14) Volodi Emilia, M532 Iulia si Andrei folosesa criptosistemul RSA. Iulie one Ke = (nI = 9881, 6I = 3817) a) Determinati chia privatà a Iuliei. $9991 = p.q \Rightarrow q(9931) = (p-1)(q-1)$ B=87, q=103 = (1228 bom) = 108= d (3321) = (32-1)(102-1) = 29335 dAeA = 1 (mod y(n)) => d = 3917 -1 (mod 9792) Euclid: 3817.8+1958 = 9792 1+ S. 9287 = R122 1828 = 1828 + 0 J = 3371 -5.7324

 $7 = (2) \cdot 3213 - 5 \cdot 3235 => Kg^{2} = (3231, 2)$ $1 = 2313 - 5 \cdot (3255 - 5 \cdot 2313)$ $1 = 2313 - 5 \cdot (3255 - 5 \cdot 2313)$ $1 = 2313 - 5 \cdot (3255 - 5 \cdot 2313)$

b) Deeriptati mesa jul BMHA_X
primit de Inlia, dacă lungimea bloomilor
în clar este 2 și criptate-3. BMH + 1227 LEBB IN = 1 NO WILL A-X - 0 26 23 ptowns of production of an interest of the BMX = 1.302+12.30+7 = 1267 = 1267 (mod 9981) $A - X = 26.30 + 23 = 805 = 760_{2} = 803^{5} \pmod{9894} = 530 \pmod{10?}$ = 404 (mod 10?) $\rightarrow 14 \rightarrow 0$ -> 13 ->276 = (1-801)(1-62) = (1882) p

(8000 pan) + spec = 6 = ((w) + form) = 12/16

5.868 - 88 HE + 9.

(B) + 8 - 1/12 E

: 152 , H-