AES i thjeshtuar me CBC

Erjon Asllani
Departamenti Matematikë
Shkenca Kompjuterike
Universiteti i Prishtinës "Hasan Prishtina"
Prishtinë, Kosovë
erjon.asllani@student.uni-pr.edu

Fatbardh Gashi
Departamenti Matematikë
Shkenca Kompjuterike
Universiteti i Prishtinës "Hasan Prishtina"
Prishtinë, Kosovë
fatbardh.gashi6@student.uni-pr.edu

Vullnet Gërvalla
Departamenti Matematikë
Shkenca Kompjuterike
Universiteti i Prishtinës "Hasan Prishtina"
Prishtinë, Kosovë
vullnet.gervalla@student.uni-pr.edu

***Abstrakti*— Ky punim paraqet një përmbledhje gjithëpërfshirëse të Standardit të Enkriptimit të Avancuar (AES), një algoritëm i përdorur gjerësisht i enkriptimit të bllokut të shifruar me çelës simetrik, i cili është përzgjedhur si zëvendësim për Standardin e Kriptimit të të Dhënave (DES) nga Instituti Kombëtar i Standardeve dhe Teknologjisë. NIST). Punimi eksploron strukturën dhe funksionimin e algoritmit AES, veçoritë dhe avantazhet kryesore të tij, si dhe kufizimet dhe dobësitë e tij. Punimi shqyrton gjithashtu aplikimet e ndryshme të AES, duke përfshirë përdorimin e tij në sigurimin e të dhënave dixhitale në një gamë të gjerë pajisjesh dhe sistemesh.**

***Indeksi*—AES, AES i thjeshtuar, CBC**

I. Hyrje

AES (Advanced Encryption Standard) është një algoritëm enkriptimi i përdorur gjerësisht që përdoret për të siguruar të dhëna dixhitale. AES është një shifrim me blloqe me çelës simetrik që u zgjodh nga Instituti Kombëtar i Standardeve dhe Teknologjisë (NIST) si një zëvendësim për standardin e mëparshëm, Standardin e Kriptimit të të Dhënave (DES). Algoritmi u botua për herë të parë në 1998 dhe që atëherë është bërë një nga standardet më të përdorura të enkriptimit në botë.

A. Si funksionon AES

Algoritmi AES përdor një çelës simetrik për të kriptuar dhe deshifruar të dhënat. Kjo do të thotë se i njëjti çelës përdoret si për enkriptim ashtu edhe për deshifrim, dhe kushdo që ka çelësin mund t'i qaset të dhënave. Madhësia e çelësit mund të jetë ose 128, 192 ose 256 bit, me madhësi më të mëdha të çelësave që ofrojnë siguri më të madhe. AES operon në blloqe të dhënash, me madhësinë e secilit bllok 128 bit. Algoritmi përbëhet nga disa raunde operacionesh zëvendësimi dhe ndërrimi që përziejnë dhe transformojnë të dhënat në një mënyrë që është jashtëzakonisht e vështirë për t'u kthyer pa çelës.

Procesi i kriptimit përfshin hapat e mëposhtëm:

1. Zgjerimi i çelësit: Çelësi sekret zgjerohet në një grup çelësash të rrumbullakët që do të përdoren në raundet pasuese të enkriptimit.
2. Raundi fillestar: Teksti i thjeshtë 128-bit ndahet në blloqe 16-bajtësh dhe i nënshtrohet një transformimi fillestar duke përdorur çelësin e raundit të parë.
3. Rounds: Transformimi i tekstit të thjeshtë vazhdon përmes një serie raundesh, secili i përbërë nga katër hapa të veçantë: SubBytes, ShiftRows, MixColumns dhe AddRoundKey. Këta hapa punojnë së bashku për të zëvendësuar, ndryshuar dhe shpërndarë të dhënat në një mënyrë që i bën ato rezistente ndaj sulmeve.
4. Raundi Final: Raundi final është i ngjashëm me raundet e mëparshme, por e anashkalon hapin MixColumns.
5. Dalja: Teksti i shifruar që rezulton merret pas raundit përfundimtar, i cili më pas deshifrohet duke përdorur të njëjtin çelës sekret, por në rend të kundërt.

