UNIVERSITATEA TEHNICĂ „Gheorghe Asachi” din IAȘI
FACULTATEA DE AUTOMATICĂ ȘI CALCULATOARE

Implementare AES în C++
Documentație

Proiect la disciplina *CSD*

Student(ă)
Ungureanu Alex-Mihai

Iași, 2021

Ce este AES?

AES (de la Advanced Encryption Standard - în limba engleză, Standard Avansat de Criptare), cunoscut şi sub numele de Rijndael, este un algoritm standardizat pentru criptarea simetrică, pe blocuri, folosit astăzi pe scară largă în aplicaţii şi adoptat ca standard de organizaţia guvernamentală americană NIST. Standardul oficializează algoritmul dezvoltat de doi criptografi belgieni, Joan Daemen şi Vincent Rijmen şi trimis la NIST pentru selecţie sub numele Rijndael.

Descrierea algoritmului AES

• AES operează cu matrici de 4x4 octeţi.

• Pentru criptare, fiecare rundă AES execută următorii paşi:

1.SubBytes() – substituţie în care fiecare octet este înlocuit cu un altul cu ajutorul unei "look-up table"

2.ShiftRows() – transpoziţie ciclică cu un anumit număr de paşi

3.MixColumns – o operaţie de amestec ce foloseşte o funcţie polinomială

4.AddKeyRound() – fiecare octet este combinat cu o cheie specifică rundei, ce a fost în prealabil calculată din cheia iniţială

Pasul SubBytes

Pasul SubBytes este un cifru cu substituţie, fără punct fix, denumit Rijndael S-box, care rulează independent pe fiecare octet din state. Această transformare este neliniară şi face astfel întreg cifrul să fie neliniar, ceea ce îi conferă un nivel sporit de securitate. Fiecare octet este calculat astfel:.

$$b'_i = b_i \oplus b_{(i+4) mod 8} \oplus b_{(i+5) mod 8} \oplus b_{(i+6) mod 8} \oplus b_{(i+7) mod 8} \oplus c_i$$

unde bi este bitul corespunzător poziţiei i din cadrul octetului, iar ci este bitul corespunzător poziţiei i din octetul ce reprezintă valoarea hexazecimală 63, sau, pe biţi, 01100011. Maparea octeţilor se poate reţine într-un tabel, explicitat în FIPS PUB 197, în care este specificat rezultatul operaţiei de mai sus efectuată pe fiecare din cele 256 de valori posibile reprezentabile pe un octet.

Pasul ShiftRows

Pasul ShiftRows operează la nivel de rând al matricii de stare state. Pasul constă în simpla deplasare ciclică a octeţilor de pe rânduri, astfel: primul rând nu se deplasează; al doilea rând se deplasează la stânga cu o poziţie; al treilea rând se deplasează la stânga cu două poziţii; al patrulea se deplasează la stânga cu trei poziţii. Rezultatul acestui pas este că fiecare coloană din tabloul state rezultat este compusă din octeţi de pe fiecare coloană a stării iniţiale. Acesta este un aspect important, din cauză că tabloul state este populat iniţial pe coloane, iar paşii ulteriori, inclusiv AddRoundKey în care este folosită cheia de criptare, operaţiile se efectuează pe coloane.

Pasul MixColumns

In acest pas, fiecare coloana a tabloului de stare este considerata un polinom de gradul 4 peste corpul Galois F28. Fiecare coloana, tratata ca polinom, este înmulțită, modulo x4 + 1 cu polinomul a(x) = 3x3 + x2 +x + 2. Operația se poate scrie ca înmulțire de matrice astfel:

