

962-G1-555

**Joshua R Holden\*** ([holden@math.duke.edu](mailto:holden@math.duke.edu)), Department of Mathematics, Duke University,  
Box 90320, Durham, NC 27708-0320. *Cryptography and Society: Report on a new course.*

During the fall of 2000, the presenter taught a new course entitled “Cryptography and Society” to 14 students at Duke University. This course was intended to introduce the student to the basic ideas of modern cryptography and its applications. Three main themes were addressed throughout the course:

- how modern cryptographic protocols are implemented and their strengths and weaknesses;
- how one encounters (and will increasingly encounter in the future) cryptography in one’s daily life;
- the implications of widespread use of cryptography in the digital age both for individuals and for society.

In addition to studying the mathematics behind modern cryptographic systems, we also examined the impact that the invention of modern cryptographic systems has had and will have on political, economic, philosophical, and sociological aspects of society. In short, this course was intended to provide students with a basic knowledge of cryptography and its uses sufficient for them to understand how it affects and will continue to affect their life and their society. This talk will relate my experiences with the course and examine my successes and failures. (Received September 15, 2000)