Zusatzaufgaben zu TigerJython

Zusatzaufgaben zu 10.5

Aufgabe 5: Erstelle ein Programm, das die Häufigkeiten der Buchstaben A-Z in einem Text (Textdatei) zählt und als Liste ausgibt. Es kann angenommen werden, dass der Text nur Grossbuchstaben und das Leerzeichen enthält.

Aufgabe 6: Erstelle ein Programm, welches aus den Primzahlen p und q und dem öffentlichen Schlüssel [m,e] den privaten Schlüssel [m, d] berechnet.
Hinweis: Lemma von Bézout.

Theorie RSA und Modulorechnen

Lemma von Bézout: Sind die ganzen Zahlen a und teilerfremd - gilt also ggT(a,b)=1 – so gibt es ganze Zahlen s und t, sodass **s*a + t*b = 1**.

Beispiel: (-1071)***11** + 2 * **5891** = 1.

Online Rechner: http://www.dcode.fr/bezout-identity

Satz von Euler:	$a^{\phi(m)} = 1$	(modulo m)	wenn ggT(a,m) = 1
Allgemeiner gilt:	$a^b = a^{b \bmod \phi(m)}$	(modulo m)	
Daraus folgt sofort:	$a * a^{\phi(m)-1} = 1$	(modulo m)	

Beispiel: wähle m = 10 = 2 * 5. Es folgt $\phi(10) = 4$. Für die Zahl a=7 gilt ggT(7,10) = 1. Der Satz von Euler ist also anwendbar und ergibt: $7^{\phi(10)} = 7^4 = 1$ (modulo 10).

Eine direkte Rechung bestätigt dies: $7^4 = 49 * 49 = 2401 = 1$ (modulo 10).

Beispiel: Man berechne 7^{222} mod 10 mit dem Satz von Euler.
7^{222} mod 10 = $(7^4) * (7^4) * (7^4)$ …..* 7^2 = 1 * 1* …. * 7^2 = 49 mod 10 = 9.