

2. Übung zur Vorlesung Kryptographie

Achtung 1: Der Text im Skriptum auf S. 16 oben ist „selbsterklärend“ („man muss aufpassen!“). $\pi(2) = 5$ bedeutet, dass die alte Position 5 (und nicht 2) auf die neue Position 2 (und nicht 5) gebracht wird.

Achtung 2: Ausgabetermin des 3. Übungsblattes ist Freitag, der 30.4.2004, in der Vorlesung, und **Rückgabetermin ist der 7. Mai 2004, ebenfalls in der Vorlesung.**

(Grund: dann liegen am Montag beim Besprechungstermin die korrigierten Fassungen vor.)

Achtung 3: Die Übung am Montag, dem 3. Mai 2004, findet von 10 bis 12 **im HS F (A10 1-121)** (nicht mehr im A5 1-160) statt.

Achtung 4: Auch für die Vorlesung am Freitag suche ich eine Raumtauschmöglichkeit. Beobachten Sie dazu die Webpage(s).

Aufgabe 6: Eulersche Φ -Funktion (2+4 Punkte)

- (a) Berechnen Sie $\Phi(28)$, $\Phi(33)$, $\Phi(35)$ und $\Phi(5^3)$.
- (b) Es seien p eine Primzahl und e eine ganze Zahl größer gleich 0.
Zeigen Sie (oder begründen Sie stichhaltig), dass $\Phi(p^e) = p^{e-1} \cdot (p - 1)$ gilt.

Aufgabe 7: Kryptanalyse (2 Punkte)

Der folgende Chiffretext wurde mit Hilfe einer Permutationschiffre π der Blocklänge 8 verschlüsselt:

EGOMNSTRAHNUTGODMMDLUNDI

Von der Funktion π kennen Sie $\pi(1) = 5$, $\pi(2) = (4)$, $\pi(3) = (2)$, $\pi(4) = (1)$. Finden Sie den Klartext und den Rest von π .

Aufgabe 8: Untergruppen (4 Punkte)

Geben Sie *alle* Untergruppen von $(\mathbb{Z}_{13}^*, \cdot)$ an.

Aufgabe 9: Extended-Euclid und Lösung modularer Gleichungen (4+4 Punkte)

- (a) Welches Tripel $(d, x, y) \in \mathbb{Z}^3$ wird durch den Aufruf von `extended_euclid(899, 493)` zurückgegeben?
- (b) Finden Sie *alle* Lösungen von $35x \equiv 10 \pmod{50}$.