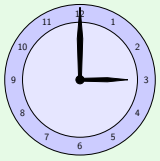
# Modulo-Rechnung

## Schlüsselaustausch

*Modulo* ist eine Rechenoperation (wie z. B. Addition oder Multiplikation). Sie wird für zahlreiche Verschlüsselungsverfahren und auch für Schlüsselaustausch-Verfahren benötigt.
Mit Modulo, **mod**, wird der Rest der ganzzahligen Division bezeichnet.

Bei der Modulo-Operation muss etwas gerechnet werden.
Sie ist aber leicht zu verstehen.

**Beispiel**



Jeder von uns benutzt fast täglich die Modulo-Rechnung. Die kommt nämlich bei der Berechnung der Uhrzeit vor. Wir sagen zu der Uhrzeit 15:00 Uhr meist 3 Uhr (nachmittags). Das ist die Modulo-Rechnung mit der Zahl 12: $15\ mod\ 12\ =\ 3$, da $15\ :\ 12\ =\ 1,\quad \mathbf{3}$ bleibt übrig.

Natürlich rechnet man nicht immer $mod\ 12$. $12$ kann durch jede ganze Zahl ersetzt werden. Bei den meisten Verschlüsselungsverfahren kommen keine negativen Zahlen vor, das macht es etwas einfacher.

**Beispiel**

Rechnungen

$18\ \ mod\ \ 5\ =\ 3$ , da $18\ :\ 5\ =\ 3$ **(Rest 3)**

$10\ \ mod\ \ 4\ =\ 2$ , da $10\ :\ 4\ =\ 2$ **(Rest 2)**

$14\ \ mod\ \ 7\ =\ 0$ , da $14\ :\ 7\ =\ 2$ **(Rest 0)**





v2 11. April 2012