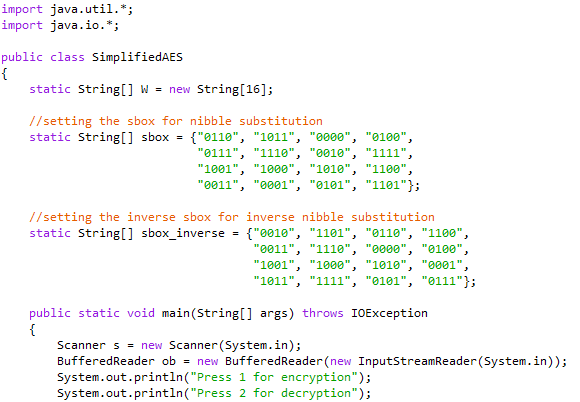
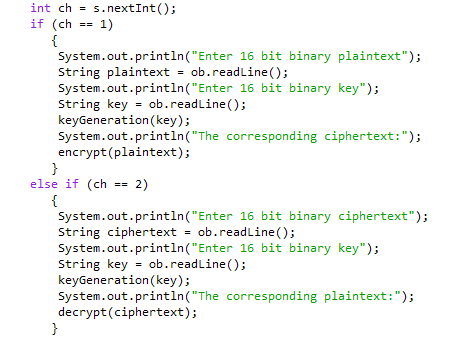
# PROJEKTI I DYTË

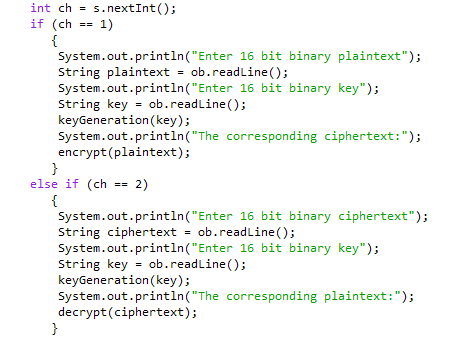
Në dokumentin “AES i thjeshtuar (Simplified AES).pdf” është dhënë skema e algoritmit AES i thjeshtuar (veprimet gjatë raundeve te algoritmi AES i thjeshtuar).

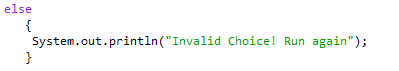
1. Implementoni në Java skemën e enkriptimit dhe dekriptimit bazuar në skemën e algoritmit AES i thjeshtuar. Aplikacioni duhet të marrë si hyrje çelësin sekret dhe nje tekst dokument (text file) dhe të bëjë enkriptimin/dekriptimin e përmbajtjes së atij tekst dokumenti.

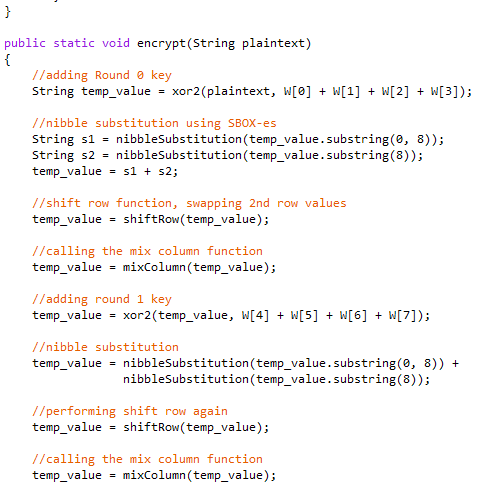
Për zgjidhjen e kësaj detyre kam krijuar klasën në vijim SimplifiedAES e cila merr si hyrje një tekst dhe një çelës të madhësisë 16 bit.

