Note that these courses may be adjusted over the coming months which may involve some adjustments of the course content, learning objectives and summative assessment.

The list of courses is the currently planned one but it is subject to change.
CS4100 - Data Analysis

Prerequisites:

Course value: 15

COURSE SUMMARY

The course teaches fundamental facts and skills in data analysis, including machine learning, data mining and statistics

Course Content:

- Supervised learning: classification, regression, and ensemble methods.
- Algorithm-independent machine learning
- Unsupervised learning and clustering
- Exploratory data analysis
- Bayesian methods. Bayes networks and causality
- Applications, such as information retrieval and natural language processing

LEARNING OUTCOMES

- Develop, validate, evaluate, and use effectively machine learning models and statistical models
- Apply methods and techniques such as clustering, regression, decision trees, and neural networks
- More generally, extract value and insight from data

TEACHING AND LEARNING METHODS

Lecture based delivery support by lab session, guided independent study. Normally 3-5 hours of lectures / practical classes and workshops per week.

KEY BIBLIOGRAPHY

FORMATIVE ASSESSMENT AND FEEDBACK

Oral feedback in lab sessions
Written feedback on three programming coursework assignments

SUMMATIVE ASSESSMENT

Details of coursework submission deadlines will be published on the department website at the start of term.
CS4200 - On Line-Machine Learning

Prerequisites: Course unit providing good knowledge of MATLAB or sufficient past experience.

Course value: 15

COURSE SUMMARY

The course addresses the on-line framework of machine learning in which the learning system learns and issues predictions or decisions in real time, perhaps in a changing environment. The course teaches protocols, methods and applications of on-line learning.

The course covers probabilistic on-line models based on Markov chains and their applications (PageRank, Markov chain Monte-Carlo) with a particular focus on hidden Markov models. Time series models are covered and their connections with Kalman filters are explored.

Learning models based on the prequential paradigm are covered in depth, including prediction with expert advice, aggregating algorithm, sleeping and switching experts. Universal algorithms are covered with an application to portfolio theory including Cover’s universal portfolios.

Finally, prediction with confidence framework is covered.

LEARNING OUTCOMES

- understand and evaluate probabilistic and non-probabilistic on-line learning protocols;
- demonstrate advanced understanding of the prequential and prediction with confidence frameworks;
- demonstrate advanced knowledge of methods of Markov models, prediction with expert advice and prediction with confidence;
- analyse the properties of on-line learning algorithms;
- apply on-line algorithms to real-world data and evaluate the results.

TEACHING AND LEARNING METHODS

Lecture based delivery support by practical classes, guided independent study. Normally 4-5 hours of lectures / practical classes per week.

KEY BIBLIOGRAPHY

• D. Barber, Bayesian Reasoning and Machine Learning, Cambridge, 2012.


FORMATIVE ASSESSMENT AND FEEDBACK

Oral feedback in practical classes / lab sessions. Written feedback on coursework assignment.

SUMMATIVE ASSESSMENT

Details of coursework submission deadlines will be published on the department website at the start of term.
CS4234 - Large-Scale Data Storage and Processing

Prerequisites: CS1801 or CS1802

Course value: 15

COURSE SUMMARY

Study underlying principles of storage and processing massive collections of data, typical of today’s Big Data systems. Gain hands-on experience in using large and unstructured data sets for analysis and prediction.

The topics covered will include techniques and paradigms for querying and processing massive data sets (MapReduce, Hadoop, data warehousing, SQL for data analytics, stream processing), fundamentals of scalable data storage (NoSQL data bases such as MongoDB, Cassandra, HBase), working with dynamic web data (data acquisition, data formats), elements of cloud computing, and applications to real world data analytics and data mining problems (sentiment analysis, social network mining).

Course Content:

- Techniques and paradigms for querying and processing massive data sets (MapReduce, Hadoop, data warehousing, SQL for data analytics, stream processing)
- Fundamentals of scalable data storage (NoSQL data bases such as MongoDB, Cassandra, HBase)
- Working with dynamic web data (data acquisition, data formats)
- Elements of cloud computing, and applications to real world data analytics and data mining problems (sentiment analysis, social network mining)

LEARNING OUTCOMES

- Knowledge and understanding of core concepts, theories and principles of large scale data storage and processing frameworks
- Sound evaluation of opportunities and challenges related to leveraging those frameworks for building massive scale analytics solutions, and an ability to make recommendations to resolve these challenges
- Proficient knowledge and use of at least one large scale data store systems, and at least one massive scale processing framework
- Ability to design, develop, and evaluate an end to end analytics solution combining large scale data storage and processing frameworks
• Knowledge of cloud computing as a platform for Big Data analytics

TEACHING AND LEARNING METHODS

Lecture based delivery and laboratory classes, guided independent study. Normally 4 hours of sessions.

