## Project name: AES128 decoding routine

The task in this project is to develop an AES128 decoding routine that needs to be added to an existing C++ STM32 project developed in Keil MDK-ARM. The freelancer gets a copy of this STM32 project to be used as the starting point.

**Step 1:**
Include the “ST Cryptographic library” in the project.
This library offers various AES128 routines.
https://www.st.com/en/embedded-software/x-cube-cryptolib.html

**Step 2:**
Based on “ST Cryptographic library” develop a function that has below inputs and outputs:

**Inputs to the routine**
unsigned char input_data[];
unsigned char AES128_key[16] = {0x33,0x44,0x55,0x66,0x77,0x88,0x99,0x00,
0x33,0x44,0x55,0x66,0x77,0x88,0x99,0x00}

**Outputs from the routine**
unsigned char output_data[];

input_data is an array of bytes representing AES128 encrypted data.

The function to be developed shall decrypt the input_data by using the AES128_key and deliver the result in output_data.