Në përgjithësi, AES është krijuar për të qenë një algoritëm i sigurt dhe efikas i enkriptimit që mund t'i rezistojë llojeve të ndryshme të sulmeve duke qenë gjithashtu mjaft i shpejtë për të operuar në kohë reale.

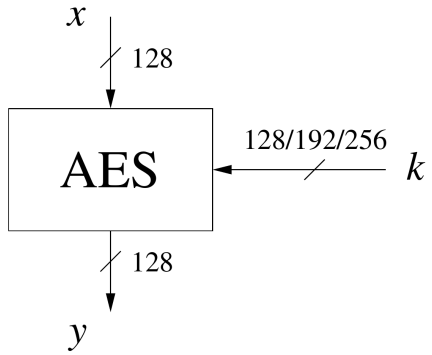


Fig 1: AES parametrat hyrës dhe dalës.

B. Avantazhet dhe kufizimet

Një nga avantazhet kryesore të AES është siguria e tij. Algoritmi është studiuar dhe testuar gjerësisht nga ekspertë kriptografikë dhe është treguar se është jashtëzakonisht rezistent ndaj sulmeve. Në fakt, AES është aktualisht algoritmi standard i kriptimit që përdoret nga qeveria amerikane për të mbrojtur informacionin e klasifikuar.

Një avantazh tjetër i AES është efikasiteti i tij. Algoritmi është projektuar të jetë i shpejtë dhe efikas, duke e lejuar atë të përdoret në një shumëllojshmëri të gjerë aplikacionesh. AES mund të zbatohet në harduer ose softuer dhe mund të përdoret në një gamë të gjerë pajisjesh, nga sistemet e vogla të integruara deri te serverët e mëdhenj.

Pavarësisht nga avantazhet e tij, AES nuk është pa kufizime. Një nga kufizimet kryesore të AES është se ai është një algoritëm me çelës simetrik, që do të thotë se i njëjti çelës përdoret si për enkriptim ashtu edhe për deshifrim. Kjo mund ta bëjë më të vështirë menaxhimin e çelësave dhe shpërndarjen e tyre të sigurt. Përveç kësaj, për shkak se i njëjti çelës përdoret për enkriptim dhe deshifrim, kushdo që ka akses te çelësi mund t'i qaset të dhënave. Kjo do të thotë që siguria e sistemit është po aq e fortë sa siguria e çelësit.

Një kufizim tjetër i AES është se është një shifër blloku, që do të thotë se funksionon në blloqe të dhënash me madhësi fikse. Kjo mund ta bëjë atë më pak efikas kur kriptoni sasi të mëdha të dhënash, pasi mund të duhet të ndahen në blloqe më të vogla. Përveç kësaj, për shkak se algoritmi funksionon në blloqe me madhësi fikse, ai mund të jetë i prekshëm ndaj llojeve të caktuara të sulmeve, siç janë sulmet e përplasjes së bllokut.

AES është një algoritëm kriptimi i përdorur gjerësisht që ofron siguri dhe efikasitet të fortë. Dizajni i tij me çelës simetrik dhe struktura e shifrimit të bllokut kanë disa kufizime, por ai mbetet një nga standardet më të përdorura të enkriptimit në botë. Me kërkimin dhe zhvillimin e vazhdueshëm, ka të ngjarë që AES të vazhdojë të zhvillohet dhe të mbetet një mjet kritik në sigurimin e të dhënave dixhitale.

II. Simplified AES

Mëposhtë është dhënë skema e algoritmit AES të thjeshtuar, i cili ka si hyrje bllokun me gjatësi 16 bit, çelësin me gjatësi 16 bit si dhe dalja e bllokut me gjatësi 16 bit. Shihet që algoritmi ka veprimet SBOX, ShiftRows, MixColums, AddRoundKey si dhe veprimet inverse të tyre InvSBOX, InvShiftRows, InvMixColums (në mënyrë analoge me algoritmin AES).