KEY BIBLIOGRAPHY

• Rajaraman, Leskovec, Ullman, Mining of Massive Datasets, Available for free from http://infolab.stanford.edu/~ullman/mmds.htm


• Miner, Shook, MapReduce Design Patterns, O’Reilly, ISBN-10: 1449327176


FORMATIVE ASSESSMENT AND FEEDBACK

Verbal feedback will be provided during laboratory sessions.

SUMMATIVE ASSESSMENT

Details of coursework submission deadlines will be published on the department website at the start of term.
CS4504 - Business Intelligence Systems, Infrastructures and Technologies

Prerequisites: CS2855

Course value: 15

COURSE SUMMARY

Business Intelligence (BI) refers to the skills, processes, methodologies, technologies, applications, and practices used in order to leverage (gathering, storing, analyzing) an organization’s internal and external information assets to support and improve decision-making. With the advent of Big-Data there is considerably increased demand for skills and knowledge, both conceptual and technological, that can be effectively applied to support this new era of Big-Data based decision-making.

This course aims to provide students with
(a) a broad understanding of the information assets and the conceptual and technical architectures of information and business intelligence systems in modern organizations
(b) the necessary background knowledge of, and skills to design, implement and evaluate business intelligence systems and technologies.

Course Content includes the following topics:

Introduction to Information Systems & Business Intelligence: Overview of Information Systems and BI Systems, Information Systems and BI Technical Architectures (Logical & Physical aspects), Acquisition models and Business cases.

Data Warehousing and Dimensional Modelling (Definitions, Concepts, Architectures, Design Processes, Implementation Aspects)

BI Applications: OLAP, Reports, Dashboards, Data Mining, Visualization and UI design

Practical Sessions (Surgeries, Labs) on Dimensional Modelling, Reports and Dashboards using BI tools.

LEARNING OUTCOMES

By the end of the course students should be able to:

- demonstrate a holistic view of business intelligence systems and their role in the IT environment of modern organizations
- understand and evaluate the concepts, terminology and architectures of Data Warehouses and BI solutions
• understand Data Modelling concepts and provide design solutions using Dimensional Modeling

• know the important elements of business intelligence applications such as Data Analysis, Data Mining and Dashboards; understand and evaluate BI Visualization aspects and the relationship of BI solutions to CRM and ERP systems

• use industrial business intelligence tools

TEACHING AND LEARNING METHODS

The course will be taught in weekly sessions over the course of a term.

KEY BIBLIOGRAPHY

Core reading material:


FORMATIVE ASSESSMENT AND FEEDBACK

The lecturers will provide oral feedback during practical sessions and written feedback to coursework.

SUMMATIVE ASSESSMENT

Details of coursework submission deadlines will be published on the department website at the start of term.
CS4860 - Advanced Distributed Systems

Prerequisites:

Course value: 15

COURSE SUMMARY

The course will cover fundamental principles of building modern distributed systems, for example in the context of the Internet of Things. The specific emphasis will be on the two central components of the IoT reference architecture: cloud infrastructure and wireless networking.
The course will discuss major challenges found in these environments (such as massive scales, wide distribution, decentralisation, unreliable communication links, component failures and network partitions) and general approaches for dealing with these challenges.
The topics covered will include:
abstract models (such as the synchronous and asynchronous distributed computing models, models for wireless networks);
algorithmic techniques (such as distributed coordination, fault-tolerant design of distributed algorithms, synchronization techniques);
practical case studies.

The students will also have an opportunity to apply the studied material for implementing various components of a realistic distributed system through a series of formative coursework assignments, lab practicals, and a final project.

LEARNING OUTCOMES

- Display a mastery of core concepts, theories and principles of distributed systems
- Demonstrate knowledge of algorithmic techniques for solving problems in a distributed environment
- Explain the practical aspects of implementing various components of a distributed system
- Implement various components of a realistic distributed system

TEACHING AND LEARNING METHODS

Normally 4 hrs per week of lectures and laboratory sessions.

KEY BIBLIOGRAPHY

- Hagit Attiya, Jennifer Welch: Distributed Computing: Fundamentals, Simulations
FORMATIVE ASSESSMENT AND FEEDBACK

Oral feedback in laboratory sessions.

SUMMATIVE ASSESSMENT

Details of coursework submission deadlines will be published on the department website at the start of term.
CS4950 - Deep Learning

Prerequisites: Course unit providing good knowledge of MATLAB or sufficient past experience.

Course value: 15

COURSE SUMMARY

The aim of the course is to give students an introduction to deep learning that covers neural network optimisation by gradient descent from first principles, and which also gives a broader introduction to a range of advanced architectures, with hands-on implementation.

The course starts by considering models of artificial neural networks for supervised learning, and introduces notions of activation function, loss function, and computation of loss-gradients using back-propagation with the chain rule. Neural network learning with back-propagation and different gradient descent algorithms will be covered in detail, and visualised in lab-sessions. Next, the ‘disappearing gradient’ problem in deep architectures will be raised, and methods for resolving this problem will be discussed. A range of deep architectures will be described for discriminative learning, generative learning and learning of representations, and for reinforcement learning. Students will implement a deep architecture using a toolkit in a project assignment at the end of the course.

LEARNING OUTCOMES

By the end of this course a student should be able to:

- Demonstrate an advanced understanding of the notions of an artificial neural network, and of learning by minimising a loss function, using training, validation, and test data sets.

- Master computation of loss-gradients for different neural network architectures, and of a range of algorithms for optimisation by gradient descent, as applied in neural networks.

- Demonstrate a good comparative understanding of a range of deep learning architectures.

- Master the basic techniques necessary for gradient optimisation of deep networks, and of some diagnostics needed for determining whether gradient descent is working correctly.

- Apply deep learning algorithms to real-world data and evaluate the results.

- Implement and run deep learning algorithms using appropriate tool-kits.
TEACHING AND LEARNING METHODS

Lecture based delivery supported by laboratory sessions. Normally 4 hours of sessions per week.

KEY BIBLIOGRAPHY

- Deep Learning, by Ian Goodfellow, Yoshua Bengio, and Aaron Courville, MIT Press Dec 2016 (already available on web)

- The course will make extensive use of notes, handouts, and freely available material on the web, which is abundant and rapidly changing.

FORMATIVE ASSESSMENT AND FEEDBACK

Verbal feedback will be given during the laboratory sessions.

SUMMATIVE ASSESSMENT

Details of coursework submission deadlines will be published on the department website at the start of term.
IY4501 - Security Management

Prerequisites:

Course value: 15

COURSE SUMMARY

This course will explain the need for effective security management, identify the problems associated with security management, and consider the ways in which various organisations solve these problems.

The list of topics may vary slightly to reflect developments in the subject but typically will include:

- What is security and is it necessary?
- Security management approaches – an overview
- The role of standards in information security management
- Internal Control, Audit and Security.
- The role of risk in information security management
- Information Security, Governance and the Law.
- Case studies in information security management

LEARNING OUTCOMES

- evaluate security management requirements
- analyse critically alternative security management strategies and methods
- propose effective methods for responding to security management problems
- compare and critically evaluate different approaches to security management

TEACHING AND LEARNING METHODS

Lecture based delivery. Normally 3 hour of lectures per week.

KEY BIBLIOGRAPHY

- Critique of Security by Mark Neocleous (on-line access through the library)

FORMATIVE ASSESSMENT AND FEEDBACK

Oral feedback during lectures.

SUMMATIVE ASSESSMENT
Details of coursework submission deadlines will be published on the department website at the start of term.
IY4523 - Secure Business Architectures

Prerequisites:

Course value: 15

COURSE SUMMARY

The high level aim of this course is to discuss the appropriate system design and business response to technical/architectural decisions which impact the security of the organisation’s information.

