Title: Algebraic Curves and Cryptography

Content (in chronological order):

1. Review of Finite Fields. A brief introduction to private and public key cryptography. (2 hours)
2. Elliptic Curves (2 hours)
3. Hyperelliptic Curves - (2 hours)
4. Complementary topics (pount-counting , pairing, factoring with elliptic curves, etc.) and Magma/GAP implementations - (2 hours)
5. Some additional topics as time permits - (2 hours)

Prerequisite: basic notions of group, ring and finite fields.

The mini-course is suitable for undergrad or graduate students in mathematics, computer science, physics and engineering.

Bibliography:

[1] Koblitz, Neal, A course in number theory and cryptography. Second edition. Graduate Texts in Mathematics, 114. Springer-Verlag, New York, 1994. x+235 pp.

[2] Koblitz, Neal Algebraic aspects of cryptography. With an appendix by Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato. Algorithms and Computation in Mathematics, 3. Springer-Verlag, Berlin, 1998. x+206 pp.

[3] Washington, Lawrence C. Elliptic curves. Number theory and cryptography. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2003. xii+428 pp.