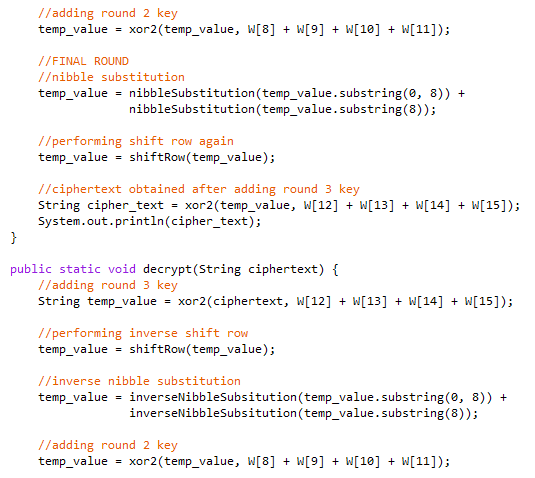


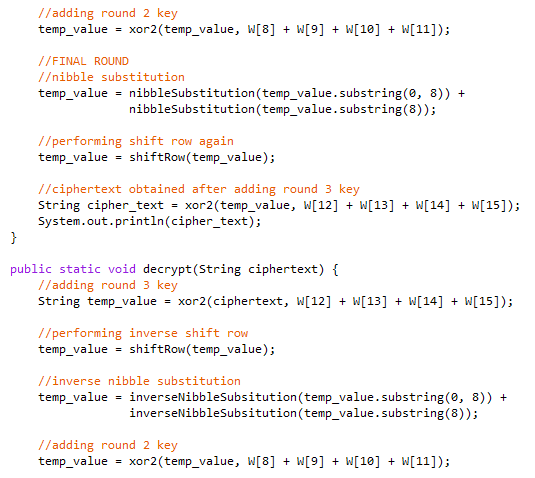


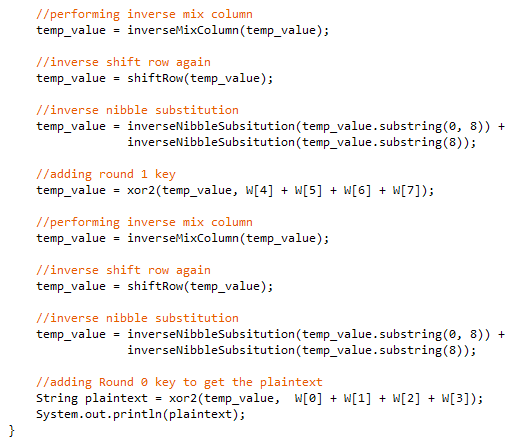


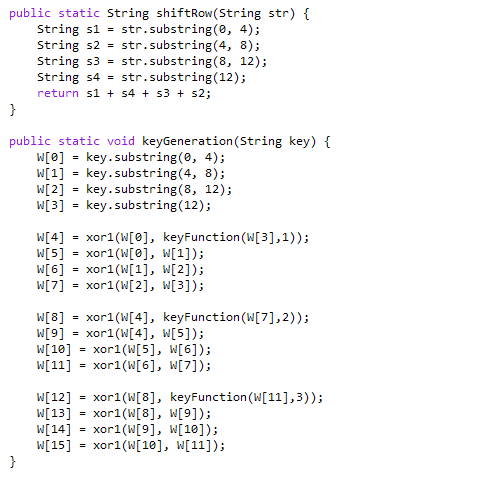


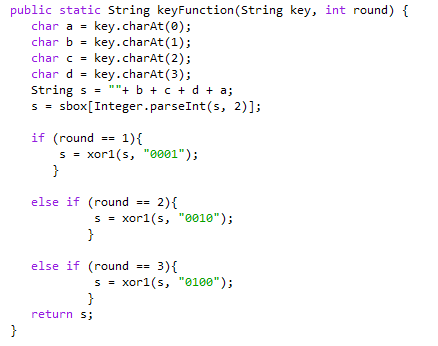


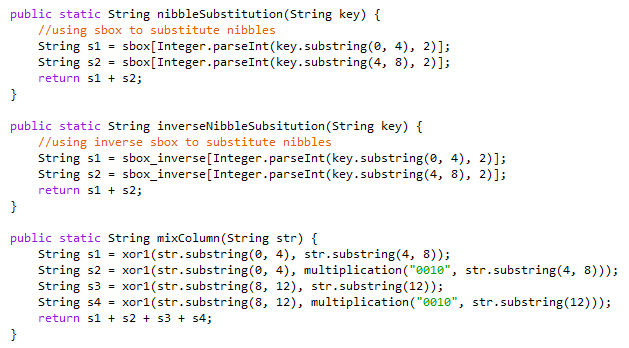


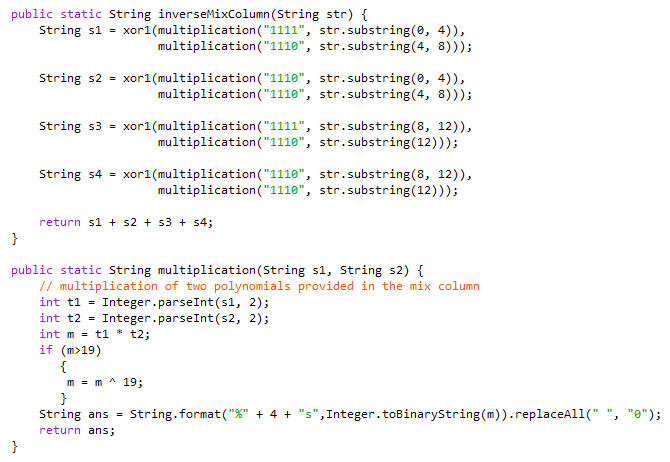


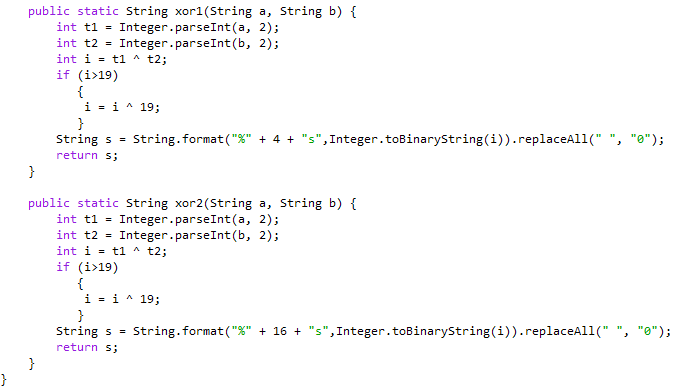








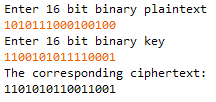




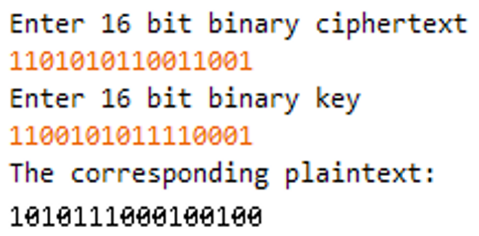
Pas ekzekutimit të programit, shfrytëzuesi duhet të zgjedh se a do të bëj enkriptimin apo dekriptimin e atij teksti.



SHEMBULL – Supozojmë se shfrytëzuesi dëshiron të bëjë enkriptimin e tekstit. Në këtë rast ai/ajo duhet të shtyp numrin 1 në tastierë. Le të jenë teksti 1010111000100100 dhe celësi 1100101011110001 hyrje të dhëna nga shfrytëzuesi.



Rezultati i fituar është teksti 1101010110011001. Tani provojmë të bëjmë dekriptimin.

