fehlererkennung und -korrektur, z. B. Rauschen beim Lesen einer Compact Disc oder im Netzwerkverkehr, und vieles mehr.*
3. Bitte nennen Sie die typischen Einsatzzwecke für kryptografische Hashfunktionen.  
   *Korrektur von Veränderungen im Speicher- oder Netzwerkverkehr und vieles mehr.*
4. Nennen Sie bitte gängige kryptografische Hashfunktionen.   
   *Die MD- und die SHA-Familie.*

## 2.1

1. Für welche Abstände d ist die Cäsar-Chiffre auto-invers, d. h. die Ausgabe der Chiffrierung entspricht der Ausgabe der Dechiffrierung?   
   *Für* d = 0 *und* 13*.*
2. Erfüllt die Cäsar-Chiffre das Kerckhoffs‘sche Prinzip?   
   Nein, die Anzahl der möglichen Schlüssel ist zu gering.
3. Warum ist eine Substitutions-Chiffre unsicher?   
   Weil zwei gleiche Buchstaben im Klartext durch zwei gleiche Buchstaben im Geheimtext ersetzt werden.

## 2.2

1. Was unterscheidet eine Stromchiffre von einer Blockchiffre?   
   *Eine Stromchiffre arbeitet mit einzelnen Zeichen, während eine Blockchiffre mit Gruppen von Zeichen arbeitet.*
2. Was ist ein Substitutions- und Permutationsnetzwerk (oder eine Feistelchiffre)?   
   *Eine Blockchiffre, bei der jeder Block nach Hinzufügen eines Schlüssels iterativ substituiert und permutiert wird.*

## 2.3

1. Welche Schlüsselgröße kommt bei DES zum Einsatz?
   * 256 Bit
   * 128 Bit
   * 112 Bit
   * *56 Bit*
2. Nennen Sie eine kryptografische Schwäche von DES.   
   *Kurze Schlüssellänge.*
3. Wofür steht 3DES?   
   *Triple DES, d. h. dreifache Anwendung von DES*
4. Welche Schlüsselgröße wird bei 3DES verwendet?
   * 256 Bit
   * 128 Bit
   * *112 Bit*
   * 56 Bit

## 2.4

1. Wie viele Runden hat AES für einen 128-Bit-Schlüssel?
   * 8
   * 10
   * 12
   * 16
2. Welche Schritte werden in jeder Runde ausgeführt?   
   *SubBytes, ShiftRows, MixColumn und AddRoundKey.*
3. Welcher dieser Schritte ist nicht-linear?
   * *SubBytes*
   * ShiftRows
   * MixColumn
   * AddRoundKey

## 2.5

1. Was ist der Unterschied zwischen einer Prüfsumme und einer kryptografischen Hashfunktion?   
   *Nur bei einer kryptografischen Hashfunktion ist es nicht möglich, Kollisionen zu erzeugen.*
2. Bitte nennen Sie die typischen Einsatzzwecke von Hashfunktionen.   
   *Schnelle Datenabfragen, Identifizierung von Dateien (z. B. Virensuche), Fehlerkorrektur und -erkennung.*
3. Bitte nennen Sie die typischen Einsatzzwecke für kryptografische Hashfunktionen.   
   *Speicherung von Passwörtern, Authentifizierung von Nachrichten, Integritätsprüfungen.*
4. Bitte geben Sie die Rundenfunktionen an, die in AES für die Verschlüsselung verwendet werden.  
   *SubBytes*   
   *ShiftRows*  
   *MixColumns*  
   *AddRoundKey*

## 

## 3.1

1. Erklärt das Diffie-Hellman-Protokoll, wie eine Nachricht mit einem öffentlichen Schlüssel verschlüsselt und mit einem geheimen Schlüssel entschlüsselt werden kann?   
   *Nein, es wird nur erklärt, wie ein wechselseitig geheimer Schlüssel öffentlich aufgebaut wird.*

