Arbeitsauftrag Informatik

Name: **Vorname:** **Klasse:**

Asymmetrische Verschlüsselung mit ASYM-Kodierer

1) Behauptung: Mit dem Schlüssel `AZS` wurde `EC-CARD` zu `JVQFQUH` verschlüsselt. Prüfen Sie die Aussage durch Verschlüsseln des Klartextes/Entschlüsseln des Geheimtextes.

Verschlüsseln							
Schlüssel	A	Z	S	A	Z	S	A
Klartext	E	C	-	C	A	R	D
Geheimtext							

Entschlüsseln							
Schlüssel	A	Z	S	A	Z	S	A
Geheimtext	J	V	Q	F	Q	U	H
Klartext							

2) Nutzen Sie nun den Schlüssel `PCT`. Prüfen Sie erneut die Aussage.

Verschlüsseln							
Schlüssel	P	C	T	P	C	T	P
Klartext	E	C	-	C	A	R	D
Geheimtext							

Entschlüsseln							
Schlüssel	P	C	T	P	C	T	P
Geheimtext	J	V	Q	F	Q	U	H
Klartext							

3) Beschreiben Sie das Vorgehen zum korrekten Ver- und Entschlüsseln.

4) Die Nutzerin Alice möchte bei der Bob AG erstmals eine Bestellung auslösen und muss dazu ihre Kreditkartennummer 81 übermitteln. Tragen Sie auf den Pfeilen die Kommunikationsdaten ein. Ergänzen Sie die Ver- und Entschlüsselung.

Alice

Bob AG
public key: BGF
private key: FDB

Wie lautet Ihr öffentlicher Schlüssel? →

← public key Bob AG: _____

Ich verschlüssle ACHTEINS und sende es! →

Ich entschlüssle!
Ergebnis: _____
Ich verschlüssle `OK` mit private key:
Ergebnis: _____
Ich sende `OK` und verschlüsseltes OK!

← Ich entschlüssle zweites Wort
Ergebnis: _____
Prüfe, ob Wort 1 = Wort 2

Die Kommunikation zeigt **zwei grundlegende Prinzipen** des asymmetrischen Verfahrens. Neben der **Ver-/Entschlüsselung** ist es möglich, **Nachrichten** digital zu **unterschreiben**. Dazu wird die Nachricht mit dem eigenen privaten Schlüssel verschlüsselt und dieser Geheimtext zusammen mit der Nachricht übermittelt. Jeder kann nun den verschlüsselten Teil der Nachricht mit dem öffentlichen Schlüssel des Absenders decodieren, mit der Ausgangsnachricht verifizieren und so prüfen, ob die Nachricht auch von ihm stammt.