A. Enkriptimi

Ka 3 raunde, ku dy raundet e para janë identike ndërsa raundi i tretë (raundi i fundit) nuk e ka veprimin MixColumns. Një raund enkriptimi në Standardin e Enkriptimit të Avancuar 16-bit (AES) përfshin kryerjen e një sërë operacionesh matematikore në tekstin e thjeshtë për ta transformuar atë në tekst shifror. Çdo raund përbëhet nga katër hapa transformimi, të cilët janë si më poshtë:

$$SBOX = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 6_{16} & B_{16} & 0_{16} & 4_{16} \\ 1 & 7_{16} & E_{16} & 2_{16} & F_{16} \\ 2 & 9_{16} & 8_{16} & A_{16} & C_{16} \\ 3 & 3_{16} & 1_{16} & 5_{16} & D_{16} \end{array}.$$

Fig 2: Tabela e zëvendësimit (Substitute Box)

Ky SBOX është ndërtuar në fushën Galua (Galois field) $GF(2^4)$ me anë të polinomit ireducibil (shiko shtojcën A – **Ndërtimi i SBOX-it**). Zëvendësimi bëhet ashtu që nga vlera B_i dy bitët e parë tregojnë rreshtin e SBOX-it ndërsa dy bitët e fundit tregojnë shtyllën e SBOX-it. Atëherë vlera B_i zëvendësohet me vlerën përkatëse të SBOX-it ku priten rreshti dhe shtylla e gjetur.

1. Zëvendësimi
   Në hapin e parë, bajtët e tekstit të thjeshtë zëvendësohen duke përdorur një tabelë fikse zëvendësimi të quajtur S-box. Çdo bajt zëvendësohet nga një bajt përkatës nga kutia S, e cila krijohet duke përdorur një funksion matematikor të quajtur Rijndael S-box.

2. Permutacioni
   Në hapin e dytë, bajtët e tekstit të thjeshtë riorganizohen duke i zhvendosur majtas. Sasia e zhvendosjes varet nga pozicioni i bajtit në tekstin e thjeshtë.

3. Përzierja
   Në hapin e tretë, bajtët e tekstit të thjeshtë përzihen duke përdorur një matricë fikse. Ky operacion i shumëzimit të matricës quhet hapi MixColumns dhe siguron shpërndarjen e të dhënave në të gjithë tekstin e shifruar.

4. Shtesa kryesore
   Në hapin e fundit, një çelës i rrumbullakët i shtohet tekstit të thjeshtë të transformuar duke përdorur një operacion XOR në bit. Çelësi i rrumbullakët gjenerohet nga çelësi kryesor i enkriptimit duke përdorur një proces të quajtur Orari i çelësave. Ky hap siguron konfuzion të të dhënave, duke e bërë të vështirë për sulmuesit të nxjerrin informacion kuptimplotë nga teksti i koduar.

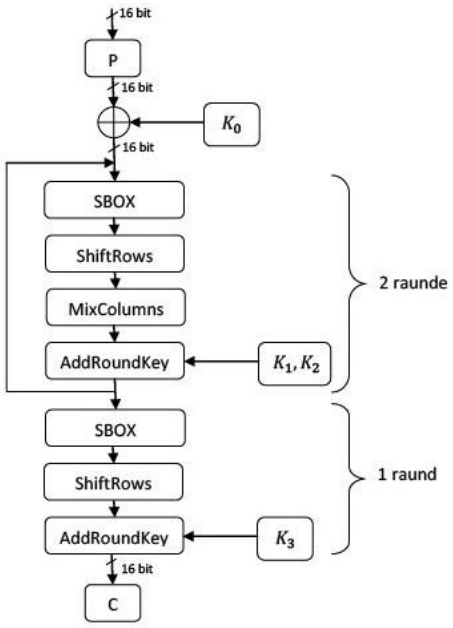


Fig 3: Skema e enkriptimit të AES.

Këta katër hapa kryhen në çdo raund të procesit të kriptimit. Në algoritmin 16-bit AES, ka gjithsej 10 raunde për çelësat 128-bit, 12 raunde për çelësat 192-bit dhe 14 raunde për çelësat 256-bit.

