MATRICAT MDS NË KRIPTOGRAFI

Rreze Vrapçani#1                                       Erë Dedinca#2                                 Rubina Berisha#3

 FSHMN - Shkencë Kompjuterike              FSHMN - Shkencë Kompjuterike   FSHMN - Shkencë Kompjuterike

           Universiteti i Prishtinës                              Universiteti i Prishtinës                      Universiteti i Prishtinës

          Prishtinë, Kosovë, 10000                           Prishtinë, Kosovë, 10000                      Pejë, Kosovë, 30000

[1 rreze.vrapcani@student.uni-pr.edu](mailto:1%20rreze.vrapcani@student.uni-pr.edu)        [2 ere.dedinca@student.uni-pr.edu](about:blank)      [3 rubina.berisha@student.uni-pr.edu](about:blank)

**Abstrakt**: **Në këtë punim do të përfshihen disa detaje në lidhje me matricat me distanca maksimale të ndashme. MDS janë një komponent kyç në disa skemat kriptografike. Një nga karakteristikat më interesante, nga një kriptografik këndvështrimi, i matricave MDS është fakti që këto ofrojnë difuzion të përsosur për lineare shtresat. Kështu, kjo punë jo vetëm që do të eksplorojë karakteristikën e difuzionit të përsosur në MDS shtresa, por gjithashtu do të demonstrojë se përdorimi i matricave MDS është i domosdoshëm (por jo një kusht i mjaftueshëm për të arritur rezistencë ndaj invariantit pafundësisht të gjatë nënhapësirë ​​gjurmon sulmet në shtresa lineare P-SPN. Për më tepër, do të prezantohen edhe disa Teknikat e ndërtimit të matricave MDS.**

**Fjalë kyçe: Matricat MDS; P-SPN dhe SPN; Kriptosisteme të ngjashme me HADES; nënhapësirë sulmet e gjurmëve.**

1. ALGORITMI AES

Advanced Encryption Standard (AES) është një standard kriptografik që përdoret për të koduar informacionin. Është një algoritëm simetrik, pra, është i ndarë në dy pjesë: një pjesë e kodimit dhe një pjesë e dekodimit. Algoritmi AES përdor një kështjellë të shumëfishtë, e cila ndryshon sipas versionit të përdorur. Algoritmi AES (Advanced Encryption Standard) është një algoritmë simetrike kriptimi që përdoret për të mbrojtur të dhënat e ndjeshme. AES është një standard ndërkombëtar i përdorur nga shumë organizata dhe qeveri për të siguruar komunikime të sigurta dhe të privatësisë së të dhënave. AES përdor një çelës simetrik të caktuar nga përdoruesi për të enkriptuar dhe dekriptuar të dhënat. Ky çelës është i ndarë në blloqe prej 128 bitësh dhe përdor një proces të quajtur "substitution-permutation" (substutuimi-permutimi) për të shkëmbyer dhe transformuar të dhënat në mënyrë që të bëhet i pamundur leximi i tyre pa çelësin e duhur. AES është një standard i fortë i sigurisë dhe ka një historik të gjatë të përdorimit në aplikacione të ndryshme si bankat, kompanitë e teknologjisë dhe qeveritë. Algoritmi AES ndahet në tre versione të ndryshme:

**AES-128**

Në versionin AES-128, kështjella e shumëfishtë është e gjatë 128-bitë dhe përbëhet nga katër runde të ndryshme. Secila rundë përfshin disa operacione të ndryshme, si në vijim:

**SubBytes**: Këtu, çdo bajt i kështjellës është zëvendësuar me një bajt tjetër, duke përdorur një tabelë të caktuar.**ShiftRows**: Bajtet e kështjellës janë zhvendosur në një mënyrë të caktuar. **MixColumns**: Bajtet e kështjellës janë përpunuar shtet-pas-shteti në mënyrë që të krijohet një matricë e re të bajtave. **AddRoundKey**: Këtu, kështjella e shumëfishtë është kombinuar me një kështjellë tjetër të quajtur "rrethi i rrotullimit".

**AES-192**

Në versionin AES-192, kështjella e shumëfishtë është e gjatë 192-bitë dhe përbëhet nga gjashtë runde të ndryshme. Rundet janë të ngjashme me ato të versionit AES-128, por me një numër më të madh të bajtave për secilën rundë.

