

## MA 4570 CRYPTOGRAPHY COURSE SYLLABUS

Text: An Introduction to Cryptology, H.C.A. van Tilborg, Kluwer Academic Press. We also will use Elementary Cryptanalysis, A. Sinkov, Random House and other texts as background material

The course is intended to provide an introduction to both the classical enciphering systems and also the more modern public key cryptosystems. We will show the strengths and weaknesses of the simple systems and indicate some simple cryptanalytic approaches to their solution. In general, the cryptanalytic techniques will lie beyond the scope of the course. A reasonable prerequisite for the course is a foundational grounding in the subject of applied modern algebra and finite fields as could be acquired in MA 3560. There will be a discussion of these topics briefly in the 3rd and 4th week of the course.

<u>HOURS</u>	<u>TOPIC</u>	<u>SECTION</u>
2-2	General Introduction	
2-4	Classical Systems, Caesar, substitutions, transpositions	
2-6	The Shannon approach	
3-9	Product ciphers, confusion & diffusion, P & S boxes	
6-15	Shift registers & finite fields	
4-19	DES	
3-22	Public key systems	
3-25	RSA	
2-27	McEliece system	
3-30	Knapsacks	
2-32	NP completeness	
3-35	Crypto complexity	
3-38	Selected topics	
6-44	Exams	