Arbeitsauftrag Informatik
Name: **Vorname:** **Klasse:**

Die Verschlüsselungsverfahren von POLYBIOS und PLAYFAIR

POLYBIOS-Verfahren

Eine mögliche Geschichte: Archäologen fanden bei Ausgrabungen verschiedenen Papyrusrollen des Griechen POLYBIOS (* 200 v. Chr.; † 120 v. Chr.). Diese enthielten unter anderem das nebenstehende Quadrat als auch den Geheimtext δα δε βγ αα αγ γε δβ αα δγ. Ihnen war schnell klar, dass es sich um ein Verschlüsselungsverfahren handeln muss.

	α	β	γ	δ	ε
α	A	B	Γ	Δ	E
β	Z	H	Θ	I	K
γ	Λ	M	N	Ξ	O
δ	Π	P	Σ	T	Y
ε	Φ	X	Ψ	Ω	

1) Versuche den **griechischen** Klartext zu bestimmen. Nutze ggf. das Tafelwerk.
2) Beschreibe das Prinzip des Verfahrens.
3) Übertrage das Verfahren ins Deutsche. Nutze als Geheimzeichen die Zahlen 1 bis 5. Setze die Klarbuchstaben I = J, um mit 25 Feldern auszukommen.
4) Verschlüssle den aus dem Griechischen stammende Ausspruch „Arzt, heil dich selbst“.

Um eine Entschlüsselung zu erschweren, kann man die Reihenfolge der Buchstaben durch ein Schlüsselwort verändern.

5) Erstelle das POLYBIOS-Quadrat mit dem Schlüsselwort `UNIVERSITÄT ROSTOCK`.
6) Sendet deinem Partner eine verschlüsselte Nachricht mit der Angabe zu einer geplanten Wochenendaktivität.

PLAYFAIR

Fast 2000 Jahr nach POLYBIOS entwickelt der englische Physiker CHARLES WHEATSTONE das nach seinem Bekannten, BARON PLAYFAIR VON ST. ANDREWS, benannte Verfahren. Bei PLAYFAIR wird das Klartextalphabet quadratisch angeordnet und der Klartext in Buchstabenpaare zerlegt. Paare aus gleichen Buchstaben oder übrig gebliebene Buchstaben müssen jedoch mit Füllzeichen verändert werden. Anschließend kann die paarweise Verschlüsselung beginnen.

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

Klartext: `TREFFPUNKT GASSE` → `TR EF FP UN KT GA SX SE`

Geheimtext: `US AK KL SP IU FB XC UC`

7) Ermittle die Verschlüsselungsregeln für PLAYFAIR. Unterteile in die Fälle (A) beide Buchstaben stehen in der gleichen Zeile, (B) beide Buchstaben stehen in der gleichen Spalte, (C) die Buchstaben stehen in unterschiedlichen Zeilen und Spalten.
8) Entschlüssle den Geheimtext `PB UG YM SU CA PS UY CP` und erläutere die Bedeutung des Klartextes.