References for elliptic curves and cryptography

See also the list on http://www.isg.rhul.ac.uk/~sdg/ecc.html

The books cover more contents than what we can do of the course. I try to highlight the parts of these book corresponding roughly to the course among three topics:

1. Cryptography: cryptography from the Discrete Logarithm Problem.
2. Elliptic curves: basic theory of finite fields and elliptic curves.
3. Pairings: basic theory of pairings.
4. Pairing based cryptography.

1 Elliptic curves and cryptography

Main reference:

- Washington, *Elliptic Curves: Number Theory and Cryptography* (intermediate level)
  Cryptography: § 5.2, Chapter 6 (§6.1, §6.2, §6.4, §6.5, §6.6).
  Elliptic curves: Chapter 2, § 3.1, Chapter 4 (§4.1, §4.2, §4.3).
  Pairings: Chapter 3.

Other basic references:

- Steven Galbraith, *Mathematics of Public Key Cryptography, Cambridge University Press* (2012), in particular Parts II, V and VII.
  Cryptography: Chapter 20.
  Elliptic curves: Chapter 9.
  Pairings: Chapter 26.
- Andreas Enge, *Elliptic curves and their applications to cryptography (an introduction).*
  Cryptography: Chapter 1, Chapter 4 (§4.1, 4.2, 4.3).
  Elliptic curves: Chapter 2 and 3.

- Koblitz, *A course in number theory and cryptography*
  Cryptography: §IV.3.
  Elliptic curves: Chapter 2, Chapter 6 (§VI.1, VI.2).

- Philippe Guillot, *Courbes elliptiques (une présentation élémentaire pour la cryptographie)*.
  Cryptography: Chapter 7.
  Elliptic curves: Chapter 1.
  Pairings: Chapter 2, Chapter 5.

- Mrabet, Joye, *Guide to pairing-based cryptography*.
  Cryptography: Chapter 1.
  Elliptic curves: Chapter 2.
  Pairings: Chapter 3.

Advanced topics to go further:

- Hankerson, Menezes, Vanstone, *Guide to elliptic curves cryptography* (for implementations).
  Cryptography: § 4.1.
  Elliptic curves: § 2.1, §3.1, §3.2.

- Blake, Seroussi, Smart, *Advances in Elliptic Curve Cryptography* (advanced cryptography).
  Pairings: Chapter IX
  Pairing based cryptography: Chapter X.

- Henri Cohen, Gerhard Frey, *Handbook of Elliptic and Hyperelliptic Curve Cryptography* (very complete).
  Cryptography: Chapter VI.23.
  Elliptic curves: Chapter II.9, III.13.
  Pairings: Chapter I.6. Pairing based cryptography: VI.24.

2 Elliptic curves and number theory

Elliptic curves are also very important for number theory. This is an advanced topic,here are some references:

- Tate, Silverman, *Rational points on elliptic curves*.
  Elliptic curves: Chapter 1.

- J. Silverman, *Arithmetic of elliptic curves* (the reference book).
  Cryptography: §XI.4, §XI.5.
  Elliptic curves: Chapter III, Chapter V, §XI.1.
  Pairings: §III.8, §XI.7, §XI.8, §XI.9.

- Milne, *Elliptic curves*, http://www.jmilne.org/math/Books/ectext6.pdf.
  Elliptic curves: Chapter II.

3 Sage

- Présentation de sage, https://www.math.u-bordeaux.fr/~gcastagn/Cryptanalyse/sage_pres.pdf
- Livre “Calcul mathématique avec Sage”, http://sagebook.gforge.inria.fr/
- Sage tutorial, https://doc.sagemath.org/html/en/tutorial/
- Quick reference, https://wiki.sagemath.org/quickref
- Sage documentation, http://doc.sagemath.org/