UNIVERSITETI I PRISHTINËS “HASAN PRISHTINA”

FAKULTETI I SHKENCAVE MATEMATIKO – NATYRORE

Departamenti: Matematikë | Programi: Shkenca Kompjuterike



Siguria e të dhënave

**MDS dhe Fusha Galois**

**Punuar nga:**

Benita Mehmeti

Erona Gashi

**Maj 2023**

# Përshkrimi I detyrës

Krijoni një aplikacion që do të gjejë matrica MDS të rendit 4 në fushën Galois GF(28) / x8+x4+x3+x+1. Pastaj tregoni efektin e shpërndarjes (difuzionit) së këtyre matricave me anë të një shembulli. Pra e gjeneroni një matricë të rendit 4 x n (n është shumëfish i numrit 4) me elemente të cfarëdoshme nga fusha Galois GF(28) / x8+x4+x3+x+1 e cila pastaj shumëzohet me matricën e gjetur MDS, pra B = MDS x A.

# MDS

MDS qëndron për Maximum Distance Separable dhe në kontekstin e korrigjimit të gabimeve në kode dhe kriptografi, MDS i referohet klasës së kodeve ose matricave që kanë vetinë e rritjes së distancës më të vogël të Hammingut mes dy fjalëve apo rreshtave.

Matricat e MDS janë matrica katrore me vetinë që çdo nënmatricë katrore e formuar duke zgjedhur ndonjë nëngrup të rreshtave të saj është jo njëjës, që do të thotë se ka renditje të plotë. Kjo veti siguron ndarje maksimale të distancës, duke i bërë matricat MDS të dobishme në aplikacione të ndryshme kriptografike, si p.sh. difuzioni në shifrat e bllokut.

Matricat MDS shpesh përdoren në hartimin e kodeve të korrigjimit të gabimeve dhe algoritmeve kriptografike për të siguruar qëndrueshmëri ndaj gabimeve dhe për të rritur sigurinë. Duke maksimizuar distancën minimale midis fjalëve të koduara ose rreshtave, kodet dhe matricat MDS mund të zbulojnë dhe korrigjojnë një numër më të madh gabimesh dhe gjithashtu mund të përhapin efektin e ndryshimeve në të gjithë fjalën e koduar ose matricën, gjë që rrit shpërndarjen e informacionit.

# Fusha Galois

Fusha Galois ose e njohur ndryshe si fushë e fundme, është një strukturë matematikore që shfaq veti të ngjashme me ato të fushave të njohura si numra realë ose racionalë. Megjithatë, ndryshe këto fusha të pafundme, fushat Galois kanë një numër të kufizuar elementesh.

Një fushë Galois shënohet si GF(q), ku "q" përfaqëson numrin e elementeve në fushë. Renditja e fushës Galois jepet nga q, e cila duhet të jetë një fuqi e thjeshtë. Për shembull, GF(2) është një fushë me dy elemente {0, 1} dhe GF(3) është një fushë me tre elementë {0, 1, 2}.

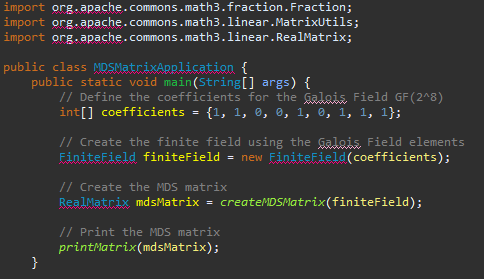
Veprimet aritmetike në një fushë Galois përcaktohen bazuar në aritmetikën modulare. Veprimet e mbledhjes dhe shumëzimit kryhen modulo q, ku q është rendi i fushës. Operacioni i mbledhjes ndjek vetitë e njohura të komutativitetit, asociativitetit dhe ekzistencës së një identiteti shtesë dhe të anasjelltë. Operacioni i shumëzimit i posedon gjithashtu këto veti, përveç mungesës së inverseve shumëzuese për identitetin shtesë (0).

