



How to implement the DES algorithm in C++

des (/edpresso)

algorithms (/edpresso)

c++ (/edpresso)

Data Encryption Standard (DES) (https://www.educative.io/shoteditor/6142741706702848/preview) is a block cipher algorithm that takes plain text in blocks of 64 bits and converts them to the ciphertext using 16 48-bit keys.

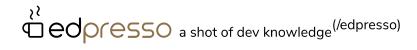
Implementation

1. Generating keys

The algorithm involves 16 rounds of encryption, with each round using a different key. Therefore, 16 keys are generated.

1 // Including dependancies 2 #include <iostream> 3 #include <string> using namespace std; // Array to hold the 16 keys string round_keys[16]; 7 // Function to do a circular left shift by 1 string shift_left_once(string key_chunk){ 8 9 string shifted=""; 10 for(int i = 1; i < 28; i++){ shifted += key_chunk[i]; 11 12 } 13 shifted += key_chunk[0]; 14 return shifted; 15 } // Function to do a circular left shift by 2 16 17 string shift_left_twice(string key_chunk){ string shifted=""; 18 19 for(int i = 0; i < 2; i++){ 20 for(int j = 1; j < 28; j++){ shifted += key_chunk[j]; 21

1 of 2 2/11/2020, 10:15





2 of 2