IS53012B/A Computer Security

Dr Ida Pu

Room 10, 29 St James
Goldsmiths, University of London

2018-19 (since 2007)

Part I

Workshop

Outline

1. Week 3 Homework

1. Week 3 Homework

Week 3 Homework

1. Following John's Cryptosystem (Week 2 Homework), demonstrate
   1. how the plaintext $m = 1011$ can be delivered from Alice to Bob without sharing a private key.
   2. how Charlie can get the plaintext $m = 1011$ by monitoring the communication traffic.
2. Let the password seed be 1101 which is known by both Alice and Bob.
   1. Demonstrate how Alice and Bob can independently generate an identical new random password of up to 15 bits without sending the new password.
   2. What are the risks?
3. Alice has 108 Bob-friends and applies private-key encryption techniques. How many keys would Alice need to privately communicate with her Bob-friends? How many keys would be necessary for the communication system?
4. Continue to work on the coursework.