Dinu Marius
Grupa A5

8.

$c_1 = m^{e_1} \bmod n$ $\quad (e_A, e_B) = 1$ (1)

$c_2 = m^{e_2} \bmod n$

Dacă $\gcd(e_1, e_2) = 1 \Rightarrow \exists a, b \in \mathbb{Z}: e_1 \cdot a + e_2 \cdot b = 1$
unde a și b le găsim folosind alg. extins a lui Euclid
și $m \equiv_n c_1^a \cdot c_2^b \bmod n \Rightarrow e_A \cdot a + e_B \cdot b = 1$ (2)

$c_1^a \cdot c_2^b \Leftrightarrow (m^{e_1})^a \cdot (m^{e_2})^b \Leftrightarrow m^{e_1 a} \cdot m^{e_2 b} \Leftrightarrow$

$m^{e_1 a + e_2 b} \Leftrightarrow m^1 \Leftrightarrow m$

$e_1 = e_A$
$e_2 = e_B$
(2)