NAME: SALLY
UOW ID: 4603229

Task 4

How to compile the program:

---

1. Open your command prompt
2. Navigate to folder where files are stored
3. javac DSA.java
4. java DSA
5. Follow instruction on the console

Output Screenshot:

DSA Generating Key

```
DSA Algorithm
-------------------------------------------------
(1) Key Generator
(2) Sign
(3) Verify
(4) Exit
Please enter your choice: 1
++++++Key Generated++++++
p: 95946262328460467179931494402676482952259849497875851139529584658743116057760351437408001622919278982233216846104123458960499355842241941461149569641349139
q: 1045850449391287268839531972301896236337928839897
g: 46235642074583107128271392114651339728317030656493655808272873004200789166223667972539820405386662283693078274940828121083633358694831670427417274163827107
u: 1030817448438014093957547275636348505918194296093
y: 40499860645980069831457037576158416263369875472574732551563781389455808401986461148494511009868245467246252319231615094672110931237355590873139451961771670

h: 1148770684833743922827140772525340006307642039457
```

DSA Signing

```
Please enter your choice: 2
++++++Generating message & store to file++++++
Random message generated: 1463384621
Please enter filename to store random message generated <press ENTER for default msg.txt>:
Message is successfully stored in msg.txt

++++++Message to be signed++++++
Please enter message input filename <press ENTER for default msg.txt>:
Finished reading message from msg.txt
+++++++++Inside hashFn+++++++++
m being hashed: 1463384621
hashedM: 1387598701728628872057058876564825324031704760310
+++++++++End hashFn+++++++++

Please enter filename to store signature <press ENTER for default sig.txt>:
Signature saved to sig.txt
r: 417118978169798095888656816103508411768174765144
s: 822590678968836398957431879371475153268493103886
+++++++++End signMsg+++++++++

++++++Message is signed and stored++++++
```

DSA Signature Verifying

```
Please enter your choice: 3
++++++Signature to be verified++++++
Please enter message filename <press ENTER for default msg.txt>:
Finished reading message from msg.txt
m: 1463384621

Please enter signature filename <press ENTER for default sig.txt>:
Finished reading signature from sig.txt
signature: 822590678968836398957431879371475153268493103886

w: 138788986487651869050913049670125668720606762603
t1: 39276523831243988013578803404626797886618810494 4
t2: 10349363010067134618220271070057354625507534568 81
v: 417118978169798095888656816103508411768174765144
r: 417118978169798095888656816103508411768174765144
Verification Result: true
++++++Signature is verified++++++
```