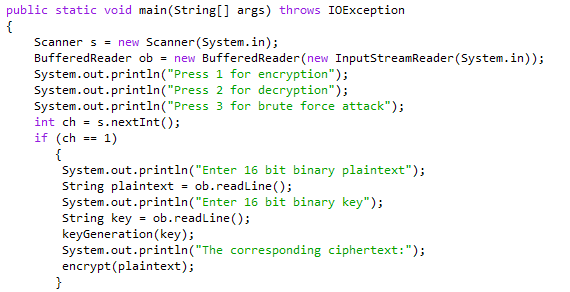


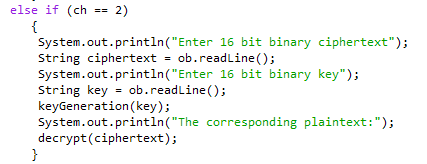
1. Implementoni në Java algoritmin AES i thjeshtuar nga dokumenti AES i thjeshtuar (Simplified AES).pdf në mënyrën e enkriptimit/dekriptimit CBC, OFB, CFB, CTR dhe GCM? (2 pikë) Sqarim: Te secila mënyrë e enkriptimit/dekriptimit duhet të kihen parasysh parametrat hyrës përkatës. Te GCM duhet të zgjedhni polinomin ireducibil.

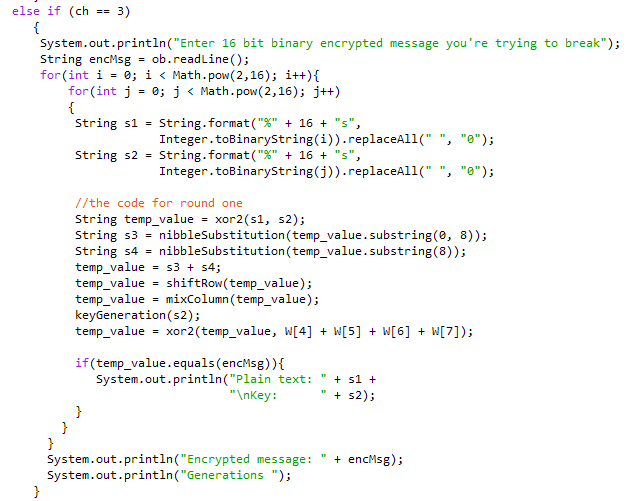
X

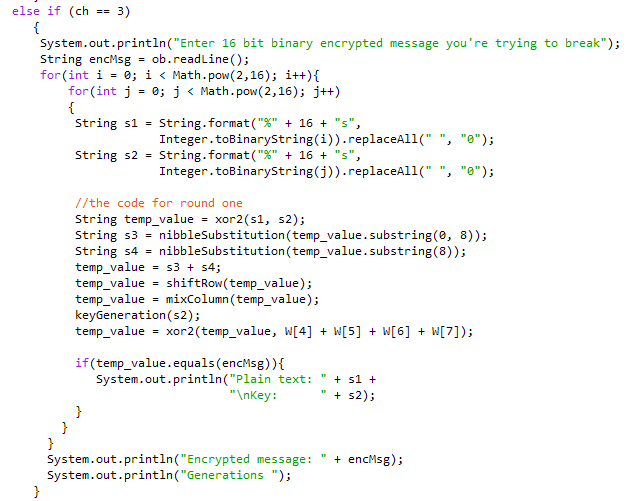
1. Implementoni sulmin e kriptanalizës diferenciale lineare në raundin e parë të AES të thjeshtuar?

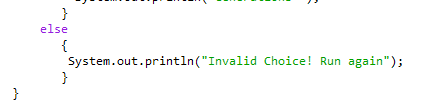
Në klasën e mëparshme SimplifiedAES kam shtuar disa urdhëra për të bërë një sulm Brute Force në raundin e pare të AES të thjeshtuar.



