Tema 7 - Criptografie

20.

a. Criptarea mesajului HELP_ME:

1. Determinarea cheii publice și private:

nr prime: $p = 23$, $q = 17$

modul: $n = p \times q = 23 \cdot 17 = 391$

funcția Euler: $\phi(n) = (p-1) \times (q-1) = 22 \times 16 = 352$

exponent de criptare: $e = 3$

2. Cheia de decriptare:

Pentru a găsi d a.î. $e \times d \equiv 1 \pmod{\phi(n)}$:

$3d \equiv 1 \pmod{352}$

Folosim algoritmul extins Euclid pentru a găsi inversul multiplicativ:

$352 = 3 \times 117 + 1$

$\therefore d = 117$

Deci, cheia publică $(n, e) = (391, 3)$ și cheia privată este $d = 117$

3. Criptarea mesajului HELP_ME!

Vom folosi alfabetul cu care am lucrat până acum,

H = 7 E = 4 L = 11 P = 15 _ = 28 M = 12

! = 27

Criptarea fiecărui caracter m se face prin calculul: $c \equiv m^e \pmod n$:

$H = 7^3 \equiv 343 \pmod{391} = 343$

$E: 4^3 = 64 \pmod{391} = 64$

$L: 11^3 \equiv 1331 \pmod{391} = 158$

$P: 15^3 \equiv 3375 \pmod{391} = 252$

$-: 28^3 \equiv 21952 \pmod{391} = 60$

$M: 12^3 \equiv 1728 \pmod{391} \equiv 555 \pmod{391} = 164$

$E: 4^3 = 64$

$!: 27^3 \equiv 19683 \pmod{391} = 135$

Mesajul criptat este: 343, 64, 158, 252, 60, 164, 64, 135

b. Determinarea cheii de decriptare și decriptarea mesajului: "EBMMAAF OMML!EBAIHJ"

1. Cheia de decriptare este $d = 117$ (enunț)

2. Decriptarea mesajului primit:

→ decriptăm fiecare blac

$m = c^d \pmod n$

A = 0 B = 1 C = 2
D = 3 E = 4 F = 5 G = 6
H = 7 I = 8 J = 9 K = 10 ...

Blocurile:

EB → 4, 1
MM → 12, 12
AA → 0, 0
F → 5

OM -> 14, 12

ML -> 12, 11

! -> 27

EB -> 4, 1

AI -> 0, 8

Hi -> 7, 8

$D_o m = c^{117} \pmod{391}$

3. Calculăm pentru fiecare bloc criptat:

$E \to 4^{117} \pmod{391}$	$O \to 14^{117} \pmod{391}$
$B \to 1^{117} \pmod{391}$	$L \to 11^{117} \pmod{391}$
$M \to 12^{117} \pmod{391}$	$! \to 27^{117} \pmod{391}$
$A \to 0^{117} \pmod{391}$	$i \to 8^{117} \pmod{391}$
$F \to 5^{117} \pmod{391}$	$H \to 7^{117} \pmod{391}$

Putem folosi un scurt program: tema7_20.cpp

bloc decriptat: 64, 1, 144, 144, 0, 0, 32, 255, 144, 144, 121, 343, 64, 1, 0, 512, 343, 512.

Mesaj: HELP_ME