

A
 d_A

B
 d_B

C
 d_C

Verzeichnis:

A -> n_A, e_A

B -> n_B, e_B

C -> n_C, e_C

$m_1^{e_A} \bmod n$

$m_2^{e_C} \bmod n$