B. Dekriptimi

Ka 3 raunde, raundi i parë nuk e ka veprimin InvMixColumns dhe dy raundet tjera (raundi i dytë dhe i tretë) janë identike. Le të jenë teksti i enkriptuar $C = \begin{vmatrix} A_0 A_1 \\ A_2 A_3 \end{vmatrix}$ dhe çelësi i gjeneruar $K_3 = \begin{vmatrix} k_{12} k_{14} \\ k_{13} k_{15} \end{vmatrix}$ (shiko shtojcën B). Ku A_i dhe k_j janë nga 4 bit në formë heksadecimale pra A_i, $k_j \in \{0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F\}$

$$SBOX = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ 0 & 6_{16} & B_{16} & 0_{16} & 4_{16} \\ 1 & 7_{16} & E_{16} & 2_{16} & F_{16} \\ 2 & 9_{16} & 8_{16} & A_{16} & C_{16} \\ 3 & 3_{16} & 1_{16} & 5_{16} & D_{16} \end{array}.$$

Fig 4: Tabela e zëvendësimit (Substitute Box)

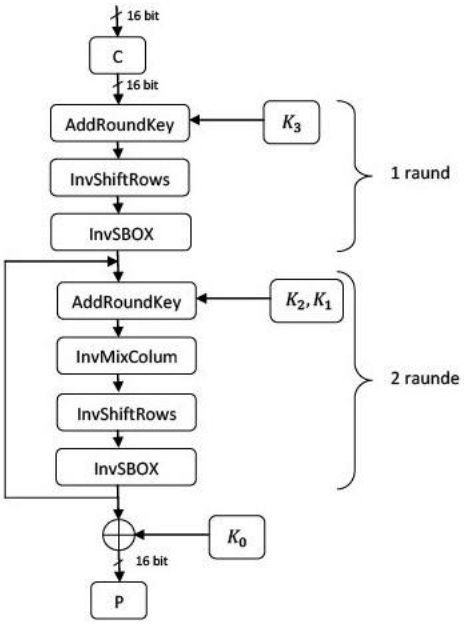


Fig 5: Skema e dekriptimit të AES.

C. Gjenerimi i qelsave

Në standardin e avancuar të enkriptimit 16-bit (AES), procesi i gjenerimit të çelësave është një komponent thelbësor i procesit të kriptimit dhe deshifrimit. Procesi i gjenerimit të çelësit përfshin transformimin e çelësit origjinal të furnizuar nga përdoruesi në një grup çelësash të rrumbullakët që përdoren në çdo raund të procesit të kriptimit dhe deshifrimit.

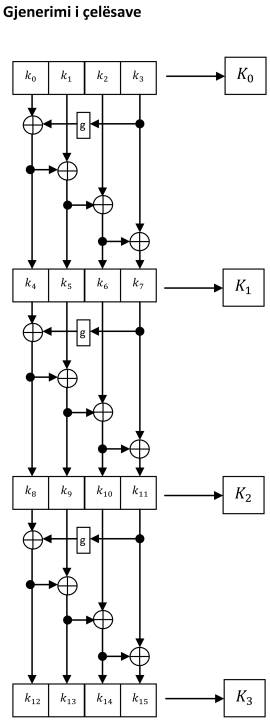
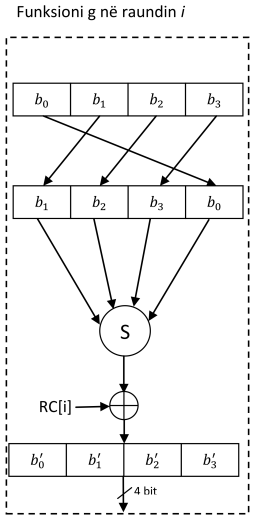


Fig 6: Funksioni g.

Procesi i gjenerimit të çelësave fillon duke marrë çelësin e dhënë nga përdoruesi, i cili mund të jetë ose një çelës 128-bit, 192-bit ose 256-bit, dhe duke kryer një proces zgjerimi të çelësit që gjeneron një grup çelësash të rrumbullakët. Procesi i zgjerimit të çelësit përfshin kryerjen e një sërë operacionesh në çelësin e furnizuar nga përdoruesi, duke përfshirë:

1. Zgjerimi i çelësit
   Çelësi i dhënë nga përdoruesi zgjerohet duke kryer një plan të çelësave që gjeneron një sekuencë çelësash të rrumbullakët. Numri i çelësave të rrumbullakët të gjeneruar varet nga madhësia e çelësit të përdorur në procesin e kriptimit.
2. Zëvendësimi
   Bajtet e çelësit të zgjeruar zëvendësohen duke përdorur kutinë Rijndael S, e cila është një tabelë fikse vlerash që siguron një zëvendësim jolinear të bajteve.
3. Permutacioni
   Bajtet e tastit të zgjeruar ndërrohen duke përdorur një tabelë permutacioni fikse. Ky ndërrim siguron difuzion të mëtejshëm të çelësit përgjatë orarit të çelësave.
4. Mbledhja konstante e rrumbullakët
   Një seri konstantesh të rrumbullakëta i shtohen çelësit të zgjeruar në çdo raund. Këto konstante të rrumbullakëta gjenerohen duke përdorur një funksion matematikor dhe sigurojnë konfuzion shtesë të orarit kyç.



$$RC[1] = x^0 = (0001)_2$$
$$RC[2] = x^1 = (0010)_2$$
$$RC[3] = x^2 = (0100)_2$$

Fig 7: Skema e enkriptimit të AES.

Çelësat e rrumbullakët të gjeneruar nga procesi i zgjerimit të çelësit përdoren më pas në çdo raund të procesit të kriptimit dhe deshifrimit. Çdo çelës i rrumbullakët është XOR me të dhënat në raundin përkatës për të ofruar siguri shtesë.

III. CBC (Cypher Block Chaining)

A. Block Cyphers (Shifra e Bllokut)

Një shifër blloku (block cypher) është një algoritëm kriptografik që kodon të dhënat në blloqe me madhësi fikse. Madhësia e bllokut është zakonisht 64 ose 128 bit, por mund të ndryshojë në varësi të shifrave specifike. Shifrat e bllokut përdoren gjerësisht në shumë aplikacione kriptografike si enkriptimi i diskut, siguria e rrjetit dhe komunikimet e siguurta.

Funksioni themelor i një kodi blloku është të marrë një bllok teksti të thjeshtë të të dhënave dhe ta transformojë atë në një bllok teksti të koduar me të njëjtën madhësi duke përdorur një çelës sekret. Çelësi përdoret për të gjeneruar një grup tabelash zëvendësimi dhe ndryshimi, të cilat më pas aplikohen në bllokun e tekstit të thjeshtë në një seri raundesh. Çdo raund zakonisht përbëhet nga operacione të shumëfishta zëvendësimi dhepermutimii.

Një nga avantazhet kryesore të shifrave të bllokut është aftësia e tyre për të siguruar kriptim të fortë për sasi të mëdha të dhënash. Për shkak se të dhënat janë të koduara në blloqe me madhësi fikse, shifrat e bllokut mund të përdoren për të enkriptuar të dhënat e çdo madhësie. Ato ofrojnë gjithashtu një nivel të lartë sigurie, pasi procesi i kriptimit bazohet në një çelës sekret që duhet të mbahet konfidencial.

Megjithatë, shifrat e bllokut mund të jenë gjithashtu të prekshëm ndaj llojeve të caktuara të sulmeve, të tilla si sulmet me forcë brutale dhe sulmet vetëm me tekst të koduar. Për të zbutur këto rreziqe, kodet e bllokut përdoren shpesh në lidhje me teknika të tjera kriptografike, të tilla si forcimi i çelësave dhe skemat e mënyrës së funksionimit si CBC ose ECB.

B. CBC

CBC ose Cypher block chaining (zinxhiri i blloqeve të shifruara) është një metodë që përdoret në kodet e bllokut për të siguruar konfidencialitet dhe integritet për të dhënat e transmetuara. Ai funksionon duke ndarë tekstin e thjeshtë në blloqe me madhësi fikse, dhe më pas duke XORuar çdo bllok me bllokun e mëparshëm të tekstit të shifruar përpara kriptimit. Ky bllok i bërë XOR më pas enkriptohet me çelësin sekret për të prodhuar tekstin e shifruar.

