## **COURSE SPECIFICATION FORM**

for new course proposals and course amendments

of cipher systems;         2. understand the structure of stream ciphers and block ciphers;         Know how to construct as well as have an appreciation of desirable properties of key stream generators, understand and manipulate the concept of perfect secrecy;         3. understand the modes of operation of block ciphers and their properties;         4. understand the concept of public key cryptography, including details of the RSA a ElGamal cryptosystems both in the description of the schemes and in their cryptanalys understand the concepts of authentication, identification and signature, be familiar w techniques that provide these, including one way functions, hash functions and interacti protocols, including the Fiat-Shamir scheme;         5. understand the problems of key management, be aware of key distribution techniques         6. demonstrate a breadth of understanding appropriate for an M-level course.         Cipher systems: An introductory overview of the aims and types of ciphers. Methods and types of attack. Information theory. Statistical tests.         Stream ciphers: The one time pad. Pseudo-random key streams - properties and generation.         Block ciphers: Confusion and diffusion. Iterated ciphers - substitution/ permutation. The Feistal principle, DES, AES, Modes of operation.         Public key ciphers: Discussion of key management. Diffie-Hellman key exchange. Oneway         Tunctions and trap-doors. RSA; ElGamal cryptosystem.         Authentication/identification: Protocols. Challenge/response. MACs. Zero-knowledge protocols; Fiat-Shamir protocol.         Digital signatures. Digital signature methods. Hash functions. DSS. Ce	Department/School:	Mathematics	Academic Session:	2017-18
Course Code:         MT4620         IPrease contact team Management in advect         G100           Availability: Immagine under the determination immagine under the determination advect         Term 1         Status:         Optional Condonable           Pre-requisites:         MT1820 and some probability         Co-requisites:         -           Course Staff:         -         -         -           Aims:         To introduce both symmetric key cipher systems and public key cryptography covering methods of obtaining the two objectives of privacy and authentication.         -           Learning Outcomes:         1. understand the concepts of socure communications and cipher systems; understand and use statistical information and the concept of optices of perfect socrecy; 3. understand the structure of stream ciphers and block ciphers; know how to construct as well as have an appreciation of desirable properties of key stream generators, understand and mainpulate the concept of perfect socrecy; 3. understand the concept of public key cryptography, including details of the RSA a ElGamal cryptosystems both in the description of the schemes and in their cryptanaby understand the concept of key management, be aware of key distribution techniques 6. demonstrate a breadth of understanding appropriate for an M-level course.           Course Content:         Chipher systems: The one time pad. Pseudo-random key streams - properties and generation.           Block ciphers: Confusion and diffusion. Iterated ciphers - substitution/ permutation. The Feistal principle, DES, AES, Modes of operation.         Diptic key ciphers: Distructure or 11 weeks. Total 33 hours.	Course Title:	Cipher Systems	(UG courses = unit value, PG courses = notional learning	0.5 units
Control         Term 1         Condonable           Pre-requisites:         MT1820 and some probability         Co-requisites:         -           Co-ordinator:         -         -         -           Aims:         To introduce both symmetric key cipher systems and public key cryptography covering methods of obtaining the two objectives of privacy and authentication.         -           Learning Outcomes:         1. understand the concepts of secure communications and cipher systems; understand and use statistical information and the concept of entropy in the cryptanalysis of cipher systems;         -           . understand the concept of public key cryptography, including details of the RSA as ElGamal cryptosystems both in the description of block ciphers;         -           . understand the concept of public key cryptography, including details of the RSA as ElGamal cryptosystems both in the description of the schemes and in their cryptanalys understand the concept of public key cryptography, including defails of the RSA as ElGamal cryptosystems. An introductory overview of the aims and their cryptanalys understand the concept of public key cryptography, including defails of the RSA as ElGamal cryptosystems both in the description of the schemes and in their cryptanalys understand the concept of public key cryptography, including defails of the RSA as ElGamal cryptosystems: An introductory overview of the aims and types of ciphers; Steman ciphers: Shamir scheme;           6. demonstrate a breadth of understanding appropriate for an M-level course.         -           6. demonstrate a breadth of understanding appropriate for and M-level course. <t< th=""><td>Course Code:</td><td>MT4620</td><td>(Please contact Data</td><td>G100</td></t<>	Course Code:	MT4620	(Please contact Data	G100
