The Role of Mathematics in Information Security Education

Stephen D. Wolthusen[1,2]

[1] Gjøvik University College, N-2802 Gjøvik, Norway,
stephen.wolthusen@hig.no
[2] Royal Holloway, University of London, Egham TW20 0EX, United Kingdom,
stephen.wolthusen@rhul.ac.uk

Abstract. There exists a disconnect between the expectations of students of information security and the requirements imposed on their mathematical abilities and maturity at both the M.Sc. and Ph.D. levels. In this paper we discuss efforts at Gjøvik University College, Norway, to bridge this gap on one hand by providing a targeted curriculum component intended to provide the necessary mathematical tools for conducting research at the doctoral level. On the other hand we are critically examining the curricular dependencies and requirements at the M.Sc. level where two factors are becoming evident. First, not all students at this level have adequate mathematical backgrounds to be able to profit fully from the program even though they may meet all formal prerequisites. Second, there may exist areas where the depth and rigor of the mathematical foundations currently in place in the curriculum is not be strictly necessary. Both of these factors can impede access and subsequent success of graduate programs and must therefore be addressed carefully with the aim of striking a balance between these competing objectives.

1 Introduction

The appeal of information security as a subject of studies at the graduate level transcends the core areas of computer science and mathematics, particularly in case of M.Sc. studies where the objectives of students may be more oriented towards improving their insight into pragmatic questions rather than towards academic research questions [1].

As a result of this broad appeal, it can be observed that the mathematical background knowledge, skills, and maturity vary considerably for students entering M.Sc. degree programs in information security, even though formal requirements have been met. Reasons for this diversity include that students may have been enrolled in undergraduate degree programs which placed a different emphasis, e.g. a curriculum oriented more towards calculus instead of discrete mathematics and theoretical computer science in case of students from engineering programs.

In other cases students enter the program with significant work experience that did not exercise their mathematical skills acquired earlier, resulting in students that are formally qualified but whose capabilities have atrophied. A key

Please use the following format when citing this chapter:

Wolthusen, S., 2007, in IFIP International Federation for Information Processing, Volume 237, Fifth World Conference on Information Security Education, eds. Futcher, L., Dodge, R., (Boston: Springer), pp. 129–136.

challenge is therefore to provide a curriculum which can bridge these diverse levels of preparedness, inclination, and skill while maintaining sufficient rigor [2].

Research students at the doctoral level present a different set of challenges. While these research-oriented students typically do not take a utilitarian approach as may be the case for M.Sc. students who – rightfully – see the mathematical foundations of information security as only one tool of many to equip them to solve problems in what is typically an application domain, the nature of information security research as a cross-cutting concern implies a need for an equally broad theoretical background depending on the research interests of individual students.

While in some cases it may be possible to approach these problems to requiring completion of core courses in mathematics and theoretical computer science, the density and interdependencies within the study programs make such an approach problematic and potentially wasteful (see also [3] for a recent survey of approaches to information security program organization). A more targeted integration of the requisite foundations holds several potential advantages. First and foremost, the material can be presented in a more targeted manner unencumbered by the traditions in some areas which, while essential to the understanding of the area as a whole for research mathematicians, tend to include elements of limited interest when dealing with the typically more applied problems faced by students of information security. A second advantage inherent in this focused approach in that it allows a tighter integration into core information security curricula.

By ensuring that key concepts, e.g. from complexity and computability theory or number-theoretical foundations, which are required in several core curriculum components, are covered in such a way to both reinforce the concepts on one hand and to minimize the need for redundant yet, owing to its necessary brevity, superficial treatment of such material, it becomes possible to maintain a sufficiently challenging depth of coverage while at the same time providing a stronger motivation for interacting with these foundations since the curriculum helps to see interconnections and interdependencies which may be lost when covered in a more linear and independent manner. This, however, can only succeed if students view these foundations not merely as part of an isolated part of the curriculum (i.e. primarily cryptography courses) but rather as an integral and in many ways unifying element which is key to achieving a deeper understanding of the subject matter.

