Aufgabe 3

Das Programm Pretty Good Privacy (PGP), das zum Beispiel zur Verschlüsselung privater E-Mails benutzt werden kann, verwendet ein Hybrid-Verfahren aus symmetrischer und asymmetrischer Verschlüsselung.

a) Erläutern Sie das Prinzip symmetrischer und asymmetrischer Verschlüsselungsverfahren.
Erklären Sie, worauf jeweils die Sicherheit beruht.
Erklären Sie als Beispiel eines symmetrischen Verfahrens die Verschlüsselung nach Vigenère.

b) Bei einer symmetrischen Blockchiffrierung, wie etwa dem Data Encryption Standard (DES), werden genau wie bei den klassischen Chiffrierverfahren Substitutionen (Ersetzungen) und Transpositionen (Vertauschungen) verwandt.
Verschlüsseln Sie die Nachricht GELD mit dem folgenden Algorithmus, der Ähnlichkeiten mit dem DES-Verfahren aufweist:

   (1) Ordnen Sie den Buchstaben ihren binären ASCII-Wert zu (siehe Material).

   (2) Fassen Sie jeweils zwei Buchstaben in einem 16-Bit-Block zusammen.

   (3) Vertauschen Sie die zweiten vier Bits mit den letzten vier Bits des jeweiligen Blocks.

   (4) Verschlüsseln Sie jeden Block mit dem 16-Bit-Schlüssel „0001011100010110“, indem Sie den zu verschlüsselnden Block mit dem Schlüssel durch eine XOR-Operation bitweise verknüpfen.

   (5) Wandeln Sie die entstandenen Blöcke mithilfe des ASCII-Codes in Buchstaben um.

   Erläutern Sie, wie sich die Nachricht wieder entschlüsseln lässt.

c) Bei PGP werden das DES- und ein asymmetrisches Verfahren (z. B. RSA-Verfahren) kombiniert. Erklären Sie, wie sich die beiden Verfahren sinnvoll kombinieren lassen, und erläutern Sie, worin der Vorteil der Kombination der beiden Verfahren liegt.

Zu Aufgabe 3

Auszug aus der ASCII-Tabelle

Buchstabe	Dezimal	Binär	Buchstabe	Dezimal	Binär
A	65	01000001	N	78	01001110
B	66	01000010	O	79	01001111
C	67	01000011	P	80	01010000
D	68	01000100	Q	81	01010001
E	69	01000101	R	82	01010010
F	70	01000110	S	83	01010011
G	71	01000111	T	84	01010100
H	72	01001000	U	85	01010101
I	73	01001001	V	86	01010110
J	74	01001010	W	87	01010111
K	75	01001011	X	88	01011000
L	76	01001100	Y	89	01011001
M	77	01001101	Z	90	01011010

Abbildung 3.1