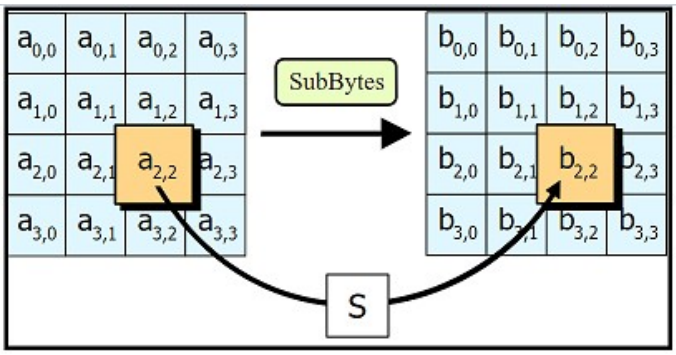
$$\begin{bmatrix} s'_0 \\ s'_1 \\ s'_2 \\ s'_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix}$$

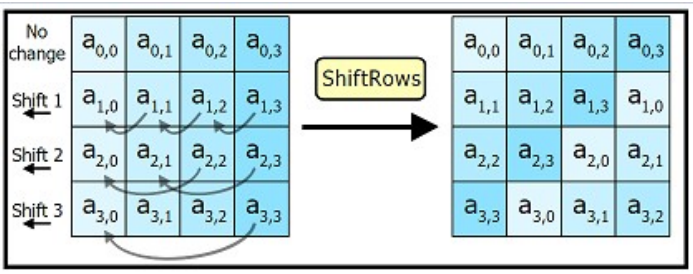
unde ***si'*** sunt elementele de pe un vector coloana rezultate in urma inmultirii, iar ***si*** sunt elementele de pe același vector înaintea aplicării pasului.

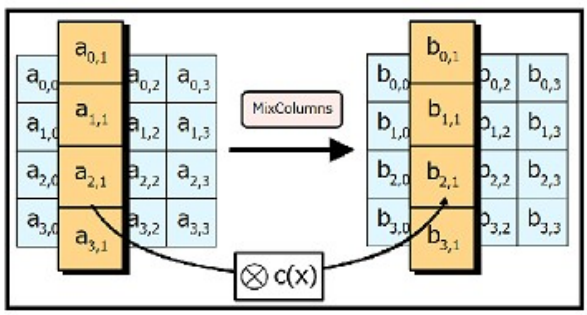
Pasul AddRoundKey şi planificarea cheilor

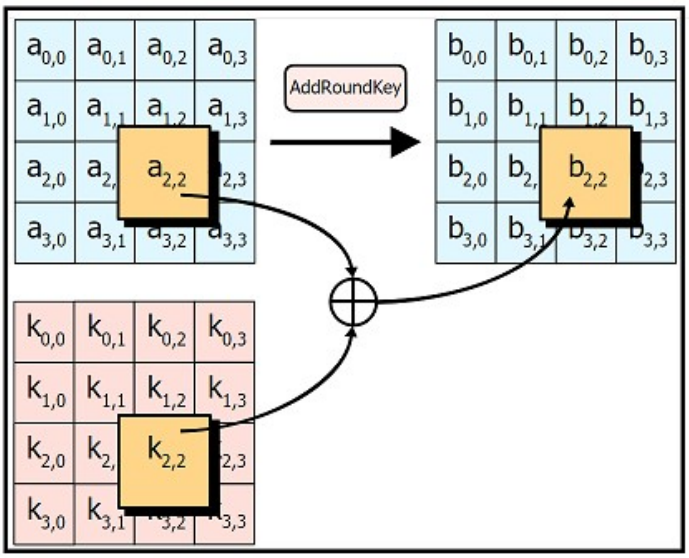
Pasul AddRoundKey este pasul în care este implicata cheia. El consta într-o simpla operație de „sau" exclusiv pe biți intre stare şi cheia de runda (o cheie care este unica pentru fiecare iterație, cheie calculata pe baza cheii secrete). Operația de combinare cu cheia secreta este una extrem de simpla si rapida, dar algoritmul rămâne complex, din cauza complexității calculului cheilor de runda (Key Schedule), precum şi a celorlalți paşi ai algoritmului.

Reprezentare grafică a paşilor









Decriptarea se face în mod similar cu criptarea, ambele fiind prezentate în schema de mai jos.

Schema generală a algoritmului