Faculty of Computer Science and Engineering

Ho Chi Minh City University of Technology



Nguyen Phuong Vuong - 1614186

# 

Cryptography and Network Security

Lab 2

# Exercise 1.

A transformation is singular if it is not invertible or undoable. This means if you apply that, you will lose information. A nonsingular transform means you can undo the transform.

# Exercise 2.

A block cipher is one in which a block of plain-text is treated as a whole and used to produce cipher-text block of equal length.

A stream cipher is one that encrypts a digital data stream one bit or one byte at a time.

# Exercise 4.