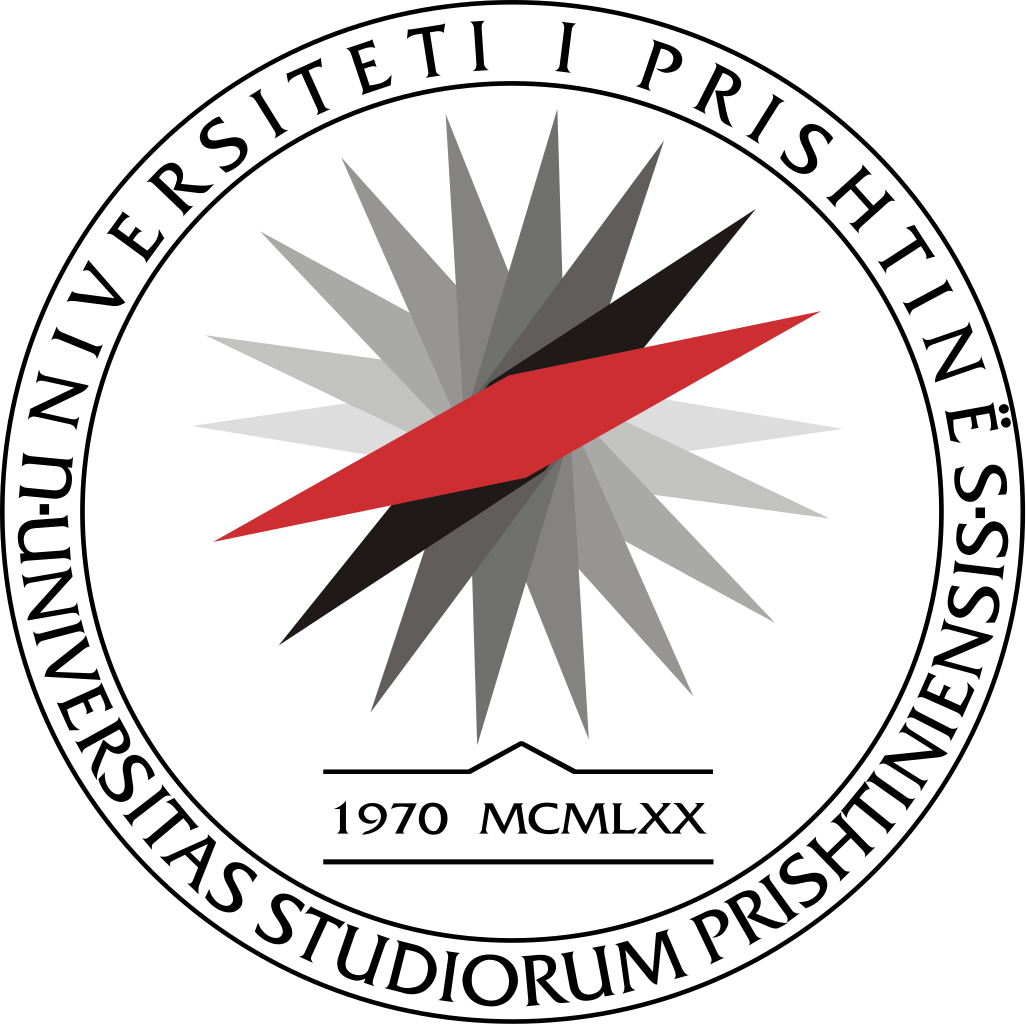
**UNIVERSITETI I PRISHTINËS**

**FAKULTETI I SHKENCAVE MATEMATIKE – NATYRORE**

**DEPARTAMENTI I MATEMATIKËS**

**PROGRAMI: Shkencë Kompjuterike**



Lënda: Siguria e te dhenave

Tema: Enkriptimi dhe Dekriptimi RSA

Studentët:

* Lisa Ramizi

# Enkriptimi

## a) Kriptimi dhe deshifrimi RSA:

Pasi qe

n = 253  
e = 31 (çelës publik)  
m = 10 (tekst i thjeshtë që do të kodohet)  
c = 35 (teksti i shifruar që do të deshifrohet)

Për të gjetur p, q dhe d:

1. Llogarisim p dhe q:

* Meqenëse n është prodhim i dy numrave të thjeshtë (p dhe q), duhet të gjejmë faktorët e thjeshtë të n-së.
* Faktorët e 253 janë 11 dhe 23.
* Prandaj, p = 11 dhe q = 23.

1. Llogaritni funksionin totient të Euler-it (phi):

* phi(n) = (p - 1) \* (q - 1)
* phi (253) = (11 - 1) \* (23 - 1) = 10 \* 22 = 220

1. Llogaritni çelësin privat (d):

* Duhet të gjejmë inversin shumëzues modular të e modulo phi(n).
* d = e^(-1) mod phi(n)
* Për të llogaritur inversin modular, mund të përdorim Algoritmin Euklidian të Zgjeruar.
* Në këtë rast, d = 179, pasi plotëson kushtin (31 \* 179) % 220 = 1.

1. **Enkriptojme tekstin e thjeshtë (m):**

* Për të enkriptuar tekstin e thjeshtë, ne përdorim vlerat e çelësit publik (n, e).
* c = m^e mod n
* Duke zëvendësuar vlerat, c = 10^31 mod 253 = 35.

1. **Deshifroni tekstin e shifruar (c):**

* Për të deshifruar tekstin e shifruar, ne përdorim vlerën e çelësit privat (d).
* m = c^d mod n
* Duke zëvendësuar vlerat, m = 35^179 mod 253 = 10.

Prandaj, vlerat e p, q dhe d janë përkatësisht 11, 23 dhe 179. Vlera e koduar e 10 (m) është 35 (c), dhe vlera e deshifruar e 35 (c) është 10 (m).

## b) Kriptimi RSA me gjatësinë e bllokut 2:

Pasi qe:

p = 67  
q = 73  
e = 89 (çelës publik)  
Tekst i thjeshtë: "SIGURIA"  
Gjatësia e bllokut: 2

Për të enkriptuar tekstin e thjeshtë duke përdorur RSA:

1. **Shndërrojme tekstin e thjeshtë në paraqitje numerike:**

* "SIGURIA" mund të përfaqësohet si një sekuencë numrash duke përdorur vlerat ASCII.
* S = 83, E = 69, C = 67, U = 85, R = 82, I = 73, T = 84, Y = 89.

1. **Ndajme paraqitjen numerike në blloqe me gjatësi 2:**

* Blloqet: [83, 69], [67, 85], [82, 73], [84, 89]

1. **Enkriptojme çdo bllok duke përdorur çelësin publik (n, e):**

* Për çdo bllok [x, y], kryeni kriptim: c = (x^e mod n, y^e mod n)
* Për shembull, [83, 69] bëhet [c1, c2] = [83^89 mod (6773), 69^89 mod (6773)].

1. **Teksti i shifruar që rezulton është lidhja e blloqeve të koduara:**

Teksti shifror: [c1, c2, c3, c4]

Operacioni i fuqizimit modular (x^e mod n) mund të kryhet në mënyrë efikase duke përdorur algoritme modulare të fuqizimit si Square dhe Multiply.