Philadelphia University  
Faculty of Engineering  
Department of Communications & Electronics

Course Syllabus

Course Title: Special Topics (GSM Security Principles)  
Course code: (650594)

Course Level: 5th year  
Course prerequisite(s) and/or corequisite(s):

Lecture Time:  
Credit hours: 3  
Tutorial: 1 hour/Week

Academic Staff Specifics

<table>
<thead>
<tr>
<th>Academic Staff Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
</tbody>
</table>

Course module description:
The GSM standard was designed to be a secure mobile phone system with strong subscriber authentication and over-the-air transmission encryption. The security model and algorithms were developed in secrecy and were never published. Eventually some of the algorithms and specifications have leaked out. The algorithms have been studied since and critical errors have been found. Thus, after a closer look at the GSM standard, one can see that the security model is not all that good. An attacker can go through the security model or even around it, and attack other parts of a GSM network, instead of the actual phone call. Although the GSM standard was supposed to prevent phone cloning and over-the-air eavesdropping, both of these are possible with little additional work compared to the analog mobile phone systems and can be implemented through various attacks. One should not send anything confidential over a GSM network without additional encryption if the data is supposed to stay confidential.

Course module objectives:
On Completing of this course, the student will be able to understand:
1- GSM System.  
2- SIM Card and GSM Security Model.  
3- A8 Algorithm.  
4- A3 Algorithm.  
5- A5 Algorithm.
Course/ module components:

- Books (title, author(s), publisher, year of publication)
  - Anderson Ross, “The GSM Encryption Algorithms”
- Support material(s) (vcs, acs, etc).
- Study guide(s) (if applicable)
- Homework and laboratory guide(s) if (applicable).

Teaching methods:
Lectures & assignments.

Learning Outcomes:

A) Knowledge and understanding Skills:
Students will obtain knowledge and understanding of:
1) Mathematical tools relevant to communications and electronics systems.
2) Fundamental technological concepts, principles, and techniques associated with electronics and communications systems.
3) The structure of different communication systems.
4) The way of thinking and how to design.
5) The methods of developing the communication systems.
6) Design and simulate different communication system, and the electronic subsystems.
7) How to build, as hardware, different communication systems.

B) Intellectual Skills:
The students will acquire and develop the thinking skills that should enable them to:
1) Develop a strong grounding in the fundamentals and how to apply them.
2) Develop an ability to analyze communication and electronic engineering problems and synthesize solutions.
3) Apply appropriate techniques to the transmission systems that are currently used for data, voice and video over LAN and WAN broadband networks.
4) Understanding, designing and developing different communication and electronic systems for processing signals and data.
5) Analyze and identify the specifications and tools to design typical process control applications, applicable to data communications and its related electronics systems.

C) Practical Skills:
Students will acquire and develop the practical skills that should allow them to:
1) Use appropriate numerical and mathematical skills to describe, analyze and solve a problem in electronics or/and communication system.
2) Use various laboratory equipment as diagnostic tool to detect a faults and identify a problem in electronics or/and communication system.
3) Analyze, design, evaluate, system behavior and test electronic or/and communication system using simulation or computer-based tool (engineering software tool).
4) Implement electronic circuits for communication system.
5) Undertake ongoing learning in order to keep up to date in the field on electronics and communication technologies.
6) Deal with computer hardware and use it in electronic and communication project.

D) Practical and subject specific skills (Transferable Skills):
Students will acquire and develop the key transferable skills that will enable them to:
1) Clarify personal values and objectives. 
2) Negotiate learning contracts.
3) Use a range of technological equipment and systems.

**Assessment instruments:**

- Short reports and/or presentations, and/or Short research projects
- Quizzes.
- Home works
- Final examination: 50 marks

<table>
<thead>
<tr>
<th>Allocation of Marks</th>
<th>Mark</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment Instruments</td>
<td></td>
</tr>
<tr>
<td>First examination</td>
<td>15%</td>
</tr>
<tr>
<td>Second examination</td>
<td>15%</td>
</tr>
<tr>
<td>Final examination: 50 marks</td>
<td>50%</td>
</tr>
<tr>
<td>Reports, research projects, Quizzes, Home</td>
<td>20%</td>
</tr>
<tr>
<td>works, Projects</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

**Documentation and Academic Honesty**

Submit your home work covered with a sheet containing your name, number, course title and number, and type and number of the home work (e.g. tutorial, assignment, and project).

Any completed homework must be handed in to classroom. After the deadline “zero” will be awarded. You must keep a duplicate copy of your work because it may be needed while the original is being marked.

You should hand in with your assignments:
1- A printed listing of your test programs (if any).
2- A brief report to explain your findings.
3- Your solution of questions.