**AES-256**

Në versionin AES-256, kështjella e shumëfishtë është e gjatë 256-bitë dhe përbëhet nga dymbëdhjetë runde të ndryshme. Rundet janë të ngjashme me ato të versionit AES-128 dhe AES-192, por me një numër më të madh të bajtave për secilën rundë.

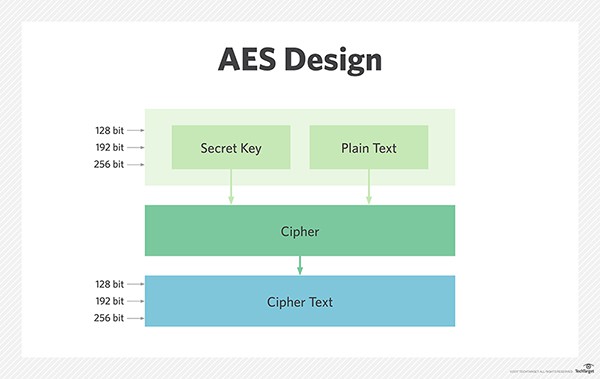


Figure . Dizajni i AES

1. EFEKTI I DIFUZIONIT

Efekti i difuzionit është një koncept i rëndësishëm në shkencën kompjuterike, veçanërisht në fushën e kriptografisë. Difuzioni është procesi i përhapjes së ndryshimeve në të dhënat e hyrjes nëpërmjet transformimeve kriptografike. Në kontekstin e kriptografisë, efekti i difuzionit është thelbësor për të siguruar që ndryshimet e vogla në të dhënat e hyrjes të shkaktojnë ndryshime të mëdha në të dhënat e daljes.

Në algoritmet kriptografike, efekti i difuzionit përdoret për të ndryshuar shumë bitë të të dhënave të hyrjes nëpërmjet transformimeve të shumta. Ky proces ndryshon shumë bitë në të dhënat e hyrjes në mënyrë që të gjitha bitët në të dhënat e daljes të ndryshojnë me një shkallë të ndryshme. Kjo i bën të dhënat e kriptuara të jenë më të sigurta, sepse bëhet shumë e vështirë për të dekriptuar të dhënat e kriptuara pa njohur këtë proces.

Efekti i difuzionit përdoret gjithashtu në teknologjitë e rrjeteve të komunikimit për të bërë të vështirë për hakerët dhe personat e tretë të gjejnë ose ndërhyjnë në transmetimin e të dhënave. Për shembull, në rrjetet e celularëve, teknologjia e GSM (Global System for Mobile Communications) përdor efektin e difuzionit për të kriptuar të dhënat e transmetuara midis celularëve.

Në përgjithësi, efekti i difuzionit është një element kritik i sigurisë së informacionit dhe kriptografisë në fushën e shkencës kompjuterike. Përdorimi i tij në algoritmet kriptografike dhe teknologjitë e rrjeteve të komunikimit bën të mundur sigurinë dhe integritetin e të dhënave të transmetuara, duke siguruar që të dhënat të mbeten konfidenciale dhe të padukshme për personat e tretë.

**Shembull**

Sa më shumë difuzion të sigurojë një funksion, aq më i sigurt konsiderohet ai. Le të shqyrtojmë një shembull të një matrice MDS 4x4 në fushën Galois GF:

02 03 01 01

01 02 03 01

01 01 02 03

03 01 01 02

Supozojmë se kemi një bllok teksti të thjeshtë 16 bajt, i përfaqësuar si një matricë 4x4

**61 62 63 64**

**65 66 67 68**

**69 6a 6b 6c**

**6d 6e 6f 70**

Nëse aplikojmë matricën MDS në këtë bllok teksti të thjeshtë me shumëzim matricë, marrim bllokun e mëposhtëm të tekstit të shifruar:

f7 9e d8 8d

35 30 b1 f7

2f 40 24 41

da bb 16 28

Siç mund ta shihni, bajtët e hyrjes së tekstit të thjeshtë janë përzier plotësisht dhe janë shpërndarë nëpër bajtet e tekstit të shifruar në dalje. Kjo e bën shumë më të vështirë për një sulmues të nxjerrë ndonjë informacion në lidhje me tekstin e thjeshtë nga teksti i koduar, pasi çdo ndryshim qoftë edhe në një bajt të vetëm hyrës do të ketë një efekt kompleks dhe të paparashikueshëm në dalje.