Blloku i parë i tekstit të thjeshtë bëhet XOR me një vektor inicializimi (IV) përpara enkriptimit, i cili shërben si blloku i parë i tekstit të shifruar. IV duhet të jetë i paparashikueshëm dhe unik për çdo mesazh të koduar me të njëjtin çelës, për të parandaluar sulme të tilla si sulmet e përsëritjes.

Enkriptimi dhe dekriptimi i tekstit të thjeshtë paraqiet më poshtë me anë të formulave dhe diagrameve.

Formulat për enkriptim është:

$$y_1 = E_k(x_1 \oplus IV), \qquad y_i = E_k\left(x_i \oplus y_{i-1}\right), i \geq 2$$

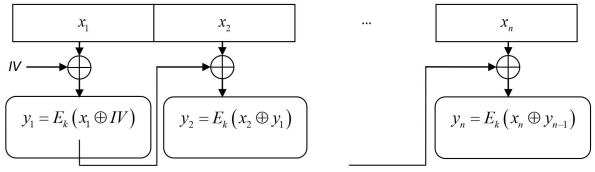


Fig 8: Skema e enkriptimit të CBC.

Formulat për dekriptim janë:

$$x_1 = D_k\left(y_1\right) \oplus IV, \qquad x_i = D_k\left(y_i\right) \oplus y_{i-1}, i \geq 2$$

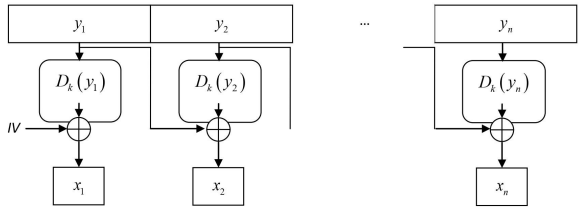


Fig 9: Skema e dekriptimit të CBC.

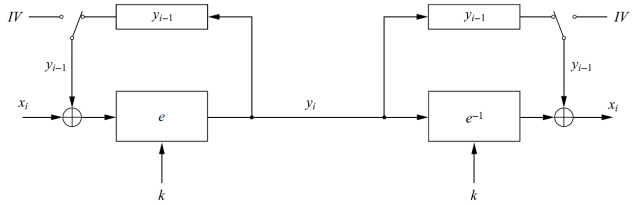


Fig 10: Skema e CBC.

Një nga avantazhet kryesore të CBC është se ai siguron mbrojtje kundër llojeve të caktuara të sulmeve, si p.sh. i njëjti bllok teksti të thjeshtë që prodhon të njëjtin bllok teksti të koduar (i njohur si sulmi i pinguinëve ECB). Për më tepër, çdo ndryshim në tekstin e shifruar do të korruptojë bllokun përkatës të tekstit të thjeshtë dhe të gjitha blloqet pasuese, duke e bërë të vështirë për një sulmues të modifikojë mesazhin pa u zbuluar.

Sidoqoftë, CBC ka disa dobësi të. Nëse një sulmues mund të manipulojë IV ose tekstin e koduar, ai mund të jetë në gjendje të kryejë një sulm të zgjedhur të tekstit të thjeshtë, ku mund të deshifrojë pjesë të tekstit të shifruar dhe të marrë informacion rreth tekstit të thjeshtë. Për më tepër, CBC është i prekshëm ndaj sulmit “padding oracle”, ku një sulmues mund të përdorë gabimet e krijuara gjatë deshifrimit për të rikuperuar informacionin rreth tekstit të thjeshtë.

Për ti ikur këtyre rreziqeve, rekomandohet përdorimi i një IV unik dhe të paparashikueshëm për çdo mesazh të koduar me të njëjtin çelës dhe për të vërtetuar tekstin e shifruar duke përdorur një kod të sigurt të vërtetimit të mesazhit (Message Authentication Code - MAC). Kjo mund të arrihet duke përdorur një mënyrë kriptimi si GCM ose CCM, të cilat kombinojnë enkriptimin dhe vërtetimin në një hap të vetëm.