Ananya-Anita-Shahnaz-Satyam-IBE (AASS_IBE): An Open-Access IBE Encryption Tool

User Guidelines

STEP-1: Open and Edit the 'parampath.txt' file. Correct the path for the 'a.param' file depending on the exact path of the pbc-0.5.14/param Folder in your system.

Note: Make sure that there is no extra 'blank-space' or 'new-line' at the end of the string.

STEP-2: On terminal, run the setup phase using the following command:-

```
./aass_ibe_setup
```

This will generate two binary files, viz., 'MSK.bin' (containing the MSK (α)) and 'ibeparams.bin' (containing the IBE parameters g and $g1$)

STEP-3: run the KeyGen phase using the following command:-

```
./aass_ibe_keygen <MSK_file_name.bin> <User-ID>
```

For example, if you use the MSK file generated in Step-2 and want to generate the private key for the ID "soumyadev@iiita.ac.in", then use the following command:-

```
./aass_ibe_keygen MSK.bin soumyadev@iiita.ac.in
```

This will generate and store the Private-Key in a binary file named 'private_key.bin'

STEP-4: run the Encryption phase using the following command:-

```
 ./aass_ibe_encrypt <input_file_name.jpeg> <IBE_Params_file_name.bin> <User-ID>
```

Note that, **you have to give a JPEG image file as the input**. For example, if you use the IBE-Parameters file generated in Step-2 and want to encrypt the image file 'input.jpeg' for the ID "soumyadev@iiita.ac.in", then use the following command:-

```
./aass_ibe_encrypt input.jpeg ibeparams.bin soumyadev@iiita.ac.in
```

This will generate two binary files, viz., 'ciphertext.bin' and 'encrypted_key.bin'. The first file contains the encryption of the given data-file ('input.jpeg') - which has been encrypted using AES encryption using a randomly generated symmetric-key. The second file contains the IBE-Encrypted ciphertext of the symmetric-key.

STEP-5: run the Decryption phase using the following command:-

```
./aass_ibe_decrypt  <ciphertext_ile_name.bin>  <encryted_key_file_name.bin>
<IBE_Params_ile_name