CS-364: Introduction to Cryptography and Network Security LAB

LAB Assignment IV

Course Instructor: Dr. Dibyendu Roy Due: April 26, 2022, 11:59 pm

Instructions: Code must be written in C and well commented. Submission of code in any other file extension (.pdf, .docx etc) will not be considered. The file name of the code will be YOUR ROLL NO.c. Write Your Name and Roll Number on the top of your code. I expect all students to behave according to the highest ethical standards. Any cheating or dishonesty of any nature will result in deduction of marks.

Your submission will not be considered if you submit late.

You need to implement the following protocol in C programming language.

1. Consider the prime number $p = 173$ and the Elliptic curve EL: $y^2 = x^3 + 23x + 11$ over $\mathbb{Z}_p$.
2. Select a point $\alpha (\neq$ point at infinity) on the curve EL. This α needs to be obtained inside your code. Print α. (Output)
3. Alice and Bob have agreed on the same curve EL and the point α.
4. You code will ask for Alice's private key $n_A \in [1, 150]$ and Bob's private key $n_B \in [1, 150]$. (Input)
5. Using n_A and n_B Alice and Bob perform Diffie-Hellman key exchange on the curve EL with the point α and establish a shared secret key $SK = (x_1, y_1) \in$ EL. Print the SK. (Output)
6. Alice uses SHA-256 hash function and computes a key $K_A = \text{SHA-256}(x_1||y_1)$.
7. Bob uses SHA-256 hash function and computes a key $K_B = \text{SHA-256}(x_1||y_1)$.
8. Print K_A and K_B in the form of 32 bytes (space separated). (Output)
9. Program will ask for Alice's 256-bit message (say M_A). Input will be 32 space separated bytes in hexadecimal. For example : $M_A =$ `00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff`. (Input)
10. Alice will encrypt the given message M_A using AES-256 bit encryption algorithm in CBC mode of operation using her key K_A. In CBC mode Alice will consider $IV = 0$. Let the generated ciphertext be C_A. i.e., $C_A = \text{Enc}^{\text{CBC}}_{\text{AES-256}}(M_A, K_A, IV)$.
11. Alice will generate a MAC for M_A using the described algorithm. The description of MAC is $\text{MAC}_A = \text{SHA-256}\Big((K_A \oplus 1)||\text{SHA-256}\big((K_A \oplus 2)||M_A\big)\Big)$. Here $1, 2$ are 256-bit integers.
12. Your program will display the ciphertext C_A and MAC_A in the form of bytes (space separated). (Output).
13. Alice will pass the ciphertext C_A, MAC_A and $IV (= 0)$ to Bob. This will be passed inside your code.
14. Bob will decrypt C_A using AES-256 bit decryption algorithm in CBC mode with his key K_B and $IV = 0$. Let the decrypted text be M_B. i.e., $M_B = \text{Dec}^{\text{CBC}}_{\text{AES-256}}(C_A, K_B, IV)$.
15. Bob will generate $\text{MAC}_B = \text{SHA-256}\Big((K_B \oplus 1)||\text{SHA-256}\big((K_B \oplus 2)||M_B\big)\Big)$. Here $1, 2$ are 256-bit integers.
16. Your program will display M_B and MAC_B in the form of bytes (space separated). (Output)

If your code is correct ! then $K_A = K_B$, $M_A = M_B$ and $\text{MAC}_A = \text{MAC}_B$ for every possible inputs.

All the best ☺