## 3.2

1. Welche mathematische Funktion wird zur Verschlüsselung beim RSA-Algorithmus verwendet?   
   *Potenzierung modulo einer zusammengesetzten ganzen Zahl.*
2. Welche mathematische Funktion wird zur Entschlüsselung beim RSA-Algorithmus verwendet?   
   *Wurzelbildung modulo einer zusammengesetzten ganzen Zahl.*
3. Wofür wird RSA heute hauptsächlich im Internet verwendet?   
   *Überprüfung von Zertifikaten.*

## 3.3

1. Wie viel älter ist RSA als ECC?   
   *Etwa 20 Jahre.*
2. Wie läuft der Diffie-Hellman-Schlüsselaustausch beim ECC im Vergleich zum ursprünglichen Diffie-Hellman-Schlüsselaustausch ab?   
   *Der Diffie-Hellman-Schlüsselaustausch beim ECC verwendet Punkte auf einer elliptischen Kurve, die durch Zahlenpaare gegeben sind, während der ursprüngliche Diffie-Hellman-Schlüsselaustausch einfache Zahlen verwendet.*
3. Wie sind die Schlüsselgrößen von RSA und ECC im Vergleich?   
   *2048 Bit für RSA und 224 Bit für ECC.*
4. Wie viel schneller ist ECC im Vergleich zu RSA?
   * 2
   * 3
   * *5*
   * 8

## 3.4

1. Wofür wird der private Schlüssel im Algorithmus für digitale Signaturen verwendet?   
   *Signieren durch Verschlüsselung.*
2. Wofür wird der öffentliche Schlüssel im Algorithmus für digitale Signaturen verwendet?   
   *Verifizierung durch Entschlüsselung.*

## 3.5

1. Welches Problem löst die Kryptografie mit öffentlichen Schlüsseln?

*Verteilen eines geheimen Schlüssels über einen offenen Kanal.*

1. Welches Problem löst die Kryptografie nicht mit öffentlichen Schlüsseln?

*Die Authentifizierung derer, denen der private Schlüssel gehört.*

1. Was sind zwei gängige Methoden gegen einen MITM-Angriff?

*Zertifizierungsstellen und Web of Trust.*

1. Was sind gängige Protokolle gegen einen MITM-Angriff?

*X.509 (wie von S/MIME verwendet) und OpenPGP.*

## 4.1

1. Welche Bedingungen muss ein sicheres und praktisches Passwort erfüllen?   
   *Leicht zu merken, aber schwer zu erraten.*
2. Bitte nennen Sie mindestens drei häufige Angriffsmethoden bei der Eingabe von Passwörtern durch andere Personen.

*Spionage, Keylogging und Login-Spoofing.*

1. Bitte nennen Sie die Vorteile der Authentifizierung durch das, was jemand weiß, gegenüber dem, was jemand ist.

*Sicher gespeichert, kann nicht gefälscht werden, erfordert keine spezielle Hardware.*

## 4.4

1. Was leistet FIDO2?   
   *Es standardisiert die Authentifizierung im Internet durch das, was jemand hat, z. B. einen USB-Stick oder ein Smartphone, anstatt durch das, was jemand weiß, z. B. ein Passwort.*
2. Welche Parteien sind an der Erstellung eines Kerberos-Tickets beteiligt, das ein Ticket vergibt?   
   *Der Client, der Authentifizierungsserver und der Ticketvergabeserver.*
3. Was ist der einzige Schwachpunkt in einem Kerberos-Netzwerk?   
   *Das Schlüsselverteilzentrum*

## 4.5

1. Bitte nennen Sie die Vorteile der Authentifizierung durch das, was jemand weiß, gegenüber dem, was jemand hat.

*Muss nicht mitgeführt werden, ist transparent gespeichert, kann nicht verloren gehen, gestohlen oder erpresst werden*

1. Bitte nennen Sie die Nachteile der Authentifizierung durch das, was jemand weiß, gegenüber dem, was jemand hat oder ist.

