

Name: Nguyễn Việt Hoàng

Student's ID: B22DCVT214

CLASS PREP 1

Directions. After reading Sections 2.1 and 2.2 please answer the following questions (either directly on the template or on separate paper).

This class prep assignment will be **graded on effort**. Please do not leave any questions blank – if you are stuck, either formulate a question that you believe will help you get unstuck or write down some preliminary ideas.

1. What is a plaintext? Give an example

Plaintext is the original message or data that is fed into the algorithm as input

Example for plaintext: "This is a secret message"

2. What is the name of the process of **attempting to discover the plaintext or key**?

The name of the process of attempting to discover the plaintext or key is cryptanalysis

3. Check Table 2.1, what type of attack is the most difficult?

Ciphertext only is the most difficult type of attack

4. What does it mean by “Brute force” approach?

Brute-force approach is trying every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained