**(Vgl. FAS07 FQ)**Ordnen Sie die Vor- und Nachteile der symmetrischen und asymmetrischen Verschlüsselung zu.

a) Sie bieten elegante Lösungen für die Schlüsselverteilung in Netzen, da die öffentlichen Schlüssel bzw. Schlüsselzertifikate frei zugänglich auf zentralen Servern gespeichert werden können, ohne die Sicherheit des Verfahrens zu beeinträchtigen.
b) Die Sicherheit ist im wesentlichen durch die Schlüssellänge festgelegt, d. h. es sollte keine Attacken geben, die wesentlich besser sind als das Durchprobieren aller Schlüssel (Brute- Force-Attacken).
c) Es gibt wesentlich bessere Attacken als das Durchprobieren aller Schlüssel, deshalb werden relativ lange Schlüssel benötigt, um ein gleich hohes Maß an Sicherheit zu erreichen.
d) Sie bieten hohe Sicherheit bei relativ kurzem Schlüssel.
e) Die Schlüsselerzeugung ist einfach, da gewöhnlich als Schlüssel jede Bitfolge einer festen Länge erlaubt ist und als Schlüssel eine Zufallszahl gewählt werden kann.
f) Jeder Teilnehmer muss sämtliche Schlüssel seiner Kommunikationspartner geheim halten.
g) Zur Schlüsselverteilung sind sie weniger gut geeignet, insbesondere bei einer großen Anzahl von Kommunikationspartnern.
h) Jeder Teilnehmer einer vertraulichen Kommunikation muss nur seinen eigenen privaten Schlüssel geheim halten.
i) Sie sind schnell, d. h. sie haben einen hohen Datendurchsatz.
j) Sie lassen sich einfach für digitale Signaturen benutzen.
k) Sie sind langsam, d. h. sie haben im allgemeinen einen geringen Datendurchsatz.
l) Die Schlüsselerzeugung ist i. allg. komplex und aufwendig, da die Erzeugung "schwacher" Schlüsselpaare vermieden werden muss.

| | Vorteil | Nachteil |
|---|---|---|
| **Symmetrische Verschlüsselung**<br>128 - 256 AES | i, e, b, d | f, [redacted], g |
| **Asymmetrische Verschlüsselung**<br>2048 - 4096 RSA | a, [redacted], h, j | k, l, [redacted], c |