Co-ordinator:       -         Course Staff:       -         Aims:       To introduce both symmetric key cipher systems and public key cryptography covering methods of obtaining the two objectives of privacy and authentication.         Learning Outcomes:       1. understand the concepts of secure communications and cipher systems; understand and use statistical information and the concept of entropy in the cryptanalysis of cipher systems;         2. understand the structure of stream ciphers and block ciphers; know how to construct as well as have an appreciation of desirable properties of key stream generators, understand and manipulate the concept of perfect secrecy;         3. understand the concept of public key cryptography, including details of the RSA a ElGamal cryptosystems both in the description of block ciphers; know how to construct as well as have an appreciation and signature, be familiar w techniques that provide these, including one way functions, hash functions and interacti protocols, including the Fiat-Shamir scheme;         5. understand the problems of key management, be aware of key distribution techniques 6. demonstrate a breadth of understanding appropriate for an M-level course.         Course Content:       Cipher systems: An introductory overview of the aims and types of ciphers. Methods and types of attack. Information theory. Statistical tests.         Stream ciphers: The one time pad. Pseudo-random key streams - properties and generation.         Block ciphers: Discussion of key management. Diffie-Hellman key exchange. Oneway         Yunctions and trap-doors. RSA: ElGamal cryptosystem.         Authentication/Identification: Pro	(Please state which teaching	Term 1	Status:	
Course Staff:         -           Aims:         To introduce both symmetric key cipher systems and public key cryptography covering methods of obtaining the two objectives of privacy and authentication.           Learning Outcomes:         1. understand the concepts of secure communications and cipher systems; understand and use statistical information and the concept of entropy in the cryptanalysis of cipher systems; 2. understand the structure of stream ciphers and block ciphers; know how to construct as well as have an appreciation of desirable properties of key stream generators, understand and unsitive key cryptography, including the RSA a ElGamal cryptosystems both in the description of the schemes and in their cryptanalys understand the concept of public key cryptography, including thermality understand the concept of authentication, identification and signature, be familiar we techniques that provide these, including one way functions, hash functions and interact protocols, including the Fiat-Shamir scheme;           Course Content:         Cipher systems: An introductory overview of the aims and types of ciphers. Methods and types of attack. Information theory. Statistical tests.           Block ciphers: Confusion and diffusion. Iterated ciphers - substitution/ permutation. The Feistal principle, DES, AES, Modes of operation.           Block ciphers: Discussion of key management, bash unctions, and trap-doors. RSA; ElGamal cryptosystem.           Authentication/Identification: Protocols. Challeng/response. MACs. Zero-knowledge protocols; Fiat-Shamir protocol.           Digital signature subgit under stand signature (2015, 514, 514, 514, 514, 514, 514, 514, 5	Pre-requisites:	MT1820 and some probability	Co-requisites:	-