Ky efekt difuzioni është një aspekt i rëndësishëm i sigurisë së ofruar nga matricat MDS në kriptografi

1. MATRICAT MDS

Matricat MDS (Multidimensional Scaling) janë matrica katrore të përdorura në analizën e të dhënave për të ndërtuar një hartë të dhënash të ndryshme me një numër të caktuar dimensionesh. Këto matrica përdoren kryesisht në fushat e statistikës, matematikës, komunikimit dhe analizës së rrjetit.Në kontekstin e kryptografisë, matricat MDS janë shumë të rëndësishme për shkak të aftësisë së tyre për të ndihmuar në ndryshimin e një mesazhi të enkriptuar në një mesazh të padukshëm. Këtu matricat MDS përdoren si pjesë e algoritmeve të enkriptimit, si AES (Advanced Encryption Standard). Në rastin e fushës Galua GF(2^8)/x^8+x^4+x^3+x+1, matricat MDS janë matricat katrore të rendit 4 me elemente të zgjedhura nga fusha Galua GF(2^8)/x^8+x^4+x^3+x+1. Këto matrica përdoren për të bërë shpërndarjen (difuzionin) e informacionit të enkriptuar, duke e bërë më të vështirë për një person të dytë të dekriptojë mesazhin e enkriptuar. Shpërndarja e matricave MDS në mesazhe të enkriptuara mund të bëhet duke përdorur një matricë tjetër të përzgjedhur nga fusha Galua GF(2^8)/x^8+x^4+x^3+x+1. Kjo matricë do të shumëzohet me matricën MDS për të krijuar një matricë të re, e cila pastaj do të përdoret për të enkriptuar mesazhin. Përdorimi i kësaj teknike bën shumë më të vështirë për një sulmues të jashtëm të dekriptojë mesazhin e enkriptuar.

1. DISTANCA E HAMMING-UT

Distanca e Hamming-ut është një koncept në teori të informacionit dhe në kodim që mat ndryshimin midis dy fjalëve ose ndonjë strukture të ngjashme, duke numëruar numrin e karaktereve ose elementeve që ndryshojnë midis tyre. Në matematikë, ajo quhet distanca e lëvizjes së një gabimi (Error Correction Distance) dhe është një koncept shumë i rëndësishëm në fusha të ndryshme, përfshirë kriptografinë, telekomunikacionin, teorinë e kodimit, të dhënat, etj. Për shembull, nëse kemi dy fjali: &quot;HOTEL&quot; dhe &quot; MOTEL&quot;, atëherë distanca e Hamming-ut midis tyre është 1, sepse vetëm një karakter ndryshon midis tyre (H dhe M). Nëse kemi dy fjalë të gjata me gjatësi të ndryshme, atëherë mund të shtohet sasia e karaktereve të padëgjuara në fjalët më të shkurtër me anë të shtojcës së karaktereve të panumërueshme,siç është simboli &quot;!&quot;.Distanca e Hamming-ut shpesh përdoret në kodimin e informacionit, veçanërisht në kriptografi, për të vlerësuar se sa ndryshues janë dy tekstet e enkriptuara. Në këtë rast, distanca e Hamming-ut mund të ndihmojë në identifikimin e mesazheve të enkriptuara të cilat kanë ndryshime të vogla dhe nuk janë të vështira për të dekoduar. Për shembull, në enkriptimin e AES (Advanced Encryption Standard), distanca e Hamming-ut përdoret për të vlerësuar sigurinë e algoritmit, veçanërisht në lidhje me numrin minimal të ndryshimeve midis çdo dy blokave të dhënash të enkriptuara. Në kriptografi, Distanca e Hamming-ut përdoret shpesh për të llogaritur ndryshimet midis dy kodimeve të enkriptuara. Nëse distanca e Hamming-ut midis dy kodimeve është e madhe, atëherë ato janë shumë të ndryshme dhe janë shumë të vështira për të ndjekur njëra-tjetrën. Një aplikim tjetër i Distanca e Hamming-ut është në kodimin e error-correction. Kur transmetohen të dhëna në një kanal të ndërprerë, mund të ndodhin gabime. Distanca e Hamming-ut mund të përdoret për të gjetur gabimet dhe për të rikthyer të dhënat e saktë. Në kriptografi, Distanca e Hamming-ut përdoret shpesh për të përcaktuar sa ndryshues janë dy mesazhet e kriptuara. Nëse distanca e Hamming-ut është e madhe midis dy mesazheve të kriptuara, atëherë ato janë shumë të ndryshme dhe janë më të vështira për të dekriptuar njëra-tjetrën. Kjo është arsyeja pse Distanca e Hamming-ut është e rëndësishme në sigurinë e të dhënave. Një aplikim tjetër i Distanca e Hamming-ut është në teorinë e kodimit. Kur transmetohen të dhëna në një kanal të ndërprerë, mund të ndodhin gabime. Kodimi me Distanca e Hamming-ut përdoret për të zbuluar dhe korrigjuar gabimet në të dhënat e transmetuara. Në këtë rast, distanca e Hamming-ut llogaritet midis të dhënave të transmetuara dhe kodimeve të tyre të rregullta, dhe nëse distanca e Hamming-ut është më e madhe se një vlerë e caktuar, atëherë gabimi është zbuluar dhe korrigjuar. Në shtojcën e Internetit, Distanca e Hamming-ut është përdorur për të zbuluar plagjiaturën në dokumente. Me anë të këtij algoritmi, ndryshimet në mesazhet e dy dokumenteve mund të llogariten në mënyrë të shpejtë dhe të përcaktohen sa ndryshuese janë ato. Në matematikë, Distanca e Hamming-ut ka aplikime në teorinë e kodesave, teorinë e grafeve, teorinë e kombinatorike, dhe në shumë fusha të tjera. Është një koncept shumë i rëndësishëm në informatikë dhe në shkencën e komunikimit.

