**Die Asymmetrische Verschlüsselung**

Anhand der Caesar-Verschlüsselung wurde gezeigt, wie einfach diese Art der Verschlüsselung zu knacken ist. Jeder ist in der Lage, mit dem benutzten Schlüssel zu ver- und entschlüsseln.

Abhilfe schafft das von Whitfield Diffie und Martin Hellman entworfene asymmetrische Verfahren. Hierzu wird ein eindeutig zugeordnetes Schlüsselpaar verwendet. Im Folgendem wird das Wort Lehrerfortbildung mit dem Schlüssel YZS verschlüsselt.

Schlüssel: YZSYZSYZSYZSYZSYZ  
Klartext: Lehrerfortbildung  
Geheimtext: I-S.-USWUOEYIJPYC

1. Überprüfe, ob der Klartext richtig verschlüsselt worden ist.
2. Entschlüssle den entstandenen Geheimtext mit dem gleichen Schlüssel. Beschreibe, was du feststellt.
3. Benutze den Schlüssel VCT zum Entschlüsseln. Beschreibe, was du feststellst.
4. Wende die Ver- und Entschlüsselung mit dem Schlüsselpaar VDB und YGF an.
5. Erkläre das Verfahren. Nehme Bezug auf die Caesar-Verschlüsselung.