Assignment 1, part 1
by Staffan Lundström, roll no 03005201

The message *m* is encrypted in these three ways since they all have the same encryption key *e* = 3:

$$\begin{cases} E(m) = m^e \pmod{n_1} = c_1 \\ E(m) = m^e \pmod{n_2} = c_2 \\ E(m) = m^e \pmod{n_3} = c_3 \end{cases}$$

Let $m^e = a$

Since $\gcd(n_1, n_2) = 1$, $\gcd(n_2, n_3) = 1$ and $\gcd(n_1, n_3) = 1)$, the system

$$\begin{cases} a \equiv c_1 \pmod{n_1} \\ a \equiv c_2 \pmod{n_2} \\ a \equiv c_3 \pmod{n_3} \end{cases} \qquad (1)$$

has a unique solution modulo $n = n_1 * n_2 * n_3$ according to the Chinese Remainder Theorem.

Let $N_i = \prod_{j \neq i} n_j = \frac{n}{n_i}$. From $\gcd(N_i, n_i) = 1$ follows the existence of numbers b_i such that $b_i N_i \equiv 1 \pmod{n_i}$, $1 \leq i \leq 3$.

Then $a = c_1 b_1 N_1 + c_2 b_2 N_2 + c_3 b_3 N_3 \equiv c_i \pmod{n_i}$. The computational work is to find b_i. It can effectively be done using Euclid's algorithm. Since it's most likely that $m^e < n_1 * n_2 * n_3$, the message is hacked by taking $m = a^{\frac{1}{e}}$.