G53SEC Coursework
First Semester, 2012

General Description

- The three coursework accounts for **40% (20%+20%-20%)** of the final assessment.
- Deadline for submitting the 1st coursework is **13:00PM, 22nd, March, 2012**. Deadline for the 2nd coursework is **13:00PM, 29th, March, 2012**.
- Coursework 1 is about Cryptography, in particular, Asymmetric crypto technology. You are required to investigate one technique and method that select from 9 current and famous methods.
- Coursework 2 is concerned with programming and you must develop the method which selected in coursework 1.
- Coursework 3 is based on a mini conference on computer security. Each group must select a topic after two first sessions and write a paper maximum 6 pages on that topic and present in the mini conference. Date of mini conference is **14:00 Pm, 25th April, 2012**. (Join to the mini conference is free for all students from other departments and faculty)
- Coursework 3 needs to be completed individually while coursework 1 and 2 need to be done in group. Grouping information will be finished after first session and will attach in the appendices.

Coursework One and Two (Description and Requirements)

- Coursework 1 is related to the asymmetric cryptography technology. You can select one of the famous methods in this area and explain about technique. Finding the algorithm of technique and plat it is one of the major parts of this coursework.
- The objective of this coursework is to be familiar with asymmetric techniques as the normal and common cryptography techniques and also elaborate the major issues in these methods. Also, this course work can show that what you have learned in this course (Cryptography sessions).
- You should provide a maximum 6-page report in Doc format (diagrams, Figures, Tables, etc.) documenting in detail your selected method or technique. The report should demonstrate your knowledge, argumentation, creativity, and others listed in the marking scheme (see appendices).
- Coursework 2 is implementing the coursework 1 method by any programming language (You can select Java as a more useful language for security programming). A completed source code in a single zipped file developed in your work must submit.
- In Coursework 2 as a result of your program and validity please show your technique cipher text after run the program for these plaintext: **“ “, “The quick brown fox jumps over the lazy dog” and “The quick brown fox jumps over the lazy cog”.**

Coursework three (Mini Conference)

- Coursework 3 is related to the current technology in computer science. Each group can select a topic and write a maximum 6 pages article and present in the mini conference.
- The primary objective of the coursework 3 is to investigate recent research in the area of computer security. You are required to produce a survey paper with maximum 6 pages and to give a presentation (approximately 15 minutes + 5 minutes question answering) in the mini conference sessions.
- Your survey should address few important questions such as:
  1) what is the current state-of-the art in your topic
  2) Currently what are main problems or issues in that topic
  3) how might these problems be solved
  4) What general solutions do you propose for these problems that you identified
- This is a group coursework and the grouping information can be found in the appendices of this document after first session. Each group only needs to submit one report and one presentation document (.doc and .pdf for report and .ppt for presentation).
- As a suggestion, divide your work fairly among group members. If your group consists of 3 members and you select 15 research articles, you can allocate 5 papers for each one. While the survey can be divided into different sections which you write separately, you need to integrate your findings later (through group discussions) and produce a coherent report with consistent writing and layout. Please attention to research methodology sessions in LAB sessions.
- Your article must have the common structure of papers such as: Abstract, Introduction, Related works, Problems and issues, methodologies, Finding, Conclusion and references. All references must be citing in the body of article.
- For “marking method” and “Topics” of the mini conference, please find the appendixes “Call for paper” and “Review Form”.
- Each article will review by three technical committee member of mini conference and the average of these marks will be final mark for group members.

Appendixes

Coursework evaluation form

AREA	MAXIMUM POINTS %	FINAL AWARD OF MARKS %
INTRODUCTION & ADDRESSING THE PROBLEM	5	
RELEVANCE OF RESEARCH (sources of reference /bibliography)	10	
ACCURACY OF CONTENTS (relevance of answers)	15	
FINDINGS (quality & supporting details from research)	15	
APPLICATION (demonstration of practical examples)	10	
CONCLUSION AND RECOMMENDATIONS (quality of conclusion and recommendation)	10	
SPELLING AND GRAMMAR (correct usage of the language)	5	
STRUCTURE & PRESENTATION (professional style with logical flow and clarity of presentation)	5	
ORIGINAL PIECE OF WORK (evidence of not being CPT – Copy and Paste Technique)	20	
ADHERENCE TO WORD COUNT (10% more or less is permitted)	5	
TOTAL POINTS - WRITTEN PROJECT	**100%**	
TOTAL POINTS - INDIVIDUAL PRESENTATION (in the below table)	**100%**	

PLAGIARISM WILL RESULT IN AN AUTOMATIC FAILURE

PRESENTATION MARKS CRITERIA

Area	Knowledge of Topic/s presented	Presentation Quality	Quality of communication & English Language	Grooming & Dress Sense	Total Points	Award
Maximum Points %	60%	10%	20%	10%	**100%**	**10%**

Mini Conference Call for Papers

Computer Security

Important Dates

Title and Abstract submission date: 23th Feb, 2012
Paper final version submission date: 19th April, 2012
Review result date: 26th April, 2012
Conference: 26th April, 2012

Overview

The mini-Conference provides an opportunity for the student to experience writing and peer reviewing a scientific paper. All papers must be written by a team of two students, and presented by one of the two team members. Presentation is during 15 minutes and after that 5 minutes will be arrange for questions. Attending to the conference is free for all other students from another departments or universities.

Call for Papers

The program committee seeks papers describing the design, application, and validation of security technologies. Submissions across a broad range of development phases are encouraged, from exploratory research and proof-of-concept studies to practical application, deployment of the technology, and interesting overview papers.

Topics

1. **Cryptography**
2. **Security Protocols**
3. **Physical security**
4. **Software Security**
5. **Network Security**
6. **Cybernetic Security**
7. **Attacks and Anti Attacks**

Refereed Papers

Papers that have been formally reviewed and accepted by technical committee members will be presented during the mini conference.

Best Paper Awards

a prize will be given at the conference for the best paper.

How to Submit Papers

Papers should represent novel scientific contributions related to at least one of the topics listed above. Both the work described in the paper and the paper itself must be complete at the time of the submission. Papers should be at most 6 (six) A4 size pages using an 11 pt font. Papers should be submitted on .doc and .pdf formats.

Reviewing, Selection and Presentation

On the day of the hand in, each paper will be assigned to three technical committee members for peer review. All submissions will be judged on originality, contribution to the field, clarity, and correctness. The technical committee members will fill in a review form for each paper.

Mini Conference Review Form

Please give five ratings in the range **0…5** and at least one paragraph of comments for the paper.

Paper title: …

Importance: …
Low scores might be given for marketing literature and papers on inappropriate or dead topics. High scores are for papers that nearly the entire audience will want to read and understand carefully. Range (**0=unimportant, 1=hardly important, 2=some but still insufficient importance, 3=some but sufficient importance, 4=quite important, 5=very important**)

Novelty: …
Is the work novel? Low scores should be given for papers that re-hash known techniques in well-established areas. High scores are for papers that open new fields or demonstrate new ways to solve a problem. Range (**0=old hat, 1=hardly novel, 2=some but still insufficient novelty, 3=some but sufficient novelty, 4=considerable novelty, 5=entirely new**)

Quality: …
A low score might go to a paper whose main theorem is incorrect or whose proposed approach to attacking a problem is not viable in your opinion. High scores are for papers with enough justification to convince you that the work is correct and viable. Range (**0=rubbish, 1=hardly worth reading, 2=some but still insufficient merit, 3=some but sufficient merit, 4=considerable merit, 5=top quality**)

Overall: …
Should we accept this paper or should we reject it? This is by far the most important number. It need not be an average of the other numbers, but it should reflect them. This number can also reflect issues in addition to those described above (e.g. poor presentation or lack of knowledge of related work). Range (**0=reject, 1=likely reject, 2=just below borderline, 3=just above borderline, 4=likely accept, 5=definite accept**)

Self-rating: …
Please rate yourself on each paper in terms of your qualifications to judge the paper. Range (**0=I know nothing or almost nothing about this area, 1=I know a little about this area, 2=I know something about this area but my knowledge is still insufficient, 3=I have sufficient knowledge of this area, 4=I know a lot about this area, 5=I am an expert in this area**)

In addition to these ratings, you must provide a justification for your marks as well as some helpful comments to the authors.

Justification of marks and comments to authors (continue overleaf) …

Group members

No.	Surname	Forename	ID No.	Group
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				