The content of the course will include:
- Introduce the concept of a security development lifecycle
- An overview of the basics of Risk Assessment
- Elaborate on the Governance, Risk and Compliance issues discussed in the Security Management module
- Outsourcing/Cloud Computing architectures
- Identity Management
- The Payment Card Industry – Data Security Standard
- Supply Chain Security
- Big Data

LEARNING OUTCOMES

- understand, and be able to apply, the concept of a “security lifecycle” in relation to specific security architectures
- understand, and be able to outline the high-level components of a Risk Assessment and apply these components to candidate security architectures.
- appreciate the Governance, Risk and Compliance issues related to business architectures
- apply these to a number of architectures, such as: Identity Management; Outsourcing; PCI-DSS; Supply Chain

TEACHING AND LEARNING METHODS

Lecture based delivery. Normally 3 hour of lectures per week.

KEY BIBLIOGRAPHY

The course will not follow any individual text book, but is likely to make use of: international standards; industry white papers and research reports; case studies using common industry architectures.

FORMATIVE ASSESSMENT AND FEEDBACK
Oral feedback during lectures.

**SUMMATIVE ASSESSMENT**

Details of coursework submission deadlines will be published on the department website at the start of term.
IY4606 - Smart Cards, RFIDs and Embedded Systems Security

Prerequisites: IY2760 or equivalent; Cannot be taken by students who took IY3606.

Course value: 15

COURSE SUMMARY

Students will have developed a mastery of the topic of smart cards and token security.

Course contents:
Introduction to Smart Cards/Chips & RFID/NFC; Assets for Cyber Security
Smart Cards – Trusted Production Environment
Operating systems, Interoperability and Security
Applications & Security for Mobile Communications, USIM/SIM, Services and Clouds
Smart Cards for Secure Banking & Finance
Smart Cards in eIDs/Passports - & RFIDs/NFC explained
Advances in Smart Chips/Tokens, and Transport System Case Study
Common Criteria and Smart Cards
Security Attacks, Countermeasures and Testing for Smart Cards/RFIDs/NFC
Application Development Environments for JAVA and SIM Toolkit
Comparing Alternative Security Tokens/Environments; including TPM and TEE

LEARNING OUTCOMES

- identify constituent components, analyse strengths and weaknesses, identify new applications of smart cards/security tokens and their use as assets in cyber security; identify the steps in the manufacturing/personalisation processes, analyse and evaluate potential risks and compare security safeguards

- identify and compare the systems in use, analyse the strengths and weaknesses and evaluate interoperability and security issues; analyse the range of capabilities of SIM/USIM cards in Smartphones and apply them to new service ideas, evaluate the possible range of services and security measures

- understand the main standards and applications of smart cards for banking and finance, compare with earlier card solutions and analyse strengths and weaknesses of approaches; analyse the key role of the smart card/RFID for passports, IDs and satellite TV, evaluate the security measures that have protected past and current cards

- identify and describe new technologies, including NFC, TPM, TEE; and apply them to new applications and evaluate the likely suitability/success of approach; explain how common criteria may affect smart card design/development, analyse the different approaches and compare with less formal methods

- identify and describe the classes of attack and notable methods within each
class, analyse countermeasures and evaluate practicality of attacks and the effects on cyber security; identify, compare and evaluate different methods of developing applications for smart cards, and understand the development cycle and the use of practical tools

- analyse the issues concerning smart card lifecycle management, and evaluate and compare methods of local and remote card management

TEACHING AND LEARNING METHODS

Lecture based delivery. Normally 3 hour of lectures per week.

KEY BIBLIOGRAPHY


FORMATIVE ASSESSMENT AND FEEDBACK

Oral feedback during lectures.

SUMMATIVE ASSESSMENT

Details of coursework submission deadlines will be published on the department website at the start of term.
IY4609 - Digital Forensics

Prerequisites: IY2760 or equivalent; Cannot be taken by students who took IY3609.

Course value: 15

COURSE SUMMARY

Introduction to forensic science, steps from collecting data to preserving evidence, and a framework for digital forensic evidence collection and processing. Fundamentals of host forensics for Microsoft Windows, including kernel architecture, device driver architecture, registry, auditing, and security architecture, file system handling, and reconstruction of file and directory structures on the FAT and NTFS file system families. Fundamentals of host forensics for Unix derivatives using the Linux operating system as an exemplar, including kernel and device driver architecture, security and audit mechanisms, file systems and pseudo file systems, and the reconstruction of file and directory structures using UFS and Ext2/3fs as exemplars. Foundations of network forensics from data capturing and collection to network file systems and supplementary protocols as well as selected application-layer protocols and techniques used for identifying and reverse-engineering protocols used on networks. Introduction to malware including anti-forensics and propagation techniques. Introduction to steganographic techniques for images, video, textual data, and audio as well as steganalytical techniques for selected media types and approaches to traitor tracing. A survey of non-standard storage mechanisms from retention characteristics to mobile and smart phones and vehicular systems as well as network-based search and storage mechanisms.

