CSE 5673-E1 CRN97670 Cryptology, Fall 2013, Project 1

Dr. Marius Silaghi

Shuhang Zhou, Haoyan Li

Requirement:

(submit as p1, by Nov 10). Implement the Digital Signature Standard using no other library than the BigInteger and Hash functions provided by the Java API. You may work in pairs, but not with the same colleague as for previous projects. The program to generate.sign/verify a key should be called with:

java DSS -p <size_in_bits_of_p> -q <size_in_bits_q> -S <secret_key_file> -P <public_key_file>

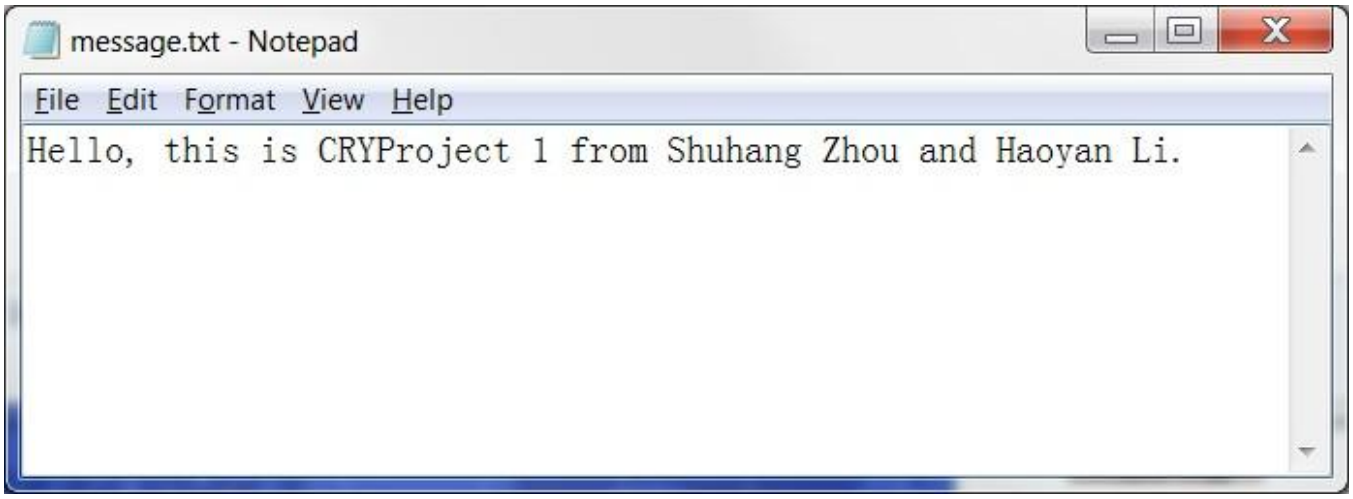
java DSS -M messagefile -S secret_key_file -s signature_file

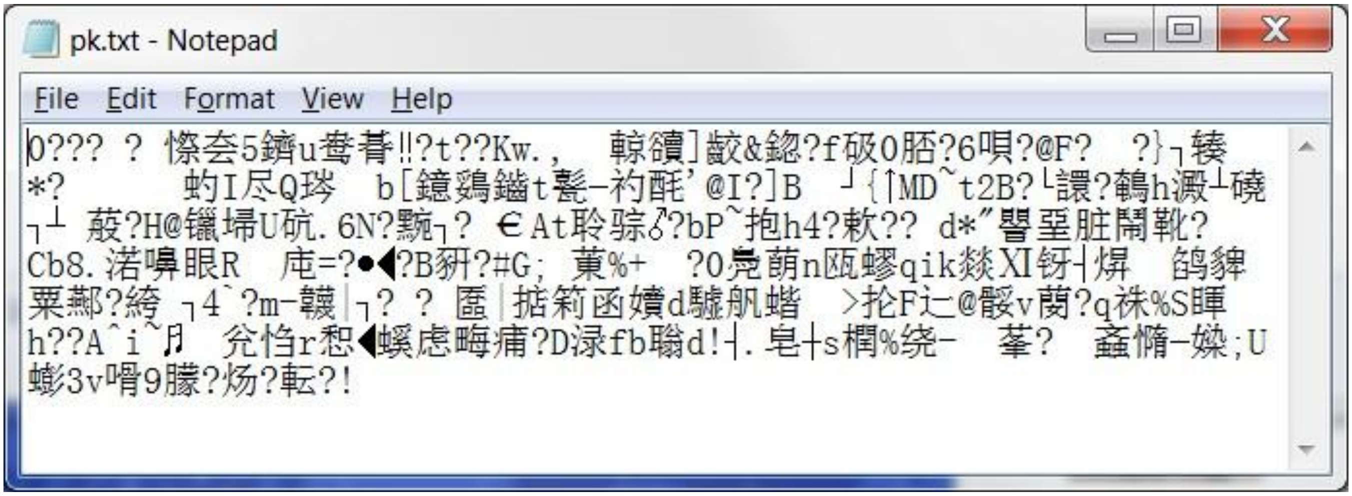
java DSS -M messagefile -P public_key_file -s signature_file

