Assignment 2

Due: 11:55 pm 13 Feb 2021
Total Mark: 100 (17% of Final Mark)

General Instructions: Please read the following instructions carefully.

[**Q1-3**] Fill out the following Assignment2.JSON file. The values in the file must be **represented as hexadecimal numbers**. For example, the hexadecimal representation of decimal number 10 is 0xA.

```
{
   "DSAParam": [<g>, <p>, <q>],
   "pubkey": <pubKey>,
   "Sig": <sig>,
   "pubKeyHash": <pubKeyHash>
}
```

Assignment2.JSON

Q1. [15 marks] Create your own public key (i.e., verification key) and private key (i.e, signing key) pair for DSA 2048 bit digital signature using **Pycryptodome.** Write the DSA public parameters, `<g>`, `<p>` and `<q>`, and the public key `<pubKey>` in *Assignment2.JSON*.

Q2. [10 marks] Compute a signature by digitally signing "CSCI301 Contemporary topic in security" using your key generated in Q1. For signing, use DSA 2048 bit and SHA256 using the DSS class in **Pycryptodome** with "fips-186-3" option. Write the signature to `<sig>` in *Assignment2.JSON*.

Q3. [10 marks] To compute `<pubKeyHash>`, firstly, compute the hash value of your public key using SHA256 and, then, take the 160 least significant bits of the hash value. Write the result to `<pubKeyHash>` in *Assignment2.JSON*.

Q4. [50 marks] Using the completed Assignment2.JSON file, execute the following **"Pay-to-Pubkey-Hash"** script and show each step of script processing by printing out the values in the stack.

`<sig>` `<pubKey>` OP_DUP OP_HASH160 `<pubKeyHash>` OP_EQUALVERIFY OP_CHECKSIG

To make the script work with the values written in *Assignment2.JSON*. The cryptographic algorithms used in OP_HASH160 and OP_CHECKSIG are redefined as follows:

OP_HASH160: This operator computes the 160 least significant bits of SHA256 hash value of the last value in the stack.

OP_CHECKSIG: This operator verifies a signature <A> with the message "CSCI301 Contemporary topic in security" using a public key <B> when the last two values in the stack are <A> <B>. For the verification, DSA 2048bits with SHA256 is used in a way defined DSS (fips-186-3).

Q5. [15 marks] **A report** that 1) gives all necessary information to run your programs (e.g., the other python packages for your code, if they are used) and 2) explain expected outcomes (with screenshots) of each program.

Submission

Make a folder named `Assignment2` and include

- Completed *Assignment2.Json* and *SigningKey.txt*
- All programs of Q1-4
- Report (Q5)

Compress the `Assignment2` folder using a zip program to create `yourSurname_Assignment2.zip`.

Use Moodle to upload your zip file.