TEMA 7

(ex.5) RSA cheia publica Ke = (m=1189, e=747)

a) cheia privata?

b) $H^{j} \leq m \leq H^{j+1}$, lungimea blocurilor l=jH H-lungime alfabet; BFCAFMBiW.

Rezdvare

a) kd= (dA, mA)

 $d = e^{-1} \pmod{f(n)}$

 $m = p \cdot g = 1189 = 29.41$

Descempumem 1189 -> [[1189] = 34 => [[1189]+1=35]

t=35=) 352- 1189 =36=62

 $M = \frac{1}{4} 35^2 - 6^2 = (35 - 6)(35 + 6) = 29.44$

f(n) = (p-1)(2-1) = 28.40

d= e-1 (mod 1120) = 747 (mod 1120)

X 100 MMM = (1,0) 1120: 747 = 1, h. 373=) X 373=

 $= \chi_{1120} - \chi_{747} = (1,0) - (0,1) = (1,-1)$

747: 373=2, n.1-) X,=X,+1,-2.X373=(0,1)-(2,-2)=(-2,3)

=> e (mod 1120)=3=> [d=3] (chein phivata)

b) H=30. 307 < 1189 < 307+1 THE TOTAL ME MINDER SONT j=2 => 900 < 1189 < 27000 deci l=3 impartim textul in blocuri de lungime3 BFCAFMBIN BFC = $(4.(1)(5)(2) = 2.30^{\circ} + 5.30 + 30^{2} = 2 + 150 + 900 = 1052$ ATM= (0)(5)(13)= 13+5.30 = 163 $BiW = (2)(8)(22) = 22 + 8.30 + 2.30^2 = 2062$ W= 1, (811)) C= 118 = 1 C311/2 C- (811) momograposod 11. 68 = (21 de) (x de) = 52 - 28 H -m OH 35 = (1-C)(1-9) = (10) H (10) + (151) bann) FILE = (051 bann) + 3 . b CHARLES IN THE FIRE OWN (O. P. WYL) WAY (1-1)-(1-1)-(1-1) = FILEX -, SILX = (1-1)-(1-1)-(1-1) 1000-1000-1000 - 100 X - FIREX - X C 1 16 & OFER FIRE (alouse mints) / E-10/6-6 (101 hum) 10 0-