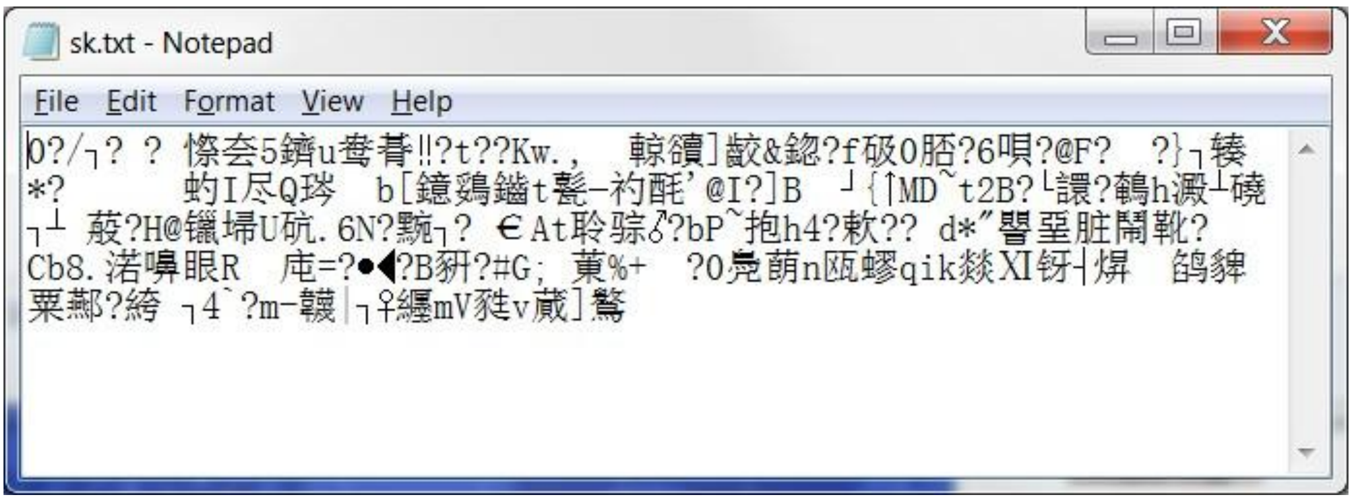
You get a 50% bonus if you make your implementation to follow the template for ECDSA on github.

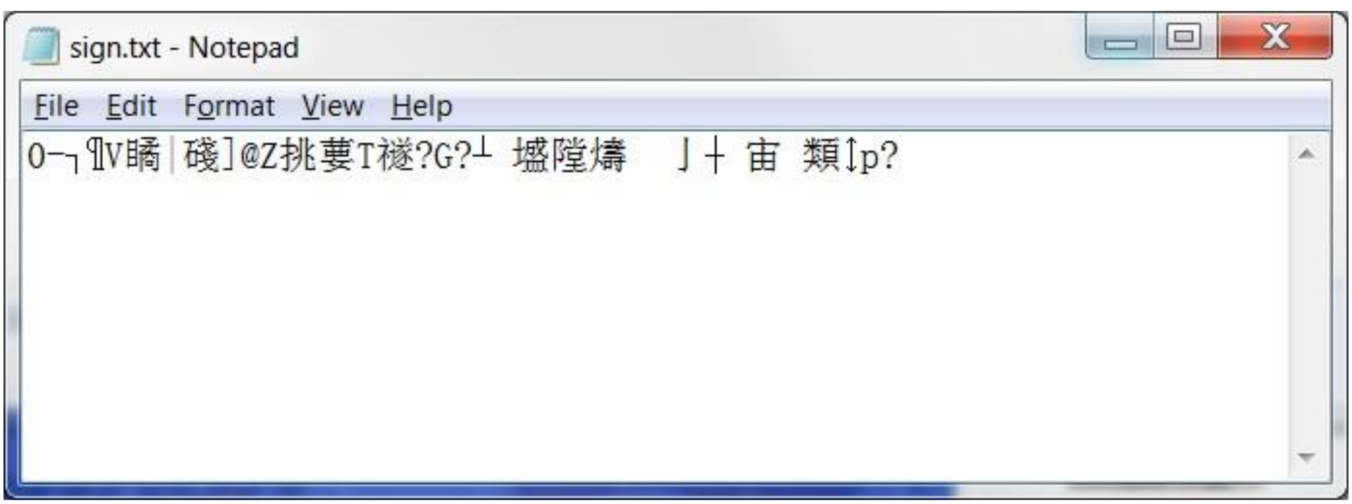
Secret DSA key with ASN1

Screenshot:




pk.txt - Notepad
File Edit Format View Help


sk.txt - Notepad
File Edit Format View Help


sign.txt - Notepad
File Edit Format View Help