Applied Cryptography

Proposal Overview

New/Revise: New

Proposal Summary and Rationale

Cryptography is an indispensable tool for protecting information in computer systems.
The word “Cryptography” means “Hidden Writing”. Cryptanalysis involves analysing ciphers. Cryptography has a long history that dates back to 1900 BC. It is believed to be used by the Romans including Julius Caesar to communicate to his generals. It has been used extensively during World Wars I and II including the famously known Enigma machine. Post World Wars an enormous amount of effort has been put into Cryptography research by the government and corporations like IBM who designed the Data Encryption Standard (DES) algorithm that became the first federal government cryptography standard in the United States. Since then, Cryptography has been extensively used in computer systems protecting networks and data. Financial institutions and Critical infrastructures all have sophisticated cryptographic algorithms to protect against attackers. Quantum Computing has brought in a new challenge to many cryptography algorithms that can be broken by powerful quantum computers. Cryptography is central to Cybersecurity.

The objective of the course is to explain the inner workings of cryptographic primitives and how to use them correctly in a broad range of applications. The emphasis is on understanding foundational concepts of encryption and authentication techniques and effectively using them to protect data and communications. Quantum Safe Cryptography will also be studied, as Classical Cryptography can be broken by powerful quantum computers.

The rationale behind this proposed course is fourfold: (1) Cryptography is a well established discipline within Cybersecurity and there is a need to have a dedicated course within the Cybersecurity specialisation. (2) Strong demand from industry to encrypt data and manage digital credentials after a series of data breaches in the recent past. (3) The proposed course has been discussed in CSE’s proposed Cybersecurity Specialisation within the Masters of Information Technology and in the Future Cybersecurity Working Group. The proposed course will be included in the planned CyberSec Masters program (MIT), which may start in 2024 as discussed within the working group. (4) A strong thrust on Quantum Technologies by the Australian Government necessitates the need to develop Quantum Safe Cryptography solutions.

Proposal Contacts:

Author: Sushmita Ruj
Proposal Sponsor: John Shepherd
Consultation: Thomas Britz (School of Mathematics and Statistics), Aruna Seneviratne (School of Electrical Engineering and Telecommunications), Cybersecurity Working group.

Course Information

Course Name: Applied Cryptography

Course Name – SiMs: Cryptography

Owning Faculty: Faculty of Engineering

Owning Academic Unit: School of Computer Science and Engineering

Administrative Campus: Sydney

Units of Credit: 6

Grading Basis: Standard UNSW grades

Academic Calendar Type: 3+

Career: Postgraduate

Academic Details

Course Description for Handbook

This course is designed to provide an understanding of Cryptographic algorithms and Cryptanalysis with an aim of using them to protect computer systems, networks, and data. The course will emphasise on the foundational aspects of encryption and authentication techniques with an aim to use them correctly in applications. By the end of this course students will learn about security notions, encryption and authentication techniques, their implementations and use them in practise. They will also learn about the recent quantum safe Cryptographic algorithms.

Field of Education (Broad): 020000 Information Technology

Field of Education (Narrow): 020100 Computer Science

Field of Education (Detailed): 029901 Security Science

Teaching Strategies and Rationale:

The lectures will provide the mathematical tools that are useful for designing cryptographic primitives and cryptanalysis. The lectures will also help understand the theoretical foundations of encryption, authentication, and cryptographic protocol design. A key component of cryptography is the ability to be able to write security proofs to justify that the protocols are secure. This will be taught during the lectures. Examples and applications will be discussed to show how the primitives and protocols are used in practice. Case studies will

help understand how cryptography is used in practice. Apart from lecture slides, web resources including popular lecture notes, research articles, blogs and videos will be posted.

Tutorials will aim at two aspects, problem solving and implementation. During the problem-solving sessions, students will be divided into two groups, one proposing a solution and the other attacking the solution. This approach will boost critical thinking. Implementation of popular security primitives and protocols will help students understand and use existing cryptographic libraries and implement larger applications.

At the end of the course the students will work on a practical project in small groups. Each group will work on a different project. This will help understand the relationship between various aspects of protocol design. Working in teams will help students appreciate the value of teamwork and collaboration. An end of term exam will also help demonstrate the understanding of foundational concepts, writing proofs and critical thinking while problem solving.

Course Aims

The objective of the course is to explain the inner workings of cryptographic primitives and how to using them correctly in a broad range of applications. The emphasis is on understanding foundational concepts of encryption and authentication techniques and effectively use them to protect data and communications. Students will be taught to think critically while analysing and designing secure protocols. Emphasis will be given to formally analyse security through mathematical proofs. Implementation of algorithms and protocols will be done. Quantum Safe Cryptography will also be studied, as some Cryptographic algorithms can be broken by powerful quantum computers. At the end of the course, the students will be equipped with a range of cryptographic tools and techniques to solve various practical security and privacy problems.

Course Properties

Course Type: Award Course

Learning outcomes

CLO1: Learn the foundations of cryptography, primitives, and protocols, including encryption and authentication.

CLO2: Understand techniques of Cryptanalysis and be able to perform Cryptanalysis on ciphers.

CLO3: Understand security notions and be able to formally analyse security of protocols.

CLO4: Implement cryptographic algorithms including practical encryption and authentication protocols.