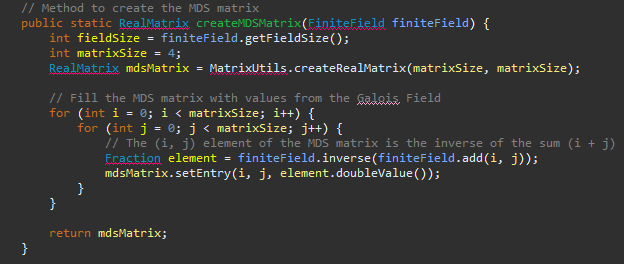
Fushat Galois gjejnë aplikime të gjera në fusha të ndryshme të matematikës, shkencave kompjuterike dhe inxhinierisë. Ato janë veçanërisht të rëmdësishme në kodet e korrigjimit të gabimeve, kriptografinë, teorinë e kodimit dhe përpunimin e sinjalit digjital. Fushat Galois ofrojnë një kornizë të fundme dhe algjebrike për adresimin e problemeve që përfshijnë sisteme të fundme dhe diskrete, duke mundësuar llogaritje efikase dhe aftësi për zbulimin/korrigjimin e gabimeve.

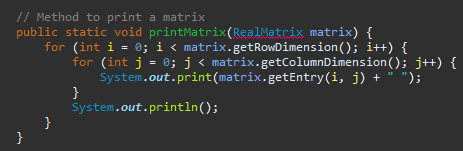
Fushat Galois ofrojnë strukturën matematikore dhe operacionet e nevojshme për ndërtimin e kodeve dhe matricave MDS. Vetitë e fundme dhe algjebrike të fushave Galois mundësojnë dizajnimin e kodeve korrigjuese të gabimeve dhe sistemeve kriptografike me vetitë e dëshirueshme të distancës dhe llogaritjet efikase, për këtë arsye kodet MDS zakonisht konstruktohen përmes fushave Galois.

# Implementimi në Java

Në kodin tonë, së pari definojmë koeficientët për fushën Galois GF(28) / x8+x4+x3+x+1 dhe krijojmë objektin **FiniteField** për të paraqitur fushën. Pastaj, metoda **createMDSMatrix** gjeneron matricën MDS duke e mbushur atë me vlera nga fusha Galois. Në fund, metoda **printMatrix** përdoret për të paraqitur matricën në konzolë.

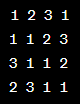






# Efekti I shpërndarjes (Difuzioni)

Efektin e shpërndarjes te këto matrica do ta ilustrojmë me një shembull të thjeshtë. Supozojmë se kemi një matricë MDS 4 x 4 në fushën Galois GF(28) / x8+x4+x3+x+1:

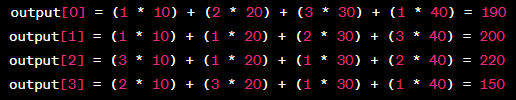


Poashtu, le të supozojmë se kemi një mesazh input të dhënë në formën e një vektori me 4 elemente:



Për të aplikuar efektin e shpërndarjes duke përdorur matricën MDS, performojmë prodhimin matricor mes secilit rresht të matricës dhe mesazhit input të dhënë në formën e vektorit me 4 elemente. Vektori rezultues do të jetë outputi pas difuzimit:







Sic shihet, vlerat e outputit janë dukshëm të ndryshme nga vlerat e inputit, indikacion ky i një vlere të lartë të difuzionit. Edhe ndryshimet më të vogla në input rezultojnë në ndryshime substanciale të outputit si rrjedhojë e vetive të matricës MDS.

Difuzioni është një veti shumë e rëndësishme e algoritmeve kriptografike, pasi që ndihmon në sigurimin e faktit që secili ndryshim në input të ketë efekt në tërë outputin, duke e bërë kështu sfiduese dallimin e lidhjeve mes të dhënave origjinale dhe atyre të modifikuarave.