



Two options

- 1- Write 1-2 pages (English or German) about a smart-grid related problem from your field of interest. Describe the problem with some details and motivation, then write something about the possible solution.

- 2- Write a C/C++ program that takes as input a 24 bit Initialization Vector (IV) and the encrypted data from an ARP or IP packet from the files ex8.cap. Perform brute force method to find the WEP password. The following steps help you in the implementation.
 - 1- Using wireshark, open the file (test_ex8.cap) with the known password **f56HA** to understand the structure of ARP packets or other types of data packets
 - 2- Complete the implementation in ex8_crack.cpp
 - 3- Get the IV from an ARP packet (data packet)
 - 4- Get the encrypted data from the Packet as hex
 - 5- Assume the password consists from small/capital letters in addition to numbers
 - 6- Concatenate a 40 bits (5 chars) key to have the complete Key.
 - 7- Key schedule step, obtain the vector S based on the key
 - 8- Using the encrypted data and S, decode the encrypted message and compare the results in byte 0, 1, 2,3,and 4, with 0xaa, 0xaa, 0x00, 0x00, 0x00.
 - 9- Decode the encrypted message and compare the results in byte 0, 1, 2, 3, and 4, with 0xaa, 0xaa, 0x00, 0x00, and 0x00.
 - 10- If the results are true, then the password is cracked
 - 11- Check if the password can decrypt the ex8.cap file in wireshark
 - 12- Send the implementation and the password of ex8.cap