Aims:         To introduce both symmetric key cipher systems and public key cryptography covering methods of obtaining the two objectives of privacy and authentication.           Learning Outcomes:         1. understand the concepts of secure communications and cipher systems; understand the structure of stream ciphers and block ciphers; know how to construct as well as have an appreciation of desirable properties of key stream generators, understand the modes of operation of block ciphers and their properties;           2. understand the structure of stream ciphers and block ciphers; know how to construct as well as have an appreciation of desirable properties;           4. understand the modes of operation of block ciphers and their properties;           4. understand the concept of public key cryptography, including details of the RSA a ElGamal cryptosystems both in the description of the schemes and in their cryptanalys understand the concepts of authentication, identification and signature, be familiar w techniques that provide these, including one way functions, hash functions and interact protocols, including the Flat-Shamir scheme;           Course Content:         Cipher systems: An introductory overview of the aims and types of ciphers. Methods and types of atack. Information theory. Statistical tests.           Stream ciphers: Chrone time pad. Pseudo-random key streams - properties and generation.         Block ciphers: Confusion and diffusion. Iterated ciphers - substitution/ permutation. The Feistal principle, DES, AES, Modes of operation.           Public key ciphers: Discussion of key management. Diffie-Hellman key exchange. Oneway         Tonicons and trap-doors. RSA; ElGamal cryptosystem.           Authentication/Identifica	Co-ordinator:	-		
Mins-         methods of obtaining the two objectives of privacy and authentication.           Learning Outcomes:         1. understand the concepts of secure communications and cipher systems; understand and use statistical information and the concept of entropy in the cryptanalysis of cipher systems;           2. understand and use statistical information and the concept of entropy in the cryptanalysis of cipher systems;         2. understand the societ of stream ciphers and block ciphers; know how to construct as well as have an appreciation of desirable properties of key stream generators, understand and manipulate the concept of prefict secrecy;           3. understand the modes of operation of block ciphers and their properties;         4. understand the concepts of authentication, identification and signature, be familiar w techniques that provide these, including on way functions, hash functions and interact protocols, including the Fiat-Shamir scheme;           Course Content:         Cipher systems: An introductory overview of the aims and types of ciphers. Methods and types of attack. Information theory. Statistical tests.           Stream ciphers: The one time pad. Pseudo-random key streams - properties and generation.         Block ciphers: Discussion of key management. Diffie-Hellman key exchange. Oneway functions and trap-doors. RSA; ElGamal cryptosystem.           Authentication/Identification: Protocols. Challenge/response. MACs. Zero-knowledge protocols; Fiat-Shamir protocol.         Digital signatures: Digital signature wethods. Hash functions. DSS. Certificates.           The total number of notional learning hours associated with this course are 150.         3 hours of lectures per week over 11 weeks. Total 33 hours. </th <th>Course Staff:</th> <th>-</th> <th></th> <th></th>	Course Staff:	-		
Course Content:         understand and use statistical information and the concept of entropy in the cryptanalysis of cipher systems;           2.         understand the structure of stream ciphers and block ciphers; know how to construct as well as have an appreciation of desirable properties of key stream generators, understand and manipulate the concept of perfect secrecy;           3.         understand the modes of operation of block ciphers and their properties;           4.         understand the concept of public key cryptography, including details of the RSA a ElGamai cryptosystems both in the description of the schemes and in their cryptanalys understand the concepts of authentication, identification and signature, be familiar w techniques that provide these, including one way functions, hash functions and interact protocols, including the Fiat-Shami's rokeme;           6.         demonstrate a breadth of understanding appropriate for an M-level course.           Cipher systems: An introductory overview of the aims and types of ciphers. Methods and types of attack. Information theory. Statistical tests.           Stream ciphers: De one time pad. Pseudo-random key streams - properties and generation.           Block ciphers: Confusion and diffusion. Iterated ciphers - substitution/ permutation. The Feistal principle, DES, AES, Modes of operation.           Public key ciphers: Discussion of key management. Diffie-Hellman key exchange. Oneway           The total number of notional learning hours associated with this course are 150.           3 hours of private study, including work on problem sheets and examination preparation.           This total number o	Aims:			
