Part 2 Elliptic Curve Report:

1. User Instructions:

   Change directory to file containing source code using operating systems terminal.
   - Syntax needed to execute commands in the terminal are highlighted in yellow
   - All commands use the format: *java Main [command] [arguments]*
   - *Compile all java files using the command javac *.java in terminal*

   *Elliptic Curve Cryptography Commands*

   **Generate elliptic key pair from passphrase**
   Java Main genkey <passphrase> <publickeyfile>
   **Encrypt file with ECIES under public key**
   Java Main eciesenc <datafile> <outputfile><publickeyfile>
   **Decrypt ECIES file with password-derived private key**
   Java Main eciesdec <inputfile><outputfile><passphrase>
   **Sign file with Schnorr using password-derived private key**
   Java Main sign <datafile> <signaturefile> <passphrase>
   **Verify Schnorr signature under public key**
   Java Main verify <datafile><signaturefile><publickeyfile>
2. Implementation overview:
   Part 2 extends the SHA3/SHAKE foundation with elliptic curve cryptography based on the NUMS-256 Edwards curve. The implementation adds asymmetric encryption and digital signatures(Schnorr) to provide complete public-key cryptographic services.
   ***Edwards.java***: implements the NUMS-256 curve (x^2 + y^2 = 1 + 15343*x^2*y^2 mod p) with a nested point class handling curve arithmetic. The implementation uses the Edwards additions formula for point operations and binary scalar multiplication for efficiency.
   ***Main.java***: extends the existing command line interface with five new services such as key pair generation, ECIES encryption/decryption, and Schnorr signature generation/verification.
   All operations maintain security through proper domain separation, authenticated encryption, and secure random number generation.
3. Known issues:
   Several test were conducted manually for part 2 of this implementation. No known issues have been found however test was not thorough due to time constraints.
4. Sources cited:


Bernstein, Daniel J., and Tanja Lange. "SafeCurves: Choosing Safe Curves for Elliptic-Curve Cryptography." *SafeCurves Project*, 2013, safecurves.cr.yp.to.

Bos, Joppe W., et al. "Elliptic Curve Cryptography in Practice." *Financial Cryptography and Data Security*, vol. 8437, Springer, 2014, pp. 157-175.

Edwards, Harold. "A Normal Form for Elliptic Curves." *Bulletin of the American Mathematical Society*, vol. 44, no. 3, 2007, pp. 393-422.

Abdalla, Michel, Mihir Bellare, and Phillip Rogaway. "DHIES: An Encryption Scheme Based on the Diffie-Hellman Problem." *Cryptology ePrint Archive*, Report 2001/048, 2001, web.cs.ucdavis.edu/~rogaway/papers/dhies.pdf.

Shoup, Victor. "A Proposal for an ISO Standard for Public Key Encryption." *Cryptology ePrint Archive*, Report 2001/112, 2001, eprint.iacr.org/2001/112.pdf.

Schnorr, Claus-Peter. "Efficient Signature Generation by Smart Cards." *Journal of Cryptology*, vol. 4, no. 3, 1991, pp. 161-174.

Bernstein, Daniel J., et al. "EdDSA for More Curves." *Cryptology ePrint Archive*, Report 2015/677, 2015, eprint.iacr.org/2015/677.pdf.

Hankerson, Darrel, Alfred Menezes, and Scott Vanstone. Guide to Elliptic Curve Cryptography. Springer-Verlag, 2004.