

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>
```

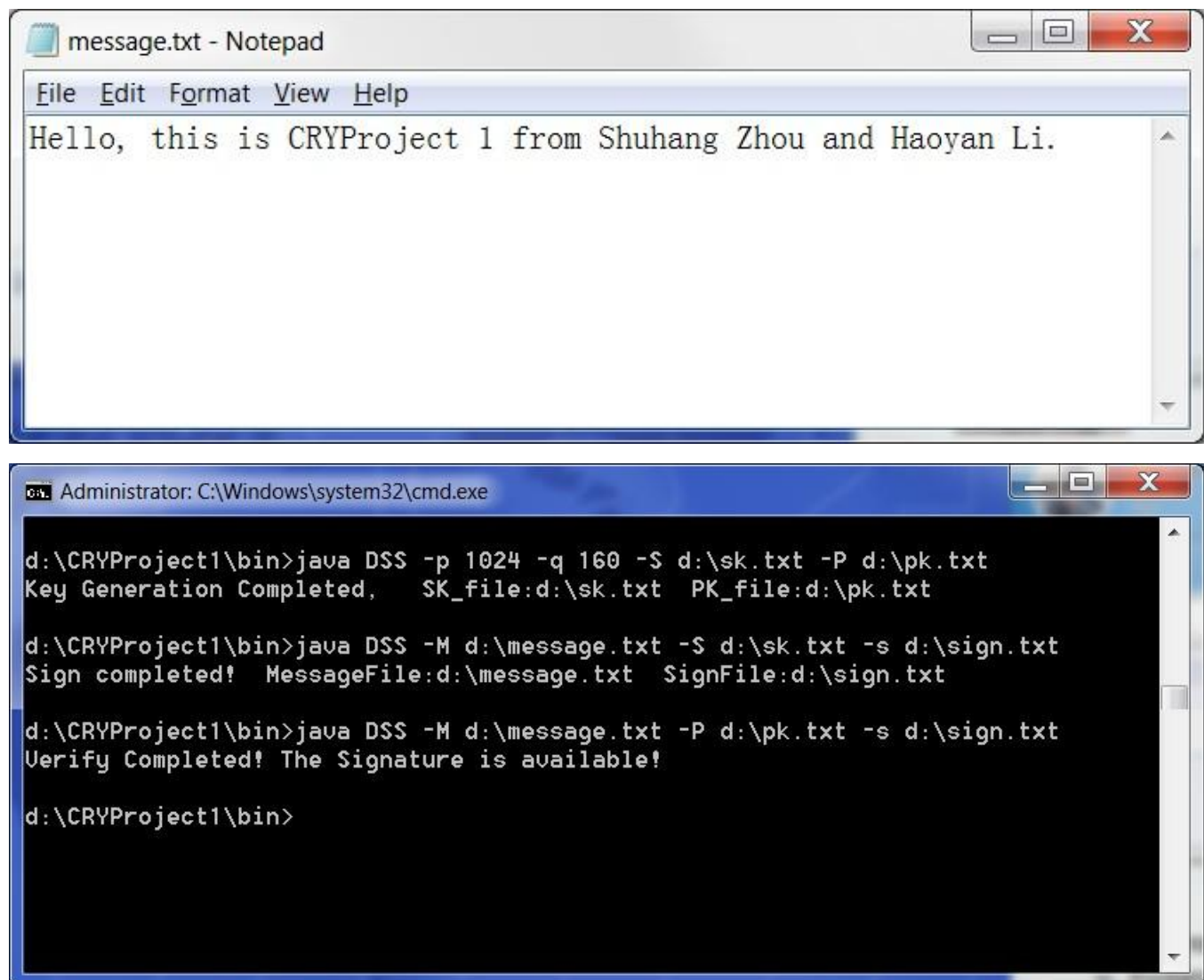
```
java DSS -M messagefile -S secret_key_file -s signature_file
```

```
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

0??? ? 憐套5鐙u鸯菁!!?t??Kw., 鯨鑽]敲&鋁?f碣0脬?6唄?@F? ?}┘棲
*? 蚰I尽Q琰 b[鑿鷄鎚t髻-杓酏'@I?]B ┘{↑MD~t2B?┘讓?鶴h澱┘磽
┘┘ 菝?H@鑷埽U硃.6N?黠┘? ∈At聆駝δ?bP~抱h4?欸?? d*"譬壘脏鬧靴?
Cb8. 渌鼻眼R 庖=?●◀?B豸?#G; 菓%+ ?0晃萌n瓠蟪qik燄XI钐┘焐 鴿貅
粟鄰?綉┘4`?m-轅┘? ? 匿|掂筴函嬪d驢舩蜡 >抡F┘@骸v蘭?q祿%S暉
h??A^i~卩 允怡r恕◀蟻慮晦痛?D渌fb聯d!┘.皂┘s櫛%绕- 葦? 蝥脩-嫫;U
蟪3v喟9滕?炀?軫?!

sk.txt - Notepad

File Edit Format View Help

0?/┘? ? 憐套5鐙u鸯菁!!?t??Kw., 鯨鑽]敲&鋁?f碣0脬?6唄?@F? ?}┘棲
*? 蚰I尽Q琰 b[鑿鷄鎚t髻-杓酏'@I?]B ┘{↑MD~t2B?┘讓?鶴h澱┘磽
┘┘ 菝?H@鑷埽U硃.6N?黠┘? ∈At聆駝δ?bP~抱h4?欸?? d*"譬壘脏鬧靴?
Cb8. 渌鼻眼R 庖=?●◀?B豸?#G; 菓%+ ?0晃萌n瓠蟪qik燄XI钐┘焐 鴿貅
粟鄰?綉┘4`?m-轅┘┘縈mV狴v葳]驚

sign.txt - Notepad

File Edit Format View Help

0┘┘V睛|磽]@Z挑蓼T襪?G?┘ 壘墮燐 ┘┘宙 類┘p?