The remainder of this paper is structured as follows: Section 2 reviews opportunities and challenges for integrating appropriate reviews and elaborations on mathematical foundations into a M.Sc. curriculum which must take the diverse backgrounds and ultimately also the objectives of students into account. Section 3 then discusses the mathematical coursework for doctoral students either mandatory or recommended regardless of the specialization individual students are pursuing. The course offerings along with the motivation for their provision for the more specialized areas of interest are then detailed in section 4, with section 5 providing a summary of the experience to date and an outlook on further reviews and refinements to the proposed curriculum.

2 M.Sc. Level Foundations

As noted in section 1, the core problems requiring careful attention in providing a rigorous and solid theoretical foundation to information security studies at the M.Sc. level stem primarily from the diversity of backgrounds and, to a lesser extent, the diverging objectives students have for entering a dedicated degree program at the M.Sc. level without necessarily wishing to pursue further studies at the doctoral level [4].

The latter manifests itself primarily in a need to continuously motivate the inclusion of theoretical foundations with a clear perspective on the implications of such results and techniques. These can either be found immediately in applications, or can be motivated by emphasizing the cross-connections made possible by applying similar mathematical techniques in areas which at least at first seem disparate. The former issue, however, cannot be addressed entirely within the confines of the regular curriculum. By offering optional summer course modules in key areas of mathematics, students are given the opportunity to gain or refresh the requisite background and dexterity in applying mathematical techniques which can yield a comparable point of departure for all students beginning the program.

Several aspects need to be considered in structuring these offerings in addition to the content itself and must take the learning experiences and expectations of students into account. For students entering into the M.Sc. program, the learning techniques and strategies acquired before entering the program will differ markedly. Students entering the program directly after completing and undergraduate degree may, depending on their previous field of study, have an advantage over mature students, which are typically mid-career professionals released, often on a part-time basis, by their employers or are re-training in that they have skills more readily at their disposal, e.g. in performing calculations or algebraic transformations.

However, regardless of student background, several key techniques are often only inadequately developed except in case of students entering from an undergraduate program in mathematics, the most important of which is the concept of rigorous proof and a selection of proof techniques and heuristics. While even an intense summer program is insufficient to impart the dexterity in using these techniques one would need for approaching novel problems, the requirements in the information security program are more modest and focused. Based on an adequate degree of familiarity, students are enabled to both follow proof arguments and to explore minor variations and extensions to existing theorems on their own.

The preparatory summer course then provides a compact overview of several areas required as background for the mandatory and most elective courses offered within the M.Sc. program itself and is also recommended for students having covered this material in their previous studies. Since an introduction to cryptography is mandatory, this necessarily includes elements of number theory. Topics covered include the ring of integers (refined further in the segment on abstract algebra), congruences, and rings of integers modulo u. Selected algorithms covered include the Chinese Remainder Theorem and Fermat's Little Theorem for prime modulus together with Euler's generalization to arbitrary moduli, primitive roots and quadratic residues along with an introduction to the problem of factorization of large integers. This then leads to a coverage of core concepts from abstract algebra, including functions and relations, groups along with cyclic and permutation groups and homomorphisms. In addition, selected aspects of the properties of commutative rings and fields along with structures of groups are discussed, which naturally leads to a brief introduction to Galois theory.

Several M.Sc. modules also require familiarity with elementary probability and statistics; this is reflected in the coverage of probability models, conditional and unconditional probability, random variables, and probability distribution models in the preparatory course. Other requirements of several modules include basic combinatorics and set theory, together with an overview of topics in computability and complexity.

Mandatory core modules on cryptography and the theory of information security can then build on these common foundations without excessive repetition, with the former relying on the on the number theoretic, algebraic, and combinatorial background and the latter relying on the material on computability and complexity, abstract algebra, and probability theory. In addition, elective courses such as those on intrusion detection and authentication also can refer back to the common mathematical background while concentrating on the actual applications of this foundational material.

