**RSA**

**Detyra 1.** Duke përdorë kriptosistemin RSA të kryhen:

1. Le të jenë 𝑛 = 253 dhe 𝑒 = 31 çelës publik. Enkripto 𝑚 = 10, dhe gjejë 𝑝, 𝑞 dhe 𝑑.

b) Le të jenë 𝑝 = 67, 𝑞 = 73 dhe 𝑒 = 89. Enkripto tekstin SIGURI me gjatësi të bllokut 2?

**Zgjidhje**

Le të kujtojmë metodën e enkriptimit dhe dekriptimit të RSA. Enkriptimi bëhet me anë të çelësit publik, por dekriptimi i mezashit bëhet me anë të çelësit privat.

Zgjedhim dy numra të thjeshtë 𝑝, 𝑞.

𝑛 = 𝑝 ∗ 𝑞

(𝑛) = (𝑝 − 1)(𝑞 − 1)

1 < 𝑒 < (𝑛) ∴ 𝑔𝑐𝑑(𝑒,𝜑(𝑛)) = 1;

𝑑 ∗ 𝑒 ≡ 1 𝑚𝑜𝑑 (𝑛) (𝑛, 𝑒)

Prej nga fitojmë (𝑛,) çelësin publik dhe (𝑛, 𝑑) çelësin privat. Le të jetë 𝑥 𝑚𝑒𝑧𝑎𝑠ℎ𝑖 𝑜𝑟𝑖𝑔𝑗𝑖𝑛𝑎𝑙, 𝑦 𝑚𝑒𝑧𝑎𝑠ℎ𝑖 𝑖 𝑒𝑛𝑘𝑟𝑖𝑝𝑡𝑢𝑎𝑟

Enkriptimi: 𝑦 ≡ 𝑥 𝑒 𝑚𝑜𝑑 𝑛

Dekriptimi: 𝑥 ≡ 𝑦 𝑑 𝑚𝑜𝑑 𝑛

Pra,

𝐷𝑒𝑘𝑟𝑖𝑝𝑡𝑜ç𝑒𝑙ë𝑠𝑖 𝑝𝑟𝑖𝑣𝑎( 𝑒𝑛𝑘𝑟𝑖𝑝𝑡𝑜ç𝑒𝑙ë𝑠𝑖 𝑝𝑢𝑏𝑙𝑖𝑘(𝑚𝑒𝑧𝑎𝑠ℎ𝑖)) = 𝑚𝑒𝑧𝑎𝑠ℎ𝑖

1. Fillimisht po gjejmë 𝑝, 𝑞 dhe 𝑑. Numrin n duhet të e shkruajme si prodhim i numrave të thjeshtë. Shikojme se cilët numra të thjeshtë e plotpjesëtojnë numrin 253, duke filluar me nga i vogli. 253 nuk plotpjesëtohet nga 2,3,5,7 por nga 11. Kemi 253/11 = 23. Meqë 23 është i thjeshtë kemi

253 = 11 ∗ 23

𝑝 = 11, 𝑞 = 23

(𝑛) = (11 − 1)(23 − 1)

Zgjidhim kongruencën lineare 𝑑 ∗ 31 ≡ 1 𝑚𝑜𝑑 220

220 = 7 ∗ 31 + 3

31 = 3 ∗ 10 + 1

1 = 31 – 3 ∗ 10 = 31 – 10 ∗ (220 − 7 ∗ 31) = 71 ∗ 31 − 10 ∗ 220

Dmth inversi 31 𝑚𝑜𝑑 220 është 𝑑 = 71

Për mezashin x = 10,

Enkriptimi: 𝑦 = 1031 ≡ 43 𝑚𝑜𝑑 253

Dekriptimi: 𝑥 = 4371 ≡ 10 𝑚𝑜𝑑 253

Për mezashin e enkriptuar c = 35,

Dekriptimi: 𝑥 = 3571 ≡ 156 𝑚𝑜𝑑 253

1. 𝑝 = 76, 𝑛 = 73, 𝑒 = 89, 𝑚𝑒𝑧𝑎𝑠ℎ𝑖 = 𝑆𝐼𝐺𝑈𝑅𝐼

𝑛 = 67 ∗ 73 = 4891

SIGURI = 01010011 01001001 01000111 01010101 01010010 01001001

= 83 ≡ 2200 𝑚𝑜𝑑 4891 2200 =

= 73 ≡ 2701𝑚𝑜𝑑 4891 2701 = = 71 ≡ 4270 𝑚𝑜𝑑 4891 4270=

= 85 ≡ 3145𝑚𝑜𝑑 4891 3145 =

= 82 ≡ 1087𝑚𝑜𝑑 4891 1087 =

= 73 ≡ 2701𝑚𝑜𝑑 4891 2701 =

Enkriptuar:

100010011000101010001101100001010111011000100100110000111111101010001101

**Prezantimi i kodit**

A picture containing text, screenshot, software

Description automatically generatedNë vazhdim i kemi paraqitur klasat kryesore që janë përdorur për eknkriptimin e një stringu me gjatësi m:

A screen shot of a computer program

Description automatically generated with medium confidence

Më lartë ishte kodi për opsionin a) kurse në vazhdim shohim zgjidhjen e opsionit b)

A picture containing text, screenshot, software, display

Description automatically generated

A picture containing text, screenshot, font

Description automatically generated

**Rezultati**

**A screenshot of a computer screen

Description automatically generated with low confidence**Pas ekzekutimit të kodit për vlerat e kërkuara në terminal shfaqen vlerat e fituara si mëposhtë: