Criptografia - AES e modos de operação

Prof. Avelino Zorzo – Escola Politécnica/PUCRS

Neste trabalho você tem que implementar um sistema para cifrar/decifrar usando a cifra de blocos AES, com os modos de operação CBC e CTR. Em todos os casos o IV de 16 bytes é escolhido de maneira aleatória e anexada na frente do texto cifrado. Para o modo de operação CBC, usar PKCS5.

Implementar a cifragem e decifragem. Abaixo são dados as chaves para o AES, e o texto cifrado ou texto claro. Sua tarefa é recuperar o texto claro para aqueles que estão cifrados e cifrar o texto claro. Todos os textos estão em hexadecimal. Para a implementação pode-se utilizer qualquer linguagem que forneça uma biblioteca para o AES, por exemplo, PyCrypto (Python), Crypto++ (C++), Java.

Submeter sua implementação e um artigo com até duas páginas com sua solução e as respostas.

Desafio valendo um ponto extra: Implementar os modos de operação você mesmo.

Tarefa 1

- CBC key: 140b41b22a29beb4061bda66b6747e14
- CBC Ciphertext:
  4ca00ff4c898d61e1edbf1800618fb2828a226d160dad07883d04e008a7897ee\
  2e4b7465d5290d0c0e6c6822236e1daafb94ffe0c5da05d9476be028ad7c1d81

Tarefa 2

- CBC key: 140b41b22a29beb4061bda66b6747e14
- CBC Ciphertext:
  5b68629feb8606f9a6667670b75b38a5b4832d0f26e1ab7da33249de7d4afc48\
  e713ac646ace36e872ad5fb8a512428a6e21364b0c374df45503473c5242a253

Tarefa 3

- CTR key: 36f18357be4dbd77f050515c73fcf9f2
- CTR Ciphertext:
  69dda8455c7dd4254bf353b773304eec0ec7702330098ce7f7520d1cbbb20fc3\
  88d1b0adb5054dbd7370849dbf0b88d393f252e764f1f5f7ad97ef79d59ce29f5f51eeca32eabedd9afa9329

Tarefa 4

- CTR key: 36f18357be4dbd77f050515c73fcf9f2
- CTR Ciphertext:
  770b80259ec33beb2561358a9f2dc617e46218c0a53cbeca695ae45faa8952aa\
  0e311bde9d4e01726d3184c34451

Tarefa 5

- CTR key: 36f18357be4dbd77f050515c73fcf9f2
- CTR Plaintext:
  5468697320697320612073656e74656e636520746f20626520656e6372797074656420757369e67204145532061
  6e6420435452206d6f64652e

Tarefa 6

- CBC key: 140b41b22a29beb4061bda66b6747e14
- CBC Plaintext:
  4e6578742054687572736461792 06f6e65206f662074686520626573742074656 16d7320696e2074686520776f726c64
  2077696c6c206661636520612062696720636 8616c6c656e676520696e20746865204c6962657274616 46f726573206
  46120416d6572696361204368616d70696f6e736869702e