Asymmetrische Verschlüsselung

Das einzige, absolut sichere Verfahren One Time Pad hat die Nachteile, das Schlüssellänge und Klartextlänge identisch sein müssen, der Schlüssel nur einmal benutzt werden darf und er aus einer zufälligen Buchstabenfolgen bestehen muss. Wenn man aber bei einem Internet-Versandhändler erstmalig bestellt und dort die Bankdaten hinterlegen möchte, sollte dies verschlüsselt geschehen. Ein **gemeinsamer** Schlüssel existiert aber nicht! Gesucht ist also ein Verfahren, das trotzdem eine sichere Kommunikation ermöglicht.

Versuch mit dem Werkzeug ASYM-Kodierer (aus GALLENBACHER: Abenteuer Informatik):
Behauptung: Mit dem Schlüssel `AZS` wurde `EC-CARD` zu `JVQFQUH` verschlüsselt.

1) Schneide den Schieber vom ASYM-Kodierer aus. Den Streifen in der Mitte entfernt man mit der Schere am besten, indem man das Blatt leicht faltet.

2) Prüfe die Aussage durch Verschlüsseln des Klartextes/Entschlüsseln des Geheimtextes Vergleiche dein Ergebnis mit deinem Sitznachbarn.

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							

3) Nutze nun den Schlüssel `PCT`. Prüfe erneut die Aussage und vergleiche mit deinem Sitznachbarn.

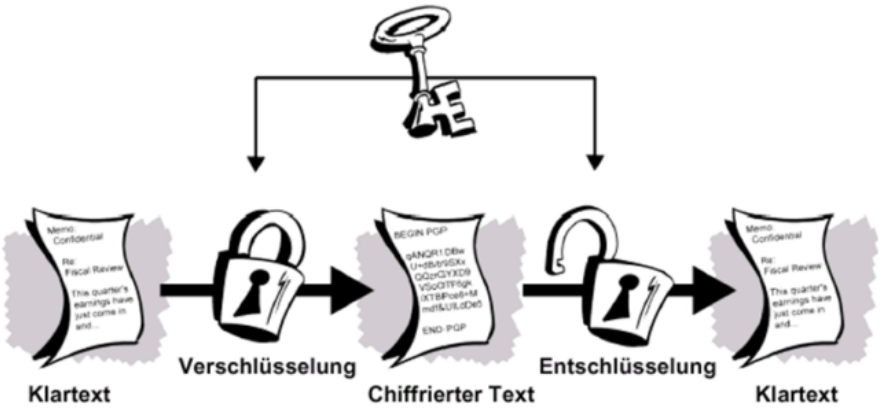
Verschlüsseln							
Schlüssel	P	C	T	P	C	T	P
Klartext	E	C	-	C	A	R	D
Geheimtext							

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

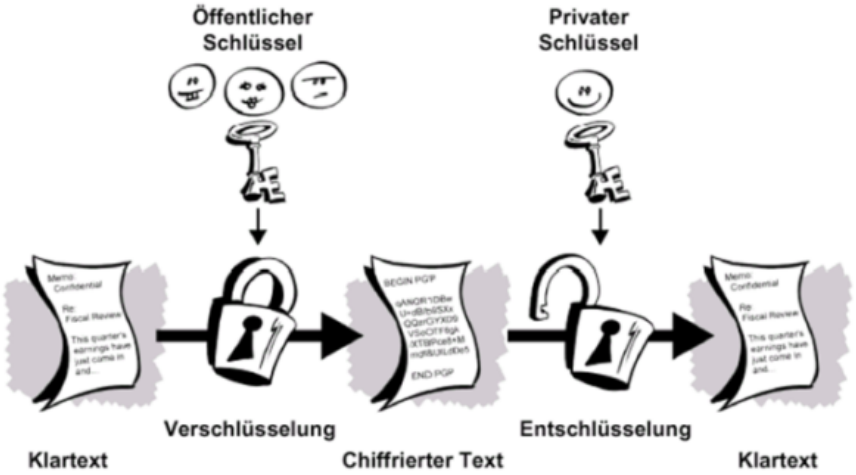
4) Beschreibe das Vorgehen zum korrekten Ver- und Entschlüsseln stichpunktartig in deinem Hefter.

5) Entscheide und begründe, ob die Sicherheitsziele Vertraulichkeit, Integrität und Authentizität mit dem ASYM-Kodierer erreicht werden. Halte deine Ergebnisse stichpunktartig im Hefter fest.

Für das Ver- und Entschlüsseln werden **verschiedene** Schlüssel benutzt. Man bezeichnet das Prinzip als asymmetrisches Verfahren oder auch Public-Key-Verfahren, die Schlüssel als privat und öffentlich. Der private Schlüssel ist geheim und nur seinem Besitzer bekannt. Der öffentliche Schlüssel wird vom Besitzer z. B. im Internet bekannt gegeben. Beide Schlüssel werden so berechnet, dass aus einem Teil nicht der andere ermittelt werden kann. Die Regeln zur Schlüsselbestimmung und Anwendung sind komplexe mathematische Verfahren unter Benutzung riesiger Primzahlen.



symmetrisches Verfahren



asymmetrisches Verfahren

Quelle: Network Associates Inc. (Hrsg.): Handbuch "Einführung in die Kryptographie", Bestandteil des Softwarepaketes PGP Ver. 6.5.1. deutsch, Datei „IntroToCrypto.pdf".