**Lënda: “Sigurimi i informacionit”**

**Profesori i lëndës:** Prof. Dr. Blerim Rexha

**Niveli:** Master, “Inxhinieri kompjuterike”

**Studenti:** Albulenë Mushica

AES – Advanced Encryption Standard

dhe transformimet e tij

Qëllimi

Programimi me C# i  ByteSub (nonlinear layer) /ShiftRow (linear mixing layer)  / MixColumn (nonlinear layer) / AddRoundKey (key addition layer) tek Algorimi AES.

Përmbajta

[Hyrja 2](#_Toc58362012)

[AES – Advanced Encryption Standard 2](#_Toc58362013)

[Transformimi **SubBytes** 2](#_Toc58362014)

[Transformimi **ShiftRows** 3](#_Toc58362015)

[Transformimi **MixColumns** 4](#_Toc58362016)

[Transformimi **AddRoundKey** 5](#_Toc58362017)

[Konkludimi 6](#_Toc58362018)

[Bibliografia 7](#_Toc58362019)

# Hyrja

Në këtë dokument do te shpjegohet përdorimi dhe funksioni i algoritmit AES – Advanced Encryption Standard, si dhe operacionet/transformimet kryesore të këtij algoritmi, sic janë **ByteSub, ShiftRow, MixColumn** dhe **AddRoundKey**.

Në pjesën ku do te shpjegohen operacionet e algoritmit AES, do te paraqesim më shumë detaje, meqenëse është edhe qëllimi i detyrës.

# AES – Advanced Encryption Standard

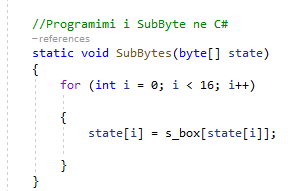
AES -Adcanced Encryptiion Standard, i cili njihet edhe me ermin Rijndael, është një specifikim për enkriptimin e të dhënave elektronike, pjesë e Rijandel block cipher (algoritëm deterministik që operon me gjatësi fikse të bita, të quajtura blloqe), i zhvilluar nga dy kriptografë Belgë, Vincent Rijmen dhe Joan Daemen.

Algoritmi i përshkruar nga AES është algoritem simetrik (ang. Symetric-key algorithm) dhe emërohen si të tilla për shkak se përdorin të njejtin celës kriptografik si në procesin e enkriptimit të plaintext-it (plaintext, quhet teksti qe do të enkriptohet) dhe në atë të dekriptimit të ciphertext-it (ciphertext, quhet teksti i enkriptuar).

AES bazohet në dizajnin e njohur si SPN - Subtitution-Permutation Network, i cili në kriptografi është një seri e opercaioneve matematikore të lidhura mes vete e që në këtë rast përdoret në block cipher e algroitmit AES. Ky algoritem përbëhet nga blloqe fikse me gjatësi 128 bita dhe me gjatësi të celësit kriptografik të 128, 192 apo 256 bita, gjatësi kjo e cila definon numrin e transformimeve qe konvertojnë plaintext-in në ciphertext, ku për celës me 128 bita kemi 10 cikle, per 192 12 cikle dhe per 256 14 cilke të transformimit. Ky algoritëm operon në matricë të bajtave 4x4 me renditje nga kolonat, e njohur si state (nga ang. gjendje).

# Transformimi **SubBytes**

SubBytes është një hap i zëvendësimit jo linear, ku secili bajt zëvendësohet me bajtin përkatës në tabelën/matricën 8-bitëshe S-box - Substitution Box, e cila në kriptografi është përbërësi bazik i algoritmeve me celësa simetrik.



