WELCOME

Computer and Information Security Fundamentals

(CSE 2203)

SEMESTER II (2018-2019)

Sandra Khan BSc MSc CISSP PG Dip Education (Higher Ed)

sandra.khan@uog.edu.gy

Computer and Information Security Fundamentals

(CSE 2203)

Semester II 2017/2018

Sandra Khan

BSc (Computer Science)

MSc (Information Security)

Pg Diploma Education (Higher Education)

CISSP

Certified Information Systems Security Professional

CISSP®

ROYAL HOLLOWAY UNIVERSITY OF LONDON

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

Before we begin..

- Please switch cell phones to silent

- Admin Issues

- Will be using Moodle to manage course
- Office Hours: (E29) Wednesdays 13:00 – 15:00 hrs

- *Email:sandra.khan @uog.edu.gy*

Course Information

This course is a second year second semester course intended for students pursuing the two year full time Associate of Science OR Bachelors of Science Degrees in Information Technology/Information Systems/Computer Science.

This course will introduce students to the fundamental elements of computer security.

As with all Department of Computer Science courses, the course will develop students' analytical skills and their ability to conduct academic research and evaluation.

Core Course

Exemption(s):   There are no exemptions for this course.

Pre-requisites: None

Follow-On Courses: CSE 3100 – Information Assurance and Security

Teaching / Assessment

Method of Teaching:

Lectures	2 x 13=	26 hrs.
Laboratories/ Tutorials	2 x 13=	26 hrs.

Method of Assessment:

Coursework (40%)
Tests (20%)
Assignments (20%)
Final Examination (60%)

Tutorials

- Tutor – Mr. Teekae Jordan

- Email: Teekae.Jordan@uog.edu.gy

- Tutorial Times:

  - **Wednesdays 12:15 – 14:10 hrs (CS Lab)**
  - **Thursdays 15:15 – 17:10 (E37)**
  - **Fridays 08:15 – 10:10 (CS Lab)**

Introductions

- Tutor – Mr. Teekae Jordan

- President, University of Guyana Cyber Security Club (UGCC) – Mr. Cloyd London

- Your Turn

Learning Outcomes

By the end of this course students will be able to:

- Identify and describe computer security risks and attacks
- Explain Cryptography and Cryptographic mechanisms such as Encryption and Authentication mechanisms
- Identify networks security issues and describe and implement security mechanisms to protect computer networks
- Identify elements of application security and describe mechanisms used to create secure applications
- Describe cybersecurity and identify means to mitigate against cyberattacks
- Develop and communicate security policies

Course Outline

Week 1 – Security Basics

Week 2 – Introduction to Cryptography

Week 3 - Authentication, Encryption (DES/RSA), Hashing

Week 4 - Integrity – Digital Certificates, Message Digests

Week 5 – Network and Internet Security

Week 6 - Internet Commerce, SSL, IPSec, Firewalls

Week 7 – VPN / IDS

Week 8 & 9 – Wireless Security

Week 10 – System Security

Week 11 – Access Control

Week 12 – Application Security

Week 13 – Cyber Crime

Readings

Required Reading(s)

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in computing*. Prentice Hall Professional Technical Reference.

Stallings, W. (2006). *Cryptography and Network Security, 4/E.* Pearson Education India.

Recommended Reading(s)

Stallings, W. (2007). *Network security essentials: applications and standards*. Pearson Education India.

The University of Guyana
Faculty of Natural Sciences

Course outline, course notes and references are available via Moodle.

End of Welcome and Introduction