3 Common Elements for Doctoral Studies

The role of course offerings for doctoral studies is primarily intended as guidance and for providing the requisite background and intellectual tools for the conduct of research, therefore frequently concentrating on foundational aspects at the expense of more concrete research-related issues as the latter is more appropriately covered in the course of seminars and reading groups since this format allows a more immediate adaptation to current research and requirements of the doctoral students.

The mandatory modules for doctoral students in information security are therefore (in addition to modules on "Ethics and Legal Aspects of Scientific Research" and "Methodology of Scientific Research", which are beyond the scope of this paper) focusing on mathematical tools and approaches which can be adapted to the specific research needs. The first module, entitled "Discrete Mathematics" provides an introductory survey of discrete mathematical tools that students primarily interested in applications will require and is also intended to assist students entering the Ph.D. program from courses of study in which discrete mathematics was not a core part of the curriculum. In the course, a rigorous introduction to core topics of abstract algebra is provided through an introduction to linear algebra. The second part of the course is concerned with the introduction of key concepts of combinatorics, including aspects of graph theory and its applications. A second mandatory module which, however, may be substituted by another if a student can demonstrate that it will not be required in his or her particular research is entitled "Applied Statistics". Since this area represents a key tool in a number of areas of applied computer science, particularly where simulations and experiments are conducted and appropriate inferences and hypotheses must be derived, it is integrated into the core Ph.D. curriculum. In this course, the fundamental aspects of probability theory and mathematical statistics including the central limit theorem are covered before moving on to studies of techniques and approaches to modeling and inference, supplemented by fundamental aspects of stochastic processes. Based on this, students can then choose further specialized modules relevant to their research as detailed in the following secction 4.

4 Research Specializations at the Doctoral Level

The research of doctoral students falls into three broad categories, each of which in turn require different supporting modules providing the appropriate mathematical background. This is required for two reasons. First, Gjøvik University College does not have a separate graduate program in mathematics, and so must provide courses from within the information security program. This, however, provides a benefit simular to those described in section 2 for the M.Sc. program in thad secondly, it allows a more targeted approach in the construction of the individual modules to better support the needs of information security students.

The categories can be characterized as:

1. Purely theoretical information security or cryptography
2. Experimental information security
3. Research involving modeling and simulation

It is obvious that there will be research which requires more specialized mathematical background; this, however, is not the focus of the common foundations concept discussed here and is more properly addressed by individual research on the part of the Ph.D. student.

The mathematical background in support of the general research areas is concentrated mainly in the form of lectures as seminars tend to focus more on the concrete applications to information security (although e.g. in cases such as a seminar on "Cryptographic Primitives" and some lectures, the distinction may well be arbitrary). This has led to the identification of the following lecture and seminar modules:

4.1 Computational Methods and Complexity

This course encompasses the core models and mechanisms required for the design and analysis of algorithms and particularly computational models. To this end, models of computation, Turing machines, recursive functions, Church's thesis, λ calculi, decidability, and computability, are covered. Beyond this core, denotational semantics and the logic of programs are covered as well as applications to automata, formal languages, program verification, and programming languages. A final component of the course provides an overview of complexity theory including analytical techniques and an introduction to complexity hierarchies.

4.2 Advanced Graph Theory and Combinatorics

The course begins with classical combinatorics, including counting functions (arbitrary, injective or surjective functions with domain and range either distinguishable or indistinguishable) and enumerations (sets, multisets, permutations, multiset permutations, partitions, set partitions, and compositions). Applications to Bell numbers, Stirling numbers of the first and second kinds, and Eulerian numbers are covered as well as the recurrence relations and bijective methods in proofs. Algebraic techniques covered include generating functions, particularly ordinary and exponential generating functions and applications to to partition problems. Gaussian polynomials are covered in connection with partitions, the lattice of subspaces of a vector space over a finite field, and the q-binomial Theorem.