LEARNING OUTCOMES

- understand the concepts of audit and indirect activity records retained by operating systems, particularly in file systems, and how to retrieve such information
- understand selected network protocols and the collection and derivation of evidence leading to the reconstruction of system and user activity based on network trace information
- understand infiltration and anti-forensics techniques used particularly by malicious software
- apply steganographic and particularly steganalytical methods for different types of media
- understand the retention characteristics of storage systems and non-standard devices such as mobile/smart phones, cloud computing, and vehicular systems
TEACHING AND LEARNING METHODS

Lecture based delivery. Normally 3 hour of lectures per week.

KEY BIBLIOGRAPHY

- B. Carrier: File System Forensic Analysis. Addison-Wesley, 2005

FORMATIVE ASSESSMENT AND FEEDBACK

Oral feedback during lectures.

SUMMATIVE ASSESSMENT

Details of coursework submission deadlines will be published on the department website at the start of term.
IY4610 - Security Testing Theory and Practice

Prerequisites: IY2760

Course value: 15

COURSE SUMMARY

To give students a mastery of Security testing theory and practice

Course Content:

- Security testing, legal aspects of penetration testing, standards and certification.
- Security testing frameworks and methodologies, and how to prepare, manage and conduct a professional penetration testing.
- Technical aspects of network security covering standards, protocols, routing, firewalls showing the theoretical basis of vulnerabilities and how these may be exploited in practice.
- Technical aspects of computer security covering operating systems, access control in windows and linux/unix, host based intrusion detection, escalation of privileges and how to exploit these vulnerabilities in practice and how to harden systems.
- Technical aspects of Internet based applications, web services, protocols, languages (e.g. SQL) and how these may be exploited using for example SQL injection and cross-site scripting; how to exploit these vulnerabilities in practice, and how to harden the applications.
- A survey of non-standard and emerging technologies and review of potential threats these may lead to.

LEARNING OUTCOMES

- Understand the legal aspects of carrying out a penetration test and an approach to preparing and managing such an audit.
- Understand, at a deep level, network protocols; computer system architectures; and application systems.
- Understand the vulnerabilities in existing protocols, systems, and applications.
- Understand the security technologies designed to mitigate these vulnerabilities.
- Understand how these vulnerabilities may be exploited in practice to penetrate a system.
TEACHING AND LEARNING METHODS
Lecture based delivery. Normally 3 hour of lectures per week.

KEY BIBLIOGRAPHY


FORMATIVE ASSESSMENT AND FEEDBACK
Oral feedback during lectures.

SUMMATIVE ASSESSMENT
Details of coursework submission deadlines will be published on the department website at the start of term.
IY4612 - Cyber Security

Prerequisites: IY2760 or equivalent; Cannot be taken by students who took IY3612.

Course value: 15

COURSE SUMMARY

Week 1: Introduction
Week 2: Networks and dependencies
Week 3: Critical infrastructures and interdependencies
Week 4: Security of Cyber-Physical Systems
Week 5: Control systems security
Week 6: Advanced persistent threats
Week 7: Attack modelling techniques
Week 8: System assurance
Week 9: Incident response mechanisms
Week 10: Offensive cyber operations
Week 11: Future challenges

LEARNING OUTCOMES

- have an understanding of network robustness and failures, together with key underlying theoretical concepts
- understand critical (information) infrastructures, vulnerabilities, and their dependencies
- appreciate the specific security problems of cyber-physical including SCADA systems and selected infrastructure
- understand complex attacks, analytical models for such attacks, and assurance mechanisms

TEACHING AND LEARNING METHODS

Lecture based delivery. Normally 3 hour of lectures per week.

KEY BIBLIOGRAPHY


FORMATIVE ASSESSMENT AND FEEDBACK

Oral feedback during lectures.
SUMMATIVE ASSESSMENT

Details of coursework submission deadlines will be published on the department website at the start of term.