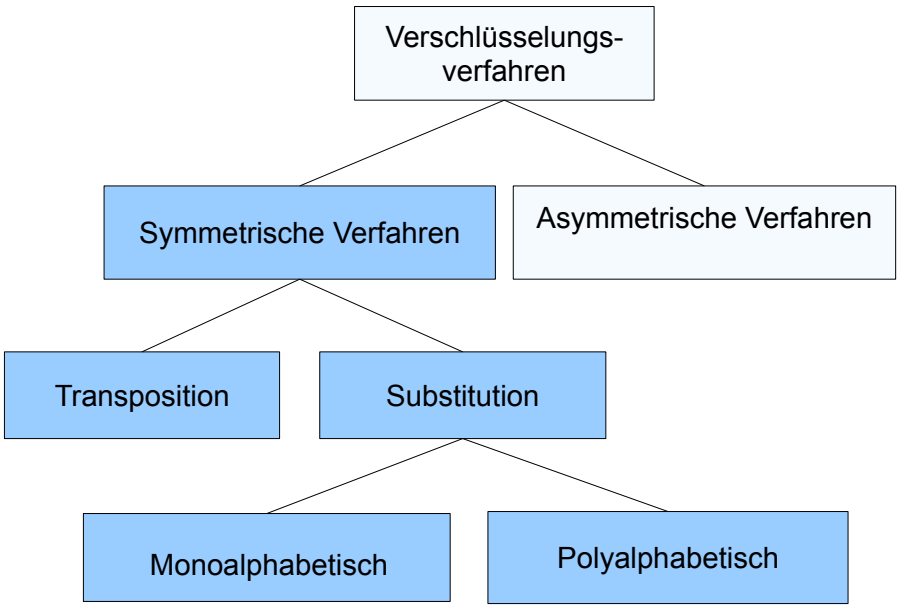
Vergleich der Krypto-Verfahren - Lösung

Aufgaben:

1. WDH aus Klasse 8:



Symmetrische Verfahren: Ver- und Entschlüssler haben den gleichen Schlüssel. Die Nachricht wird mit dem gleichen Schlüssel ver- und entschlüsselt.
Bsp.: AES, alle unten stehenden

Asymmetrische Verfahren: Sender und Empfänger haben verschiedene Schlüssel.
Bsp.: RSA

Transpositionsverfahren: Die Buchstaben des Klartextes werden durch die Verschlüsselung anders angeordnet.
Bsp.: Skytale, (Fleißner, Gartenzaun)

Substitutionsverfahren: Die Buchstaben des Klartextes werden bei der Verschlüsselung durch andere Buchstaben (oder Zeichen) ersetzt.
Bsp.: Caesar, Substitutionschiffre, Vigenère, One-Time-Pad

Monoalphabetische Substitution: ein Substitutionsverfahren, bei dem nur ein einziges Schlüsselalphabet verwendet wird.
Bsp.: Caesar, Substitutionschiffre, alle Varianten von Cäsar, RSA (wenn man es fälschlicherweise auf einzelne Buchstaben anwendet).

Polyalphabetische Substitution: ein Substitutionsverfahren, bei dem mehrere Schlüsselalphabete verwendet werden.
Bsp.: Vigenère, One-Time-Pad

2.

Verfahren	(Wie) kann es gebrochen werden? z.B. Anzahl der Möglichkeiten bei brute force etc.	Bewertung: wie sicher ist das Verfahren?
Skytale	Brute force: n Möglichkeiten (bei einer Nachricht der Länge n)	sehr unsicher
Cäsar-Verfahren	Brute force: 25 Möglichkeiten Oder: Häufigkeitsanalyse (1 Buchstabe genügt)	sehr unsicher
Cäsar mit zufälliger Anordnung der Buchstaben	Brute force: (n-1)! Möglichkeiten (bei einer Nachricht der Länge n) Aber leicht zu brechen mit: Häufigkeitsanalyse (über alle Buchstaben)	(sehr) unsicher
Vigenère-Verfahren	a) Schlüssellänge ermitteln: z.B.Kasiski Test b) Je Gruppe: Häufigkeitsanalyse (1 Buchstabe genügt)	unsicher
One-Time-Pad OTP	Absolut sicher! Selbst mit Brute force nicht zu brechen. Aber: Da der Schlüssel genauso lang sein muss wie die Nachricht, nur einmal verwendet werden darf, und auf einem sicheren Weg übermittelt werden muss, dann kann man über diesen Weg auch gleich die Nachricht selber übermitteln.	Sehr sicher, aber unpraktikabel
AES	Mathematisch ist AES mit brute force zu brechen, aber wenn der Schlüssel entsprechend lang ist, ist es nicht in vertretbarem Zeitaufwand machbar (zumindest mit den zur Zeit zur Verfügung stehenden Rechnern). Problem: Schlüsseltausch	Zur Zeit sicher, bis auf Schlüs-seltausch
RSA	Wählt man ausreichend große Zahlen, dann lassen sie sich nicht in einer akzeptablen Zeit in ihre Primfaktoren zerlegen (zumindest mit den zur Zeit zur Verfügung stehenden Rechnern). Nachteil: Asymmetrische Verschlüsselung ist viel langsamer als symmetrische. Sinnvoll also nur bei kleinen Datenmengen. Problematisch: Vertrauen in Zertifizierungsinstanzen nötig	Zur Zeit sicher

Hybrid-verfahren	Mittels RSA wird ein (zufälliger) symmetrischer Schlüssel getauscht (→ langsam, aber nur kleines Datenvolumen). Danach wird mit dem symmetrischen Schlüssel verschlüsselt - z.B. mittels AES.	Zur Zeit sicher

3. a) 2000 Bit (vom BSI empfohlen bis zum Jahr 2022, danach 3000 Bit)

b) Mindestens 128 Bit (z.B. AES-128, AES-192, AES-256)

Quelle: BSI[1]

1 *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf;jsessionid=4D2998F7DAF2C44ED7836F2D7164AA1E.1_cid503?__blob=publicationFile&v=12* (abgerufen 14.5.20)