CS-364: Introduction to Cryptography and Network Security LAB

LAB Assignment III

Course Instructor: Dr. Dibyendu Roy Due: Apr 10, 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.

1. Implement the compression function $h : \{0,1\}^{256} \to \{0,1\}^{128}$ by using the following rule

$$h(m_1||m_2) = \text{AES-128}(m_1, m_2).$$

   Here AES-128 encryption algorithm takes an 128-bit key and an 128-bit message block and generates 128-bit ciphertext block (AES-128(M,K)=C) i.e., AES-128: $\{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$.

2. Your code will take input $m_1, m_2 \in \{0,1\}^{128}$ and print $h(m_1||m_2)$.

3. Implement a second pre-image $(m_1'||m_2') \in \{0,1\}^{256}$ finding process for h corresponding to any random input $(m_1||m_2) \in \{0,1\}^{256}$.

4. Print the obtained second pre-image $(m_1'||m_2')$ and the compressed values $h(m_1'||m_2')$, $h(m_1||m_2)$.