CLO5: Design secure cryptographic protocols for a broad range of applications like blockchains, e-commerce and computer networks.

CLO6: Understand the implications of quantum computing on Cryptography and learn about existing quantum safe solutions.

Assessment 1: Fortnightly Assignments

Assessment Type: Assignment
Assessment Name: Fortnightly Assignments
Weighting (%): 25%
Group or Individual: Individual
Assessment Overview: Assignments in weeks 2, 4, 6 and 8 is a mixture of quizzes, implementations, and written assignments.
This will include cryptanalysis of a given cipher in week 2.
Quiz on symmetric key encryption and authentication algorithms in Week 4.
Quiz on public key encryption algorithms and digital signatures algorithms in Week 6.
Written assignment on zero-knowledge proofs.

These assignments will help evaluate the student's understanding of cryptographic algorithms, analysis and help in problem solving.
Mapping to Learning Outcomes: CLO1, CLO2, CLO3

Assignment 2: Term Project + Paper

Assessment Type: Assignment
Assessment Name: Term Project + Paper
Weighting (%): 30%
Group or Individual: Group of 2-3 students
Assessment Overview: The aim of this assessment is to design and implement a secure and efficient application. Students choose their problem statement after consultation with the lecturer. The type of applications could be (but not limited to) an e-voting, computing, or searching on encrypted data, privacy preserving auction, credential management, Secure messaging, quantum safe protocol for the Internet. The expected outcome is a prototype and paper. The paper should include security definition, algorithms, security proofs and results of the implementation.

Mapping to Learning Outcomes : CLO3, CLO4, CLO5, CLO6

Assignment 3: Final Exam

Assessment Type: Exam
Assessment Name: Final Exam
Weighting (%): 40%
Group or Individual: Individual

Assessment Overview: The aim of this assessment is to evaluate student's understanding about design and analysis of cryptographic protocols and use cryptographic primitives to solve a problem. Algorithm design and analysis will be evaluated.
Mapping to Learning Outcomes : CLO1, CLO2, CLO3, CLO4, CLO5, CLO6

Prerequisites: COMP9024 Data Structures and Algorithms and COMP9020 Foundations of Computer Science

Syllabus:

Overview of Cryptography and background: Mathematical foundations. What is a Cipher? Classical Ciphers. Cryptanalysis. Security Notions.

Symmetric Key Encryption: Stream Ciphers, Block Ciphers, Modes of operation, Formal models for block and stream ciphers- Pseudorandom generators, Pseudorandom functions, and permutations. Cryptanalysis of block ciphers and stream ciphers. Implementations of standard ciphers.

Message Integrity: Definitions and Applications. Hash Functions, Birthday attacks, Merkle-Damgard construction, SHA, Message Authentication Codes, and implementations.
Case study and Application- Password management, CBC-MAC, Network Protocols, searching on encrypted data.

Public Key Cryptography: Mathematical basics, Diffie Hellman Key Exchange, RSA and its variants, El Gamal Encryption, Elliptic Curve Encryption, Implementations.
Applications: (RSA) Accumulators, Commitments.

Digital Signatures and applications: Secure Signatures, RSA Signatures, Digital Signature algorithm (DSA), Lamport Signatures, Identity management. Public Key Infrastructure (PKI) management.
Case study and Application: Pretty Good Privacy (PGP), Certificate Transparency.

Zero-Knowledge Proofs (ZKP): Interactive proofs, Non-interactive proofs, Fiat Shamir Transform, ZKP in practice, Succinct non-interactive zero-knowledge proofs (SNARKs).
Applications: Privacy preserving applications including (but not limited to) Anonymous Communications, Anonymous Credentials, Self-Sovereign Identities,

Post Quantum Cryptography: Motivation, Shor's algorithm for Factorization, Lattice-based Cryptography, Hash-based Cryptography.

Applications: Cryptography for blockchains, credential management, computing on encrypted data in cloud (homomorphic encryption, secure multiparty computation).

Relationship with other courses: All the other courses are UG courses.

MATH3411 (Information, codes and Ciphers). Has three sections- Information theory, Coding Theory and Cryptography. There are four lectures in 1 week on Cryptography covering Classical ciphers, one-way functions, trapdoor functions, Diffie-Hellman key exchange, RSA and related encryption, and entropy. No implementation is provided.

TELE3119 (Trusted Networks): This course consists of some basic cryptography and network security. Topics in cryptography include classical ciphers, Block ciphers, Asymmetric Encryption, Diffie Hellman Key Exchange, Public Key Infrastructure: MACs, HASH Functions. The rest of the course is on network security.

Cryptanalysis, Cryptographic implementation, and formal analysis of protocols is not covered. ZKP, post quantum cryptography, and some applications are also not covered in the course. Secure Network is the focus of the course.

ZEIT 3102 (Cryptography): *Offered in UNSW, Canberra.* This has three weeks of classical ciphers, Stream Ciphers, Block Ciphers, Public key encryption and signature algorithms. Cryptanalysis, implementation, and formal analysis of protocols is not covered. ZKP, post quantum cryptography, and some applications are also not covered in the course.

It discusses quantum Cryptography but not post quantum cryptography. The two are very different.

The proposed course being a PG course is dense (more content), has technical rigour and strong focus on applications.