**Ministerul Educației, Culturii și Cercetării**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică și Microelectronică**

**Departamentul Ingineria Software și Automatică**

**Raport**

Lucrarea de laborator nr.1

Disciplina: Securitatea Informațională.

Tema: Algoritmul DES/AES.

**Efectuat**: st.gr. TI-202 Gorgos Ioan.

**Verificat**: asist. univ. Todus Alexandru.

Chișinău 2023

**Scopul lucrării:**

Elaborarea unui algorit de criptare și decriptare.

**Mersul lucrării:**

1. Studierea algoritmului de criptare DES şi AES
2. Analiza comparativă a acestora
3. Realizarea unei aplicaţi de criptare ce va utiliza algoritmul DES sau AES
4. **DES (Data Encryption Standard):**

Algoritmul Data Encryption Standard (DES) a fost dezvoltat de IBM în anii 1970 și a devenit ulterior un standard federal de criptare în Statele Unite ale Americii. A fost larg utilizat în industrie și în sectorul guvernamental pentru a asigura securitatea datelor.

DES funcționează cu o cheie secretă de 56 de biți pentru criptarea și decriptarea datelor. Datele de intrare sunt împărțite în blocuri de 64 de biți și sunt supuse unei serii de permutări și operații logice pentru a genera textul cifrat.

O problemă semnificativă a apărut odată cu avansul puterii de calcul, ceea ce a făcut posibilă spargerea cheilor DES prin forță brută într-un timp rezonabil. Din această cauză, DES a fost gradual înlocuit cu algoritmi mai puternici, cum ar fi Advanced Encryption Standard (AES).

1. **AES (Advanced Encryption Standard):**

AES a fost ales ca înlocuitor pentru DES în anul 2001, printr-un proces de selecție publică.

A fost dezvoltat de doi criptografi belgieni, Vincent Rijmen și Joan Daemen.

AES este un algoritm de bloc simetric care poate utiliza chei de 128, 192 sau 256 de biți. Datele de intrare sunt împărțite în blocuri de 128 de biți și sunt supuse unor runde de substituție, permutare și operații logice în funcție de cheia specificată.

AES este considerat un algoritm de criptare extrem de securizat și rezistent la atacuri de forță brută, atât timp cât cheia este selectată și gestionată corect. Acest algoritm este folosit pe scară largă în întreaga lume pentru a asigura securitatea datelor sensibile, precum informațiile bancare și cele legate de securitatea națională.

1. **Analiza comparativă a acestora**

Des (Data Encryption Standard) și AES (Advanced Encryption Standard) sunt două algoritmi de criptare folosiți pentru securizarea datelor. Voi face o analiză comparativă a acestora din punct de vedere funcțional:

**Complexitate și securitate:**

DES: DES a fost dezvoltat în anii '70 și, de-a lungul timpului, s-au descoperit vulnerabilități semnificative în algoritmul său. Lungimea cheii de 56 de biți este considerată prea scurtă în ziua de azi, iar atacurile de forță brută pot sparge cheile DES într-un timp relativ scurt. Prin urmare, DES nu este considerat sigur în prezent.

AES: AES a fost adoptat ca standard în 2001 și oferă o securitate mult mai mare decât DES. AES are opțiuni pentru lungimi de chei de 128, 192 și 256 de biți, ceea ce îl face mult mai rezistent la atacurile de forță brută. Cu o cheie suficient de lungă, AES este considerat foarte sigur și este folosit pe scară largă în întreaga lume.

**Performanță:**

DES: DES este mai rapid decât AES, datorită faptului că folosește chei mai scurte și operațiuni mai simple. Cu toate acestea, acest lucru se datorează și faptului că DES este mai puțin securizat.

AES: AES are nevoie de mai mult timp pentru a cripta și decripta datele, mai ales cu chei mai lungi. Cu toate acestea, având în vedere puterea de calcul a hardware-ului modern, diferența de performanță între DES și AES nu este adesea semnificativă în practică.