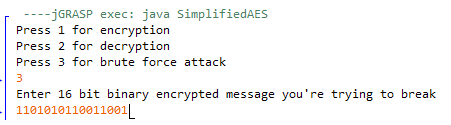




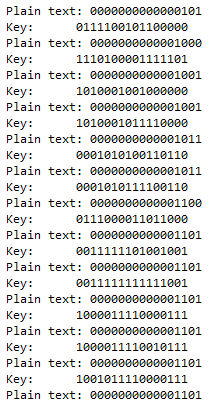




SHEMBULL – Pas ekzekutimit të kodit shtypim në tastierë numrin 3 dhe pastaj japim stringun e bitëve.



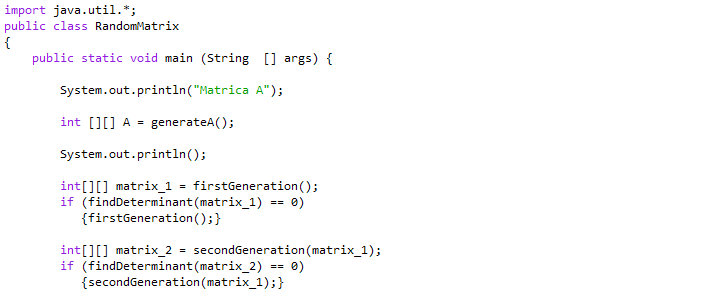
E lëmë programin të kërkojë cifte të formës (plaintext, key) të cilat i përshtaten enkriptimit të tekstit të dhënë.

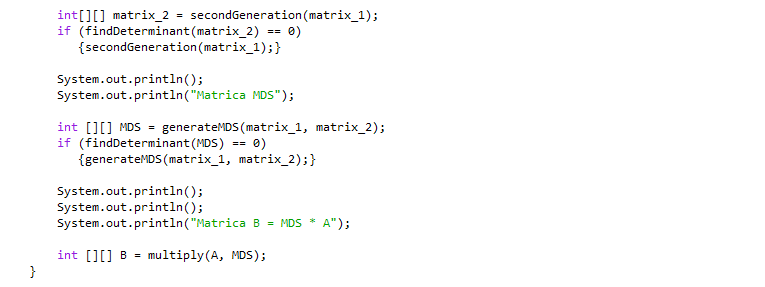


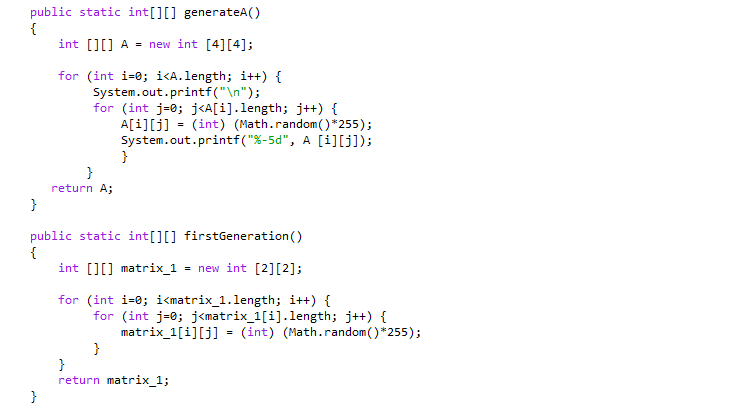
…

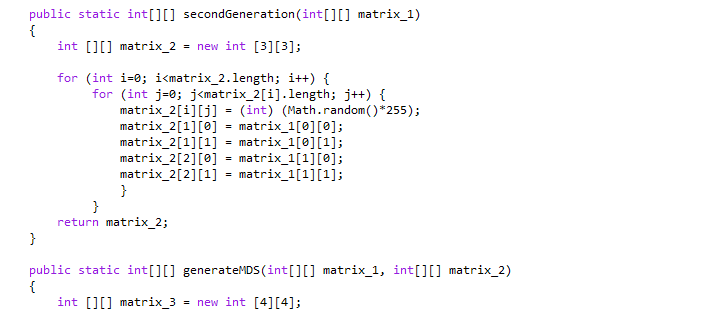
1. Krijoni një aplikacion që do të gjejë matrica MDS të rendit 4 në fushën Galua  Pastaj tregoni efektin e shpërndarjes (difuzionit) së këtyre matricave me anë të një shembulli.

