**Crypto and Cypherpunk Ethics**

*Overview*: In the early-1990s, the cypherpunks emerged as a grassroots movement simultaneously criticizing the emerging government mass surveillance made possible by the computer revolution and advocating the widespread use of digital encryption as the best means for individuals to protect their personal privacy from such surveillance. This module draws upon cypherpunk and cypherpunk-related ethical analyses of cryptography to explore the ongoing debates involving personal privacy, national security, system/device security, and the meaning of an open society. Through reading, discussion, and small group work, students will develop conceptual and practical knowledge about the ethics of cryptography.

*Learning Goals*:

Students will be introduced to real-world ethical arguments regarding security, privacy, and anonymity by movement actors.

Students will become familiar with the conceptual and ethical connections between privacy, toleration, and the open society.

Students will be introduced to the “security versus security” framing of ethical questions surrounding cryptography and law enforcement.

Students will examine the moral arguments of others regarding the ethics of cryptography.

Students will construct their own arguments regarding the ethics of cryptography.

Students will practice analyzing the tensions inherent in balancing various social goods and moral values.

*Key Questions*:

What how to we strike a balance between several desirable values—such as personal privacy, national security, and systems security—when they seem to be in conflict?

What is the relationship between cryptography, privacy, and an open society?

Are there any ethical limits to the uses of cryptography for personal privacy, and if so, what are those limits?

What is the best way to frame the ethical issues arising from the nature of cryptography?

What is the relationship between technical solutions and ethical solutions and how do we implement such solutions in relation to each other?

*Key Concepts*:

Means and Ends

Privacy

Security (multiple forms)

Open Society

Toleration

Diversity

*Activities*: This module consists of two lessons. For Lesson A, students learn about cypherpunk ethics by reading several short texts for homework and then discussing it in class. Instructors will lead students in discussing the ethical values that inform cypherpunk ethics, with special emphasis on toleration, privacy, and the open society. For Lesson B, students learn about the “security versus security” framing of cryptography ethics by reading two short texts for homework and then discussing it in class. Instructors will lead students in discussing the ethical values that inform debates about cryptography, law enforcement, and national security, with special emphasis on the value of having secure digital devices and networks.