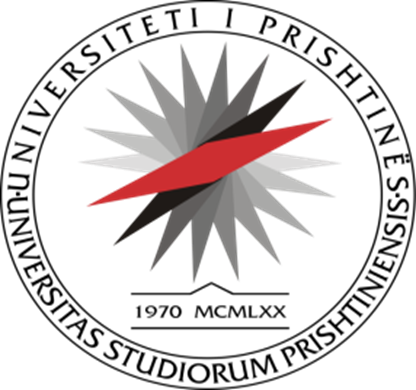
**UNIVERSITETI I PRISHTINËS**

**FAKULTETI I SHKENCAVE MATEMATIKORE DHE NATYRORE**

**DEPARTAMENTI I MATEMATIKËS**



**DETYRË**

**LËNDA: *SIGURIA E TË DHËNAVE***

**Profesor: Student:**

*Artan Berisha Elvira Jahaj Besnik Duriqi* *Dafina Sopa Elsa Tafilaj*

**KËRKESA E DETYRËS**

Te algoritmi AES\_128 është dhënë mesazhi 000102030405060708090A0B0C0D0E0F (në formë

heksadecimale) dhe çelësi 01010101010101010101010101010101 (në formë heksadecimale):

a) Gjejë vlerën e Gjendjes, si matricë ,

b) Gjejë vlerën pas AddRoundKey,

c) Gjejë vlerën pas SubBytes,

d) Gjejë vlerën pas ShiftRoës,

e) Gjejë vlerën pas MiXColumns.

Zgjidhjen e bëni në një excel file.

**ZGJIDHJA**

Kjo pyetje duket se lidhet me standardin e avancuar të enkriptimit (AES). Fillimisht Algoritmi i enkriptimit AES (i njohur gjithashtu si algoritmi Rijndael) është një algoritëm simetrik i shifrimit të bllokut me një madhësi prej 128 bit. Ai i konverton këto blloqe individuale duke përdorur çelësat 128, 192 dhe 256 bit. Pasi i kodon këto blloqe, i bashkon ato për të formuar tekstin e shifruar.

Në AES, hyrja përpunohet përmes një serie transformimesh që përfshijnë SubBytes, ShiftRows, MixColumns dhe AddRoundKey. Çdo raund i enkriptimit AES përbëhet nga këto transformime të aplikuara në një renditje specifike.

Duke supozuar se mesazhi hyrës është në formën e një blloku 16-bajtësh (128 bit), mesazhi i dhënë 000102030405060708090A0B0C0D0E0F mund të përfaqësohet si një matricë 4x4 (State) në mënyrën e mëposhtme:

***Matrica e gjendjes fillestare:***

|  |  |  |  |
| --- | --- | --- | --- |
| 00 | 04 | 08 | 0C |
| 01 | 05 | 09 | 0D |
| 02 | 06 | 0A | 0E |
| 03 | 07 | 0B | 0F |

Çelësi i dhënë 01010101010101010101010101010101 mund të përfaqësohet gjithashtu si një matricë 4x4 (Çelësi) në mënyrën e mëposhtme:

***Çelësi :***

|  |  |  |  |
| --- | --- | --- | --- |
| 01 | 01 | 01 | 01 |
| 01 | 01 | 01 | 01 |
| 01 | 01 | 01 | 01 |
| 01 | 01 | 01 | 01 |

**a)** Vlera e matricës në gjendjën fillestare, si matricë, është e njëjtë me paraqitjen matricore të mesazhit hyrës të dhënë më sipër.

**b)** Operacioni AddRoundKey përfshin XORing në bit të matricës matricës në gjendjën fillestare me Çelësin. Matrica që rezulton (***AddRoundKey***) mund të llogaritet si më poshtë:

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 5 | 9 | D |
| 0 | 4 | 8 | C |
| 3 | 7 | B | F |
| 2 | 6 | A | E |

***AddRoundKey =( Matrica e gjendjes )*XOR (*Çelësi)***

**c)** Operacioni SubBytes përfshin zëvendësimin e çdo bajt në matricën e gjendjes me një bajt tjetër nga një tabelë zëvendësimi fikse (S-box). Matrica që rezulton (***SubBytes***) mund të llogaritet si më poshtë:

|  |  |  |  |
| --- | --- | --- | --- |
| 63 | F2 | 30 | FE |
| 7C | 6B | 1 | D7 |
| 77 | 6F | 67 | AB |
| 7B | C5 | 2B | 76 |

**SubBytes*=****SubByte****(AddRoundKey)***

**d)**Operacioni ShiftRows përfshin zhvendosjen e çdo rreshti të matricës së gjendjes në mënyrë ciklike me një numër të caktuar bajtësh. Matrica që rezulton (***ShiftRows***) mund të llogaritet si më poshtë:

|  |  |  |  |
| --- | --- | --- | --- |
| 63 | 6B | 67 | 76 |
| 7C | F2 | 1 | D7 |
| 77 | 6F | 30 | AB |
| 7B | C5 | 2B | FE |

***ShiftRows****=ShiftRows(****SubBytes****)*

**e)** Operacioni MixColumns përfshin shumëzimin e secilës kolonë të matricës së gjendjes me një matricë fikse (matrica MixColumns). Matrica që rezulton (***MixColumns***) mund të llogaritet si më poshtë:

|  |  |  |  |
| --- | --- | --- | --- |
| 5F | 72 | AC | 68 |
| 57 | C3 | 2B | 8D |
| F8 | 0D | E9 | 31 |
| F5 | 74 | 66 | 9D |

***MixColumns****=MixColumns(****ShiftRows****)*

Siç mund të të shihët SubBytes, ShiftRows dhe MixColumns përfshijnë operacione specifike matematikore dhe tabela/matrica fikse. Këto operacione janë krijuar për të siguruar difuzion dhe konfuzion të mesazhit hyrës, duke e bërë atë më të sigurt kundër sulmeve. Operacioni AddRoundKey përfshin shtimin e çelësit në mesazh, duke siguruar një shtresë shtesë sigurie.