For the research report, you are required to write a report similar to a research paper. It should include:

- **Abstract**: It describes the main synopsis of your paper.
- **Introduction**: It provides background information necessary to understand the research and getting readers interested in your subject. The introduction is where you put your problem in context and is likely where the bulk of your sources will appear.
- **Methods (Algorithms and Implementation)**: Describe your methods here. Summarize the algorithms generally, highlight features relevant to your project, and refer readers to your references for further details.
- **Results and Discussion (Benchmarking and Analysis)**: This section is the most important part of your paper. It is here that you demonstrate the work you have accomplished on this project and explain its significance. The quality of your analysis will impact your final grade more than any other component on the paper. You should therefore plan to spend the bulk of your project time not just gathering data, but determining what it ultimately means and deciding how best to showcase these findings.
- **Conclusion**: The conclusion should give your reader the points to “take home” from your paper. It should state clearly what your results demonstrate about the problem you
were tackling in the paper. It should also generalize your findings, putting them into a useful context that can be built upon. All generalizations should be supported by your data, however; the discussion should prove these points, so that when the reader gets to the conclusion, the statements are logical and seem self-evident.

- **Bibliography:** Refer to any reference that you used in your assignment. Citations in the body of the paper should refer to a bibliography at the end of the paper.

- **Protection by Copyright**
  1. Coursework, laboratory exercises, reports, and essays submitted for assessment must be your own work, unless in the case of group projects a joint effort is expected and is indicated as such.
  2. Use of quotations or data from the work of others is entirely acceptable, and is often very valuable provided that the source of the quotation or data is given. Failure to provide a source or put quotation marks around material that is taken from elsewhere gives the appearance that the comments are ostensibly your own. When quoting word-for-word from the work of another person quotation marks or indenting (setting the quotation in from the margin) must be used and the source of the quoted material must be acknowledged.
  3. Sources of quotations used should be listed in full in a bibliography at the end of your piece of work.

- **Avoiding Plagiarism.**
  Unacknowledged direct copying from the work of another person, or the close paraphrasing of somebody else's work, is called plagiarism and is
  1. a serious offence, equated with cheating in examinations. This applies to copying both from other students' work and from published sources such as books, reports or journal articles.
  2. Paraphrasing, when the original statement is still identifiable and has no acknowledgement, is plagiarism. A close paraphrase of another person's work must have an acknowledgement to the source. It is not acceptable for you to put together unacknowledged passages from the same or from different sources linking these together with a few words or sentences of your own and changing a few words from the original text: this is regarded as over-dependence on other sources, which is a form of plagiarism.
  3. Direct quotations from an earlier piece of your own work, if not attributed, suggest that your work is original, when in fact it is not. The direct copying of one's own writings qualifies as plagiarism if the fact that the work has been or is to be presented elsewhere is not acknowledged.
  4. Plagiarism is a serious offence and will always result in imposition of a penalty. In deciding upon the penalty the Department will take into account factors such as the year of study, the extent and proportion of the work that has been plagiarized, and the apparent intent of the student. The penalties that can be imposed range from a minimum of a zero mark for the work (without allowing resubmission) through caution to disciplinary measures (such as suspension or expulsion).

### Course/module academic calendar

<table>
<thead>
<tr>
<th>week</th>
<th>Basic and support material to be covered</th>
<th>Homework/reports and their due dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>GSM Communications System.</td>
<td></td>
</tr>
<tr>
<td>(2)</td>
<td>SIM Card and Security Model</td>
<td>HW#1</td>
</tr>
<tr>
<td>(3)</td>
<td>Modular Arithmetic</td>
<td></td>
</tr>
<tr>
<td>(4)</td>
<td>Polynomial Arithmetic</td>
<td></td>
</tr>
<tr>
<td>(5)+(6)</td>
<td>Primitive Polynomials</td>
<td>HW#2</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>First examination</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(6)</td>
<td>Linear Feed Back Shift Register (LFSR)</td>
<td></td>
</tr>
<tr>
<td>(7)</td>
<td>A8 Algorithm</td>
<td></td>
</tr>
<tr>
<td>(8)</td>
<td>A3 Algorithm</td>
<td></td>
</tr>
<tr>
<td>(9)+(10)</td>
<td>A5 Algorithm</td>
<td>HW#3</td>
</tr>
<tr>
<td>(11)</td>
<td>Randomness Tests</td>
<td></td>
</tr>
<tr>
<td><strong>Second examination</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(12)+(13)</td>
<td>Frequency tests</td>
<td>HW#4</td>
</tr>
<tr>
<td>(14)+(15)</td>
<td>Other test</td>
<td></td>
</tr>
<tr>
<td>(16)</td>
<td><strong>Final Examination</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Expected workload:**

On average students need to spend 2 hours of study and preparation for each 50-minute lecture/tutorial.

**Attendance policy:**

Absence from lectures and/or tutorials shall not exceed 15%. Students who exceed the 15% limit without a medical or emergency excuse acceptable to and approved by the Dean of the relevant college/faculty shall not be allowed to take the final examination and shall receive a mark of zero for the course. If the excuse is approved by the Dean, the student shall be considered to have withdrawn from the course.

**Course references**

**Books:**