Course content.types of attack. Information theory. Statistical tests. Stream ciphers: The one time pad. Pseudo-random key streams - properties and generation. Block ciphers: Confusion and diffusion. Iterated ciphers - substitution/ permutation. The Feistal principle, DES, AES, Modes of operation. Public key ciphers: Discussion of key management. Diffie-Hellman key exchange. Oneway functions and trap-doors. RSA; ElGamal cryptosystem. Authentication/Identification: Protocols. Challenge/response. MACs. Zero-knowledge protocols; Fiat-Shamir protocol. Digital signatures: Digital signature methods. Hash functions. DSS. Certificates.Teaching & Learning Methods:The total number of notional learning hours associated with this course are 150. 3 hours of lectures per week over 11 weeks. Total 33 hours. 117 hours of private study, including work on problem sheets and examination preparation. This may include discussions with the course leader if the student wishes.Key Bibliography:Cryptography: theory and practice (3rd edition) - D. Stinson (Chapman & Hall/CRC, 2006) Library ref: 001.5436 STI Introduction to cryptography: with coding theory - W. Trappe and L.C. Washington (Pearson Prentice Hall, 2006) Library ref: 001.5436 TRAFormative Assessment:Exam: 100% Written exam. A 2 hour paper. Coursework: None	Learning Outcomes:	<ul> <li>understand and use statistical information and the concept of entropy in the cryptanalysis of cipher systems;</li> <li>understand the structure of stream ciphers and block ciphers;</li> <li>know how to construct as well as have an appreciation of desirable properties of key stream generators, understand and manipulate the concept of perfect secrecy;</li> <li>understand the modes of operation of block ciphers and their properties;</li> <li>understand the concept of public key cryptography, including details of the RSA and ElGamal cryptosystems both in the description of the schemes and in their cryptanalysis; understand the concepts of authentication, identification and signature, be familiar with techniques that provide these, including one way functions, hash functions and interactive protocols, including the Fiat-Shamir scheme;</li> <li>understand the problems of key management, be aware of key distribution techniques;</li> </ul>		
Teaching & Learning Methods:The total number of notional learning hours associated with this course are 150. 3 hours of lectures per week over 11 weeks. Total 33 hours. 117 hours of private study, including work on problem sheets and examination preparation. This may include discussions with the course leader if the student wishes.Key Bibliography:Cryptography : theory and practice (3rd edition) - D. Stinson (Chapman & Hall/CRC, 2006) Library ref: 001.5436 STI Introduction to cryptography: with coding theory - W. Trappe and L.C. Washington (Pearson Prentice Hall, 2006) Library ref: 001.5436 TRAFormative Assessment & Feedback:Formative assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.Summative Assessment:Exam: 100% Written exam. A 2 hour paper. Coursework: None	Course Content:	types of attack. Information theory. Statistical tests. Stream ciphers: The one time pad. Pseudo-random key streams - properties and generation. Block ciphers: Confusion and diffusion. Iterated ciphers - substitution/ permutation. The Feistal principle, DES, AES, Modes of operation. Public key ciphers: Discussion of key management. Diffie-Hellman key exchange. Oneway functions and trap-doors. RSA; ElGamal cryptosystem. Authentication/Identification: Protocols. Challenge/response. MACs. Zero-knowledge protocols; Fiat-Shamir protocol.		
Key Bibliography.2006)2006)Library ref: 001.5436 STI Introduction to cryptography: with coding theory - W. Trappe and L.C. Washington (Pearson Prentice Hall, 2006) Library ref: 001.5436 TRAFormative Assessment & Feedback:Formative assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.Summative Assessment:Exam: 100% Written exam. A 2 hour paper. Coursework: None		The total number of notional learning hours associated with this course are 150. 3 hours of lectures per week over 11 weeks. Total 33 hours. 117 hours of private study, including work on problem sheets and examination preparation. This may include discussions with the course leader if the student wishes.		
Formative       The students will receive feedback as written comments on their attempts.         Assessment & Feedback:       Exam: 100% Written exam. A 2 hour paper.         Summative Assessment:       Exam: 100% Written exam. A 2 hour paper.	Key Bibliography:	2006) Library ref: 001.5436 STI Introduction to cryptography: with coding theory - W. Trappe and L.C. Washington (Pearson Prentice Hall, 2006) Library ref: 001.5436 TRA		
Assessment: Coursework: None	Assessment &			
				ated September 2017

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department's policy of continuous improvement and development. Every effort will be made to notify you of any such changes.