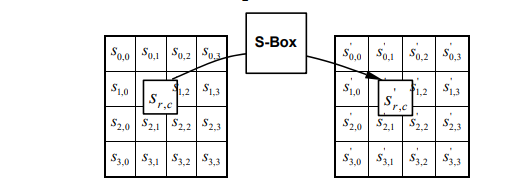
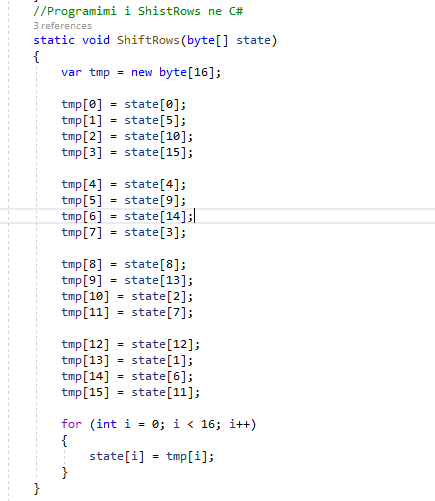


Figura 1 aplikimi i S\_Box te secili bajt i state

# Transformimi **ShiftRows**

ShiftRows është një hap i cili operon në rreshtat e state, në mënyrë ciklike zhvendos bajtat në secilin rresht sipas një hapësire specifike. Rreshti i parë nuk ndryshon, rreshti i dytë zhvendosë secilin bajt për një pozitë majtas, kurse rreshti i tretë dhe i katërt zhvendosen nga dy dhe tri pozita majtas. Në këtë mënyrë arrihet një rezultat/output i cili kur krahasohet me atë hyrës, del se secila kolonë përmbanë vlera të kolonave tjera të input-it. Rëndësia e këtij hapi është të shmanget enkriptimi i pavarur i kolonave të state-it.



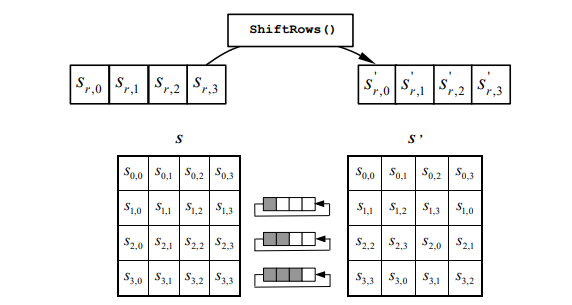
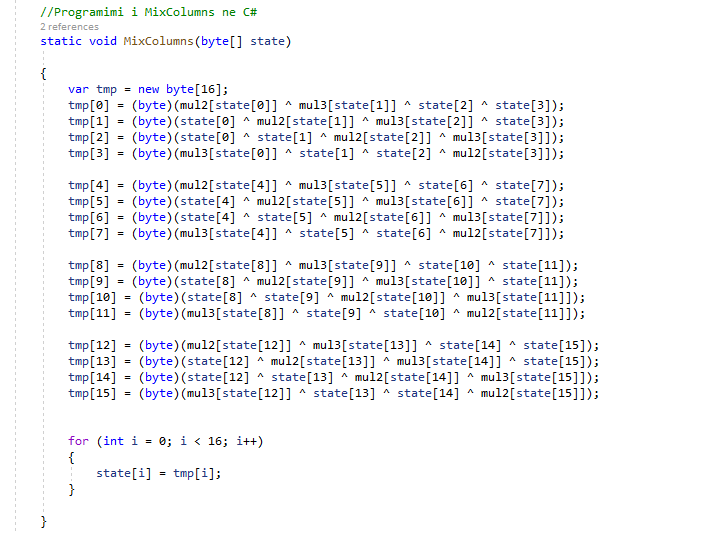


Figura 2 shiftimi i tre rreshtave te fundit te state

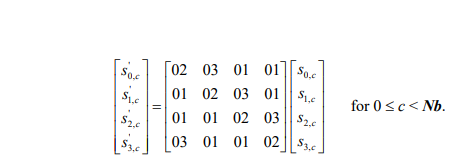
# Transformimi **MixColumns**

Në hapin MixColumns katër bajtat e secilës kolonë të state-it kombinohen duke përdorë një transformim invertibil linear. Ky funksion pranon në hyrje katër bajta dhe jep si rezultat katër bajta. Sikurse transformimi ShiftRows edhe MixColumns krijon konfuzion në algoritëm.

