2. Aufgabenstellung (so wie sie dem Prüfling vorgelegt wird):

Kryptologie

Aufgabe 1:
Im Kloster Marienbrunnen in Sachsen herrscht eine strenge Schweigepflicht. Elektronische Kommunikationsmedien sind seit jeher verboten. Die beiden Ordensbrüder Thomas und Philipp haben jedoch ein brisantes Thema zu diskutieren, bei dem es um die Zukunft des Klosters geht. Aus Angst, dass ihre schriftliche Kommunikation abgefangen werden könnte, leihen sie sich in der Bibliothek ein Buch über Kryptologie aus.

a) Nennen Sie die beiden Teilgebiete der Kryptologie und beschreiben Sie kurz deren Aufgabengebiet.

b) Ihre erste Nachricht tauschen die Ordensbrüder, über mit Zitronensaft beschriebene Servietten aus. Nach dem Erhitzen steht auf der Serviette von Thomas:
whvw 3 (a b c d e f g h i j k l m n o p q r s t u v w x y z)
Dechiffrieren Sie zuerst die Nachricht. Nennen und charakterisieren Sie im Anschluss das eingesetzte Verfahren.

c) Einen Teil des Prozesses aus 1b) haben Thomas und Philipp thematisch sicher nicht dem Kryptologiebuch entnommen. Begründen Sie diese Aussage.

d) Um ihre Kommunikation sicherer zu machen chiffrieren die beiden ihre Nachrichten nun doppelt. Diskutieren Sie die Sinnhaftigkeit dieser Maßnahme.

Aufgabe 2:
Mittlerweile kennen und nutzen die beiden das sicherere Vigenere-Verfahren.

a) Entschlüsseln Sie, mit dem beiliegenden Vigenere-Quadrat, die untenstehende Nachricht und stellen Sie dar, warum das Verfahren sicherer ist, als das in Aufgabe 1.

Geheimtext:	w t l q a m
Schlüssel:	h i
Klartext:	_ _ _ _ _ _

b) Nennen Sie eine Möglichkeit, um die Verschlüsselung in 2a) zu optimieren und begründen Sie ihre Antwort.

c) Ein Drittes Ordensmitglied hat durch Zufall die Schlüssellänge herausgefunden und ist sich nun sicher, die Verschlüsselung knacken zu können. Positionieren Sie sich zu dieser Annahme.

Aufgabe 3:
Mittlerweile finden solch klassische Verschlüsselungsverfahren, wie sie die Mönche in Aufgabe 1 und 2 benutzt haben, kaum noch Anwendung, da sich ihre Sicherheit meist auf den dahinter liegenden Algorithmus beschränkt.

a) Nennen Sie den Namen des Prinzips, welches diese Veränderung maßgeblich einläutete und erklären Sie kurz dessen Inhalt.

b) Ein klassisches modernes Hybrid-Verfahren ist das PGP Verfahren, wie es hier nicht ganz korrekt skizziert ist. Zeigen Sie die Stelle, an der das Schema nicht stimmt und stellen Sie knapp den korrekten Ablauf dar.