**SAES**

SAES është një version i thjeshtuar i AES që operon në blloqe të dhënave prej 16 bitësh dhe përdor një çelës prej 16 bitësh. Ai kryen veprime zëvendësimi, lëvizje rreshtash dhe përzjerje kolonash për të fshehur dhe përhapur të dhënat. Këto hapa sigurojnë konfuzion, shpërndarje dhe kompleksitet të shtuar. SAES përsërit këto hapa për tre raunde, duke përfshirë edhe çelësat e raundeve. Rezultati është ciphertext-i i enkriptuar. Procesi i dekriptimit ndjek një proces të ngjashëm në drejtim të kundërt. SAES e balancon thjeshtësinë me veprimet kryesore të enkriptimit për sigurinë e të dhënave.

A screen shot of a computer program

Description automatically generated with low confidence

Kodi i dhënë implementon algoritmin AES të thjeshtuar (SAES).

1. Inicializimi: Kodi fillon duke deklaruar dhe inicializuar matricat e S-Box dhe inversit S-Box. Këto matrica përdoren për zëvendësim në procesin e enkriptimit dhe dekriptimit. Gjithashtu, inicializohet edhe mapa "hex", e cila përdoret për konvertimin nga heksadecimal në binar.
2. Enkriptimi (metoda "encrypt"): Metoda "encrypt" merr si hyrje plaintextin dhe çelësin dhe kthen tekst të enkriptuar (ciphertext). Plaintexti dhe çelësi konvertohen fillimisht në blloqe 16-bitë duke përdorur funksionin "fill". Pastaj, realizohet operacioni "XOR" ndër-bitar midis bllokut të plaintextit dhe bllokut të çelësit, dhe rezultati ruhet në matricën "B".

A screen shot of a computer program

Description automatically generated with medium confidence

Procesi i enkriptimit përbëhet nga tre raunde. Në çdo raund, kryhen hapat vijues: a. Zëvendësimi: Matrica "B" zëvendësohet me vlera nga S-Box duke përdorur funksionin "substitute". b. Lëvizja e Rreshtave: Rreshtat e matricës "B" lëvizin në mënyrë ciklike. c. Përzjerja e Kolonave: Kolonat e matricës "B" (përveç në raundi të fundit) përzihen duke përdorur një operacion përzjerje të kryer nga funksioni "mixColumns". d. Shtimi i Çelësit të Raundit: Çelësi i raundit shtohet në matricën "B" duke përdorur metodën "RoundKey.addRoundKey".

Pas tre raundeve, matrica rezultuese "C" kthehet përsëri në formë stringu dhe kthehet si ciphertext.

A picture containing text, screenshot, display, software

Description automatically generated

1. Dekriptimi (metoda "decrypt"): Metoda "decrypt" merr si hyrje ciphertextin dhe çelësin dhe kthen plaintextin e dekriptuar. Ciphertexti dhe çelësi fillimisht konvertohen në blloqe 16-bitë duke përdorur funksionin "fill". Çelësi i raundeve "K0", "K1" dhe "K2" llogariten nga çelësi origjinal duke përdorur metodën "RoundKey.addRoundKey".

A picture containing text, screenshot, software, multimedia software

Description automatically generated

Procesi i dekriptimit është i ngjashëm me enkriptimin, por me disa dallime. Hapat përfshijnë: a. Shtimi i Çelësit të Raundit: Çelësi i raundit të fundit "K3" shtohet në bllokun e ciphertextit "Encrypted" duke përdorurfunksionin "xOrMatrix".

b. Lëvizja e Rreshtave: Rreshtat e matricës "B" lëvizin në mënyrë ciklike.

c. Zëvendësimi: Matrica "B" zëvendësohet me vlera nga inversi i S-Box duke përdorur funksionin "substitute".

d. Përzjerja e Kolonave: Kolonat e matricës "B" (përveç në raundin e parë dhe të fundit) përzihen duke përdorur një operacion përzjerje të kryer nga funksioni "mixColumns".

Pas raundeve të dytë dhe të tretë, matrica rezultuese "T" përpunohet përsëri në rradhë të kundërt, dhe blloku origjinal i plaintextit "L" fitohet duke shtuar çelësin e raundit "K0" duke përdorur funksionin "xOrMatrix". Blloku rezultues i plaintextit konvertohet përsëri në string dhe kthehet

A picture containing text, screenshot, display, software

Description automatically generated

1. Funksionet Ndihmëse:
   * "xOrMatrix": Kryen operacionin "XOR" midis dy matricave.
   * "substitute": Zëvendëson vlerat në një matricë duke përdorur S-Box-in e dhënë.
   * "shiftRows": Kryen lëvizjen ciklike të rreshtave në një matricë.
   * "mixColumns": Kryen operacionin e përzjerjes së kolonave në një matricë.
   * "toNibbleArray": Konverton një string binar në një varg nibblesh (vlera 4-bitëshe).
   * "fill": Konverton një string (plaintext ose çelës) në formatin e bllokut 16-bitë.

A screen shot of a computer program

Description automatically generated with low confidence