*Darf nicht vergessen werden, ist in der Komplexität begrenzt und kann aus der Ferne erlangt werden.*

## 4.6

1. Was wird unter der Anonymität eines Computers in einem Netzwerk verstanden?   
   *Dass die Identität des Computers in einem Netzwerk unbekannt ist.*

## 5.1

1. Was ist eine monoalphabetische Substitutions-Chiffre?   
   *Jeder Buchstabe im Klartext wird, unabhängig von seiner Position, durch einen anderen Buchstaben ersetzt.*
2. Welches Muster bewahrt eine monoalphabetische Substitutions-Chiffre?   
   *Unter anderem (einzelne) Buchstaben-, Bigramm- und Trigramm-Häufigkeiten.*
3. Welches Muster bewahrt eine Substitutions-Chiffre mit Homophonen?   
   *Die Häufigkeit von Buchstabenpaaren (Bigramme), Dreiergruppen (Trigramme)*

## 5.2

1. Welche minimale Schlüsselgröße wird derzeit als sicher für RSA und Diffie-Hellman empfohlen?
   * 512 Bit
   * 1024 Bit
   * *2048 Bit*
   * 4096 Bit
2. Welche minimale Schlüsselgröße wird derzeit für die Elliptic Curve Cryptography als sicher empfohlen?
   * 128 Bit
   * *256 Bit*
   * 512 Bit
   * 1024 Bit
3. Welche minimale Schlüsselgröße wird derzeit für AES als sicher empfohlen?
   * *112 Bit*
   * 128 Bit
   * 256 Bit
   * 1024 Bit

## 5.3

1. Warum ist eine doppelte Verschlüsselung mit unterschiedlichen Schlüsseln weniger sicher als eine dreifache Verschlüsselung?

*Weil der Meet-in-the-Middle-Angriff einen Speicher-Zeit-Kompromiss nutzt, um den verwendeten Schlüssel von* n *Bit in nur* 2n+1 *Verschlüsselungen zu finden.*

## 5.4

1. Bitte markieren Sie die richtige Antwort. Ist das One-Time-Pad in der Theorie vollkommen sicher?
   * *Ja*
   * Nein
2. Bitte markieren Sie die richtige Antwort. Welche theoretisch vollkommen sicheren Kryptosysteme sind bekannt?

*One-Time-Pad.*

1. Bitte markieren Sie die richtige Antwort. Ist das One-Time-Pad in der Praxis absolut sicher?
   * Ja
   * *Nein*
2. Was ist ein praktischer Nachteil des One-Time-Pad?   
   *Sein Schlüssel muss genauso lang sein wie der Klartext.*

## 5.5

1. Bitte nennen Sie Beispiele für Seitenkanalangriffe.   
   *Messungen der Rechenzeit, des Stromverbrauchs, der elektromagnetischen oder akustischen Emissionen.*

## 5.6

1. Was ist ein Differenzial in einem Substitutions- und Permutationsnetzwerk?   
   *Ein Paar* D = (ΔX, ΔY) *von Eingabe- bzw. Ausgabedifferenzen* ΔX *bzw.* ΔY*.*
2. Was ist ein Differenzpfad in einem Substitutions- und Permutationsnetzwerk?   
   *Ein Tupel von Differenzen* ΔU1*,* ΔU2*, ..., so dass jeder Eintrag* ΔUi *die Eingabe der S-Box der* i*-ten Verschlüsselungsrunde ist.*
3. Wie finden wir den wahrscheinlichsten Differenzpfad?   
   *Durch die Maximierung der Häufigkeiten, mit denen die S-Box die eingehende Differenz durch die ausgehende Differenz des Teildifferenzials ersetzt.*

## 6.1

1. Bitte nennen Sie die Schichten des OSI-Modells.  
   *Anwendungen, Darstellung, Sitzung, Transport, Vermittlung, Sicherung, Bitübertragung.*
2. Bitte nennen Sie die Schichten des DoD-Modells.  
   *Anwendungen, Transport, Internet, Netzwerkzugang.*
3. Bitte geben Sie Beispielprotokolle für die ersten fünf Schichten des OSI-Modells an.   
   *HTTP, SOCKS, TCP, IP, Ethernet, UDP.*
4. Bitte liefern Sie Beispielprotokolle für jede Schicht des DoD-Modells.   
   *HTTP, TCP, IP, Ethernet.*

## 6.2

1. Auf welcher Schicht des DoD-Modells befindet sich das IPsec-Protokoll?

* 1.
* *2.*
* 3.
* 4.