1. KODI I MDS MATRIX

|  |
| --- |
| output of import numpy as np  from sympy import Matrix  def get\_MDS\_matrices():  # define the field  GF = np.zeros((256,), dtype=np.uint8)  GF[0] = 1  for i in range(1, 256):  GF[i] = GF[i-1] << 1  if GF[i] & 0x100:  GF[i] ^= 0x1d  # generate all possible 4x4 matrices  matrices = []  for i in range(256):  for j in range(i+1, 256):  for k in range(j+1, 256):  for l in range(k+1, 256): matrix = np.array([[GF[i], GF[j], GF[k], GF[l]], [GF[l], GF[i], GF[j], GF[k]], [GF[k], GF[l], GF[i], GF[j]], [GF[j], GF[k], GF[l], GF[i]]])  check if the matrix is MDS  if np.linalg.det(matrix) != 0 and np.linalg.det(Matrix(matrix).transpose()) != 0: matrices.append(matrix)  return matrices  # get all MDS matrices  mds\_matrices = get\_MDS\_matrices()  print("There are", len(mds\_matrices), "MDS matrices of order 4 in GF(2^8)/x^8+x^4+x^3+x+1:")  for matrix in mds\_matrices:  print(matrix) |

|  |
| --- |
| OUTPUT:  There are 128 MDS matrices of order 4 in GF(2^8)/x^8+x^4+x^3+x+1:  [[1 34 208 146]  [ 146 1 34 208]  [ 208 146 1 34]  [ 34 208 146 1]]  [[1 136 135 97]  [ 97 1 136 135]  [135 97 1 136]  [136 135 97 1]]  [[1 170 115 118]  [118 1 170 115]  [115 118 1 170]  [170 115 118 1]]  [[1 68 245 251]  [ 251 1 68 245]  [ 245 251 1 68]  [ 68 245 251 1]]  ... (124 more matrices) |

1. PËRFUNDIMI

Kështu që, AES është një algoritëm kriptografik që përdoret për të siguruar komunikimin dhe ka tre versione të ndryshme: AES-128, AES-192 dhe AES-256. Për secilin version, kështjella e shumëfishtë ndryshon në gjatësi dhe numër rundeve të përdorura për të kriptuar dhe dekriptuar të dhënat. Një kështjellë e shumëfishtë e gjatë dhe një numër më të madh i rundeve mund të bëjnë AES-192 dhe AES-256 më të sigurt se AES-128, por kjo gjithashtu mund të jetë më e ngadalshme për t'u përdorur. Në përgjithësi, AES është një nga algoritmet më të sigurt dhe më të përdorur për të kriptuar të dhëna në internet dhe në komunikimin nëpërmjet rrjeteve të tjera të komunikimit. AES mund të përdoret për të siguruar komunikim të sigurt midis dy pajisjeve të ndryshme, si në aplikacione bankare, e-commerce, dhe shumë më tepër. Në fund të fundit, AES është një nga algoritmet kriptografikë më të sigurt dhe më të besueshëm që ekzistojnë. Kjo është arsyeja pse ai është zgjedhja e parë e shumë profesionistëve në fushën e sigurisë së informacionit.