

CSE 498U/598U – Computer Security

Class 4: Wednesday, September 1

Reminders

- Homework
 - Background Survey, Homework 1 – Computer Ethics **Due Today**
 - Homework 2 - Password Cracking
 - Reading / Web Browsing
 - Google : Breaking simple ciphers
 - Topic Ideas – Final Project
-

Schedule

Wednesday, September 1
Basic Cipherring / Breaking

Friday, September 3
Encryption Principles, Block/Stream, DES / AES

Monday, September 8
DES, RSA / PKI

Lecture Outline

Final Project Ideas

Substitution Cipher

- Caesar Cipher
- Keyed Substitution Cipher
- Complexity

Breaking Ciphertext

- Frequency / quantity

One-Time Pad

- Vernam Cipher

Transposition Cipher

Key Points

- What is the difference between a substitution and a transposition cipher?
- Why is regularity/predictability bad for an encryption system?
- What is a Vernam cipher?
- What is a one-time pad?