1. Welche Transportprotokolle liegen dem IPsec-Protokoll zugrunde?

* TCP
* UDP
* TLS
* HTTPS

1. Welches dieser beiden Protokolle ist das schnellere, aber weniger zuverlässige?

* TCP
* UDP

1. Wie viele Ports verwendet IPsec zur Herstellung einer sicheren Verbindung?

* 1
* 2
* *3*
* 4

## 6.3

1. Über welchen Schichten des OSI-Modells befindet sich TSL?   
   *1., 2., 3., und 4. Schicht.*
2. Über welchen Schichten des IP- (oder DoD-) Modells befindet sich TSL?   
   *1., 2., 3., und 4. Schicht.*
3. Bitte nennen Sie die kryptografischen Algorithmen, die während des TLS-Handshakes vereinbart werden und nennen Sie deren Zwecke.

*Ein asymmetrischer Algorithmus (wie RSA) zur Authentifizierung und zum Austausch der Schlüssel, ein symmetrischer Algorithmus wie AES zur Verschlüsselung der Verbindung und ein kryptografischer Hash-Algorithmus wie SHA256.*

## 6.4

1. Wie steht es um die Sicherheit von E-Mails über TLS im Vergleich zu S/MIME und OpenPGP?   
   *TLS verschlüsselt nur während des Transports (aber nicht an Knotenpunkten), während S/MIME und OpenPGP von Ende zu Ende verschlüsseln.*
2. Wie sieht es mit der Authentifizierung zum Aufbau von Vertrauen zwischen S/MIME und OpenPGP aus?   
   *S/MIME vertraut auf Zertifizierungsstellen, während OpenPGP nur auf persönlich autorisierte Schlüssel vertraut.*
3. Für welche Art von Angriff ist der automatische Schlüsselaustausch über das OpenPGP-Protokoll anfällig?  
   *Man-in-the-Middle-Angriff.*
4. Welche Art von Sicherheit bietet der automatische Schlüsselaustausch über das OpenPGP-Protokoll?   
   *Opportunistische Sicherheit, die meiste Zeit etwas Schutz.*

## 6.5

1. Welche Daten verraten den Server, den Benutzende besucht haben, außer seiner DNS-Anfrage?

*Die IP-Adresse*, *im HTTPS-Protokoll die Server Name Indication (SNI)*, *und im HTTP-Protokoll das Header-Feld Host*.

1. Bitte nennen Sie drei Protokolle zum sicheren Nachschlagen von Domainnamen

*DNSCrypt-Protokoll*,*dNS-over-TLS (oder DoT), DNS-Auflösung über TLS*, und *DNS-over-HTTPS (oder DoH), DNS-Auflösung über HTTPS**.*

## 7.1

1. Was ist charakteristisch für ein von einem Computer erzeugtes Geheimnis?  
   *Für ein Geheimnis ist es notwendig, dass die Ausgabe der Generierung unvorhersehbar ist, und da der Generierungsalgorithmus in der Regel bekannt ist, muss auch seine Eingabe unvorhersehbar sein.*
2. Nennen Sie mindestens drei Verwendungsmöglichkeiten von Zufallszahlen zur Schlüsselgenerierung.

*rein zufälliger Schlüssel*

*langer Schlüssel*

*speziell formatierter Schlüssel*

*automatisch generierter Schlüssel*

## 7.2

1. Bitte nennen Sie drei Arten von Algorithmen, die im Zuge der Einführung von Quantencomputern als sicher gelten.
   * *symmetrischer kryptografischer Algorithmus*
   * *gitterbasierter kryptografischer Algorithmus*
   * *kryptografischer Algorithmus auf der Basis von fehlerkorrigierenden Codes*
   * *kryptografischer Algorithmus auf der Basis von Hashfunktionen*

## 7.3

1. Bitte markieren Sie die richtige Antwort. Um eine Nachricht zu authentifizieren und zu verschlüsseln, sollte sie
   * gemeinsam authentifiziert und verschlüsselt werden.
   * zuerst authentifiziert und dann verschlüsselt werden.
   * *zuerst verschlüsselt und dann authentifiziert werden.*
2. Bitte markieren Sie die richtige Antwort. Kryptografische Funktionen sollten
   * neu implementiert werden.
   * *wiederverwendet werden.*
3. Bitte markieren Sie die richtige Antwort. Welche kryptografische Hashfunktion sollte *nicht* für die Speicherung von Passwörtern verwendet werden?
   * bcrypt
   * scrypt
   * PBKDF2
   * *MD5*

## 7.4

1. Wie dürfen persönliche Daten gesammelt werden?

*Mit einem klaren Ziel und der ausdrücklichen Zustimmung der Person.*

1. Bitte nennen Sie mindestens drei Beispiele für besonders geschützte persönliche Daten.

*ethnische Herkunft, politische Meinungen, religiöse Überzeugungen und biometrische Daten, wie z. B. Gendaten und Gesundheitsdaten.*

## 8.1

1. Bitte markieren Sie die richtige Antwort. Welches TAN-Verfahren ist resistent gegen Phishing- und Man-in-the-Middle-Angriffe?

* *Einfache TAN*
* *Mobile TAN (mTAN)*
* *Indizierte TAN (iTAN)*

1. Bitte nennen Sie die Rollen, die ein Kunde bei FinTS-Geschäftstransaktionen übernehmen kann.

*Aussteller, Bote, Zeuge oder Intermediär.*

## 8.2

1. Wie viele Transaktionen enthält ein Block der Bitcoin-Blockchain im Durchschnitt?

* *1000*
* *2000*
* *100 000*
* *1 000 000*

1. Wie lange dauert derzeit das Hinzufügen eines Blocks zur Bitcoin-Blockchain auf einem normalen Computer mindestens?

* *1 000 Stunden*
* *1 000 Tage*
* *1 000 000 Jahre*
* *1 000 000 000 Jahre*

1. Bitte nennen Sie drei Kriterien, die ein durchgängig von Wählenden überprüfbares Wahlsystem erfüllen sollte.

*Vertraulichkeit*

*Authentizität*

*Integrität*

*Anonymität*

*Rückverfolgbarkeit*

1. Welche Wahlschritte sollten in einem durchgängig verifizierbaren Wahlsystem von Wählenden verifizierbar sein.
2. Ob die Stimme

*wie vorgesehen abgegeben wurde*,

*wie abgegeben registriert wurde* und

*wie registriert gezählt wurde*.

## 8.4

1. Wie unterscheidet sich die Steganografie von der Kryptografie?

*Im Griechischen bedeutet steganos „verdecken“, während krypto „verstecken“ bedeutet. Bei der Steganografie wird eine geheime Nachricht durch eine einfache Nachricht verdeckt; bei der Kryptografie wird der Inhalt reversibel verschlüsselt.*

1. Bitte geben Sie ein Beispiel für das Verstecken von Informationen (eine Nachricht, ein Bitstrom) in einem Bild.

*Die Ersetzung des niedrigstwertigen Bits*

## 8.5

1. Wie oft verschlüsselt ein Client ein Paket, bevor er es über zehn Knoten in einem Tor-Netzwerk an den Server schickt?

*Der Client verschlüsselt es so oft, wie es Knoten gibt, also zehn Mal.*

1. Bitte vervollständigen Sie den folgenden Satz.

Onion Routing ist eineKette, in der jeder Knoten nur *seinen unmittelbaren Vorgänger und Nachfolger* kennt und in der der gesamte Datenverkehr zwischen den beiden Endpunkten für *jeden Knoten außer den Endpunkten* nicht zu entziffern ist*.*