**Implementare și utilizare:**

DES: Implementarea DES este mai simplă și mai ușor de înțeles, ceea ce a dus la utilizarea sa în sisteme mai vechi sau în aplicații care nu necesită un nivel înalt de securitate.

AES: AES este folosit în mod obișnuit în aplicații care necesită securitate sporită, cum ar fi criptarea datelor personale, a datelor bancare și a comunicațiilor online. Implementarea corectă a AES necesită cunoștințe avansate de criptografie.

**Standardizare:**

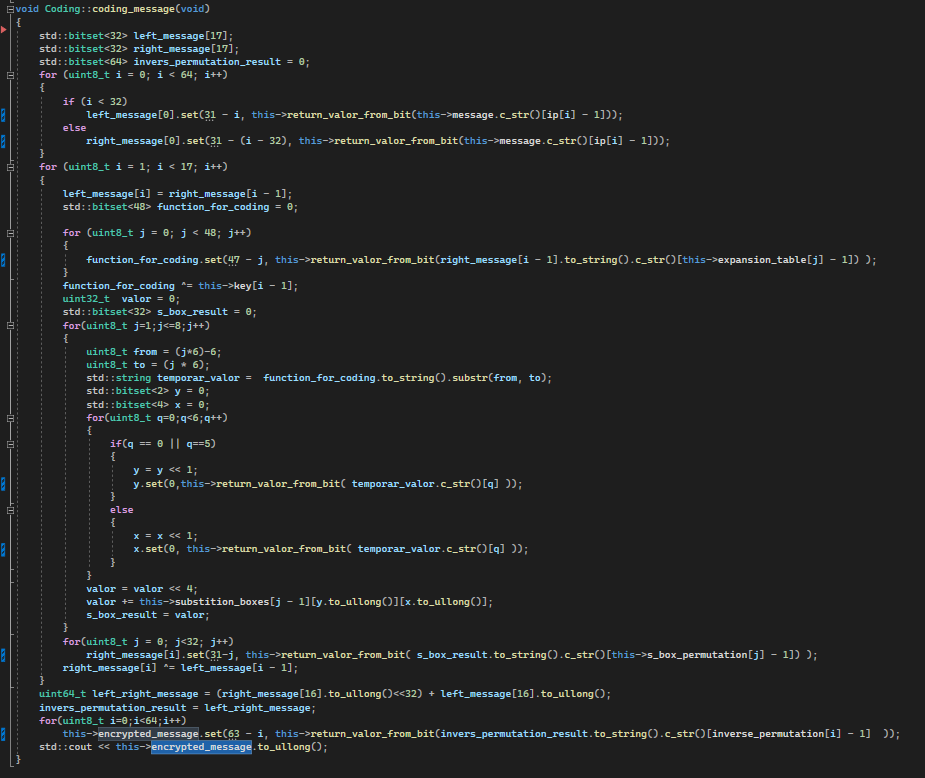
DES: DES a fost standardizat la nivel federal în Statele Unite, dar a fost ulterior înlocuit de AES ca standard federal.

AES: AES este standardul de criptare recomandat la nivel mondial și este utilizat pe scară largă în industrie.

