CS-3610: Information Security (Spring 2025)

Assignment Type: Individual

Assignment - 2 **Marks: 70**
Assign Date: Feb 20, 2025 *Submit Date: 23:55, Mar 2, 2025*

1

Write an expository note on the material discussed during Lecture 4 (February 11). We want you to develop and demonstrate your intuition for what motivated the technical definitions and theorems discussed in class.

2

Test your understanding by solving these exercises.

a. What is the size of the term below? What are its subterms?

$$\mathsf{aenc}(\mathsf{pair}(\mathsf{aenc}(m, \mathsf{pk}(k_1)), \mathsf{pair}(n_1, n_2)), \mathsf{pk}(k_2))$$

b. Given the following X, can X derive $\mathsf{aenc}(m, \mathsf{pk}(k_3))$ using a normal proof?

$$\begin{aligned} X = \{ & \\ & \mathsf{aenc}(m, \mathsf{pk}(k_1)), \\ & \mathsf{pair}(k_2, \mathsf{aenc}(\mathsf{pair}(m, k_1), \mathsf{pk}(k_3))), \\ & \mathsf{aenc}(k_3, \mathsf{pk}(k_2)), \\ \} & \end{aligned}$$

3

Write code to formally verify or refute the security of the protocol you implemented in Task 6 of Assignment 1 using the Dolev-Yao model. Make expedient design choices for how to represent terms, derivations, and so on.