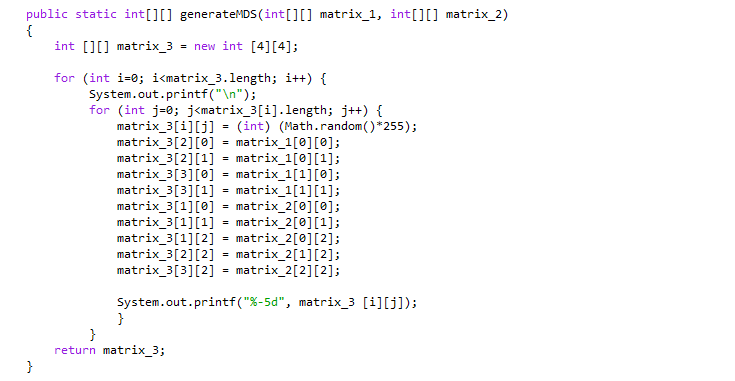
Kam krijuar një klasë RandomMatrix që e bë edhe gjenerimin e matricës A edhe atë të matricës MDS e pastaj kam përfituar matricën B si prodhim A \* MDS.

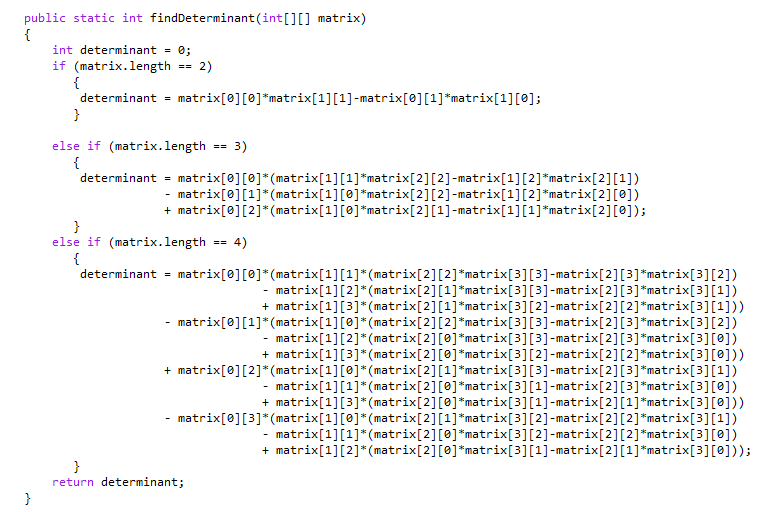


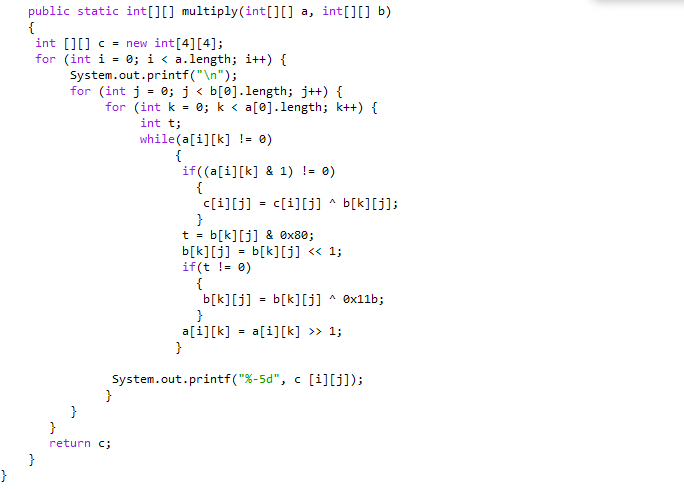












Nuk kam arritur të implementoj në java një kod për pjesën e difuzionit.