This course also covers core aspects of graph theory and combinatorics. Beginning with Hamiltonian and Euler circuits and flows including the Max-Flow Min-Cut theorem, integral flows and Menger's theorem, approaches to extremal problems are examined together with selected aspects of Ramsey theory and representation mechanisms. Graph topologies as well as both random and power-law graphs are covered along with selected tools on graph morphology.

4.3 Pattern Recognition

In this course, fundamental aspects of classification techniques are covered, including both parametric and nonparametric techniques. Specific approaches and techniques discussed include linear classifiers and support vector machines, multilayer neural networks, stochastic classification methods that include genetic algorithms and simulated annealing, as well as unsupervised learning and clustering, while emphasizing the connections to applied statistics.

4.4 Computation in Number Theory and Elliptic Curves

This course is primarily intended for students interested in cryptography and covers elements of computational number theory and particularly elliptic curves. Areas covered include a detailed analysis of the Extended Euclidean algorithm and the Montgomery method, deterministic primality testing, generators in $\mathbb{Z}_p^*$, arithmetic over polynomial and finite fields.

5 Conclusions

In this paper we have presented a proposed curriculum structure which deliberately concentrates the mathematical foundations and prerequisite material for research in information security with the aim of striking an appropriate balance between accessibility and rigor.

We believe that the inclusion of these theoretical foundations are an essential prerequisite for conducting successful research not only in the theory of information security and related areas such as cryptography but also in quantitative and applied areas. At the same time we recognize that, particularly at the M.Sc. level, students expect to be exposed to applied and immediately applicable material which they can leverage directly in their subsequent career. At the same time, there appears to be a strengthening negative correlation between the perceived (mathematical) rigor of a degree program and the uptake by students.

It is therefore incumbent on degree programs such as the one we describe to provide a compelling argument for the retention of the theoretical background of information security in the curriculum instead of cutting back on this apparent impediment to student uptake of the degree programs. The key argument we see in favor of the more rigorous and mathematically oriented curriculum is that it enables students to see interconnections and common patterns more clearly, particularly if the courses are designed to strengthen such discovery and analysis. While such a bespoke approach may not be feasible in environments below a certain size or where graduate-level mathematics courses are provided as a service from an established mathematics department, both constraints are not present in case of Gjøvik University College, enabling the development of a mathematics and theory curriculum intended first and foremost to support the core information security curriculum.

As research foci and student requirements change, this curriculum will require constant adjustment to maintain this balance, e.g. also in response to an increased intake of students at both the M.Sc. and Ph.D. levels from countries in which, even though formal degree equivalence may be given, the relevant undergraduate programs may have placed the relative emphasis on different areas. Above all, however, the curriculum must evolve in response to the objective requirements of students and, at the M.Sc. level based on longitudinal surveys of graduates.

Acknowledgments The author would like to thank E. Hjelmås, H. Engenes, J. Gonzalez, S. Petrović, E. Snekkenes, and C.-H. Tan for valuable discussiona and comments.

References

1. Hjelmås, E., Wolthusen, S.: Full-Spectrum Information Security Education: Integrating B.Sc., M.Sc., and Ph.D. Programs. In: Proceedings of the 3rd Annual Conference on Information Security Curriculum Development, Kennesaw, GA, USA, ACM, ACM Press (2006) 9–16

2. Hentea, M., Dhillon, H.S., Dhillon, M.: Towards Changes in Information Security Education. Journal of Information Technology Education **5** (2006) 221–233
3. Taylor, C., Shumba, R., Walden, J.: Computer Security Education: Past, Present and Future. In: Proceedings of the Seventh Workshop on Education in Computer Security (WECS7). (2006) 67–78
4. Ciechanowicz, C., Martin, K.M., Piper, F., Robshaw, M.J.B.: Ten Years of Information Security Masters Programmes. In: World Conference on Information Security Education. (2003) 215–230