Gjatë këtij operacioni secila kolonë transformohet duke përdorë një matricë fikse. Ky operacion si bazë ka shumëzimin dhe shumën/shtimin(XOR) e hyrjeve.







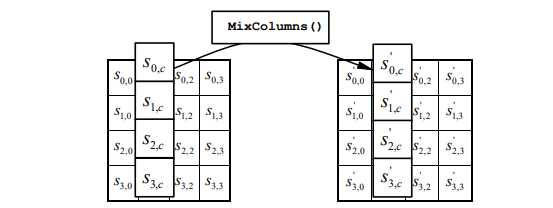
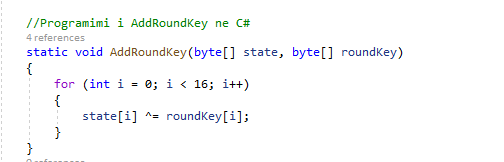


Figura 3 transformimi i state duke perzier kolonat

# Transformimi **AddRoundKey**

Në hapin AddRoundKey nëncelësi kombinohet me state (gjendjen) dhe për secilin cikël gjenerohet një nëncelës nga celësi kryesor, duke përdorë metodën key schedule për zgjerimin e një celësi të shkurtër në një numër të caktuar të celësave ciklik. Secili cikël në AES kërkon një celës të vecantë prej bit-a. Këta celësa prodhohen nga celësi primar dhe secili ka gjatësi të barabartë me state-tin. Nëncelësi krijohet duke kombinuar me XOR secilin bajt të state-tit me bajtat përkatës të nëncelësit.



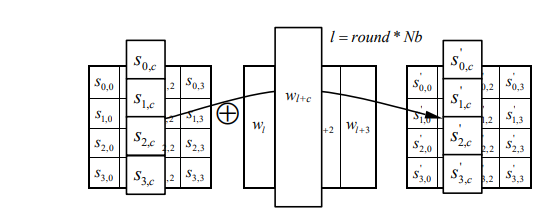


Figura 4 XOR i state me 4 bajta te celesit apo "word"

# Konkludimi

Në ditët e sotme, teknologjia është zhvilluar aq shumë sa përdoret gati në të gjitha sferat e jetës, prandaj është e rëndësishme që sigurimi i informacionit të jetë në nivel me siguri sa më të lartë. Algoritmi AES është mjaft i qëndrueshëm ndaj tentimeve të thyerjes së tij, kjo për shkak të celësave me gjatësi më të madhe dhe transformimeve të përmendura më lartë.

Mund të implementohet në software dhe hardware dhe është algoritmi që përdoret më së shumti.

Rezultati final i plaintext-it “Encrypted message!”, sipas katër transformimeve t, sipas katër transformimeve të algoritmit AES, i programuar në C# është:

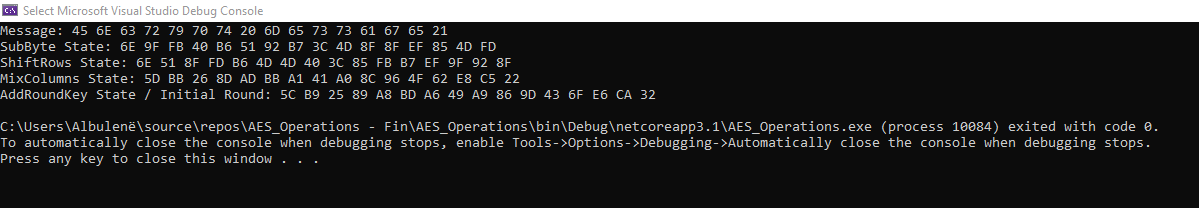


Figura 5 Programimi ne C# i kater transformimeve te AES

# Bibliografia

* Federal Information Processing Standards Publication 197 November 26, 2001 Announcing the ADVANCED ENCRYPTION STANDARD (AES)

<https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf>

* AES Wikipedia

<https://en.wikipedia.org/wiki/Advanced_Encryption_Standard>