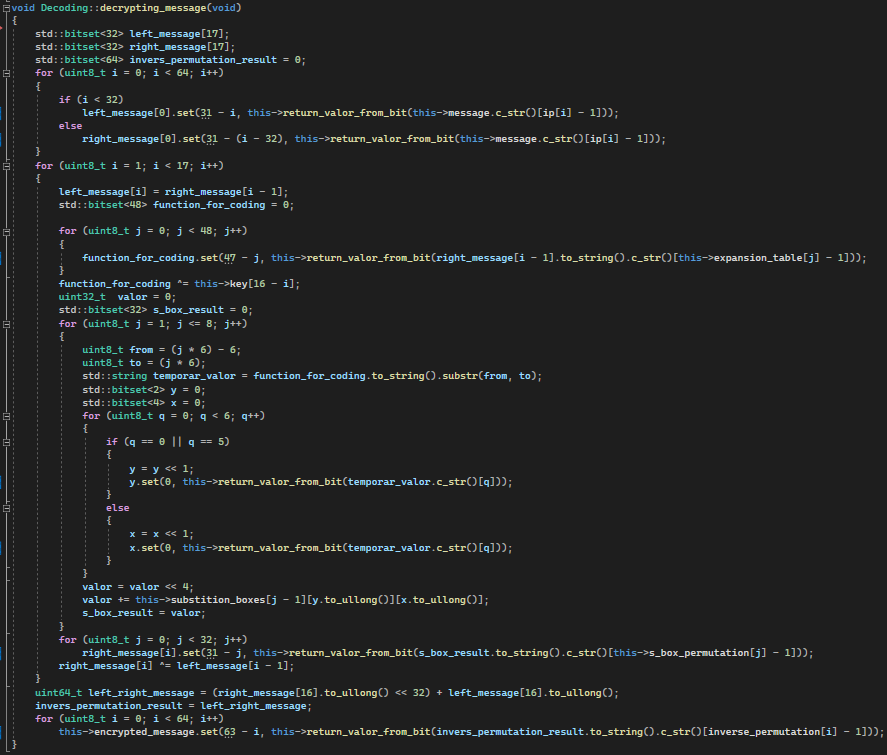
În concluzie, AES este preferat în mod clar în comparație cu DES în ceea ce privește funcționalitatea și securitatea. DES este considerat depășit și nesigur în ziua de azi, în timp ce AES oferă un nivel înalt de securitate și este folosit pe scară largă în întreaga lume pentru a proteja datele sensibile.

1. **Realizarea unei aplicaţi de criptare ce va utiliza algoritmul DES , ulilizînd diferite biblitoeci, cum ar bitset, sstream**

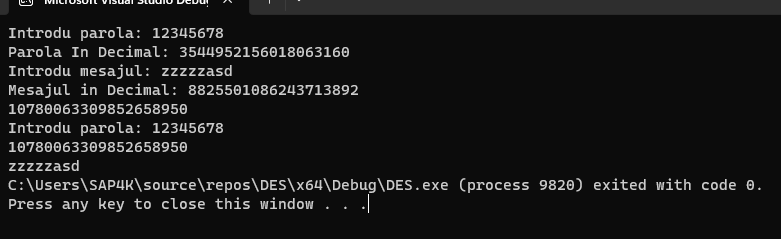
**Codul Sursă:**



Figură 1. Functia de criptare



Figură 2. Functia de decriptare



Figură 3. Răspunsul în urma criptării și decriptării mesajului nostru

**Concluzie:**

În urma realizării lucrării date a fost cercetat, dar și implementat algoritmul Data Encryption Standard (DES), care pentru criptare folosește o cheie de 8 caractere și deja mesajul insuși care urmează a fi codificat. Acest algorim a fosto dezvoltat și folosit în anii 70 al secoului XX de către Statele Unite ale Americii ca standart pentru securitatea informațională, însă cu dezvoltarea intensivă a tehnologiilor acest algoritm a fost înlocuit cu Advanced Encryption Standard (AES). Avantajul DES este căci acesta are o viteză mai mare de criptare, dar în schimb este mai puțin securizat.

Algoritmul AES a fost dezvoltat în 2001 și oferă o securitate mult mai înaltă, cu opțiuni pentru chei de 128, 192 și 256 de biți. Chiar dacă AES poate necesita mai mult timp pentru criptare și decriptare în comparație cu DES, acest lucru este compensat de securitatea sa sporită. AES este acum standardul de criptare recomandat la nivel mondial și este folosit pe scară largă în industrie și în aplicații care necesită protejarea datelor sensibile. Astfel, în contextul securității și al performanței, AES este preferat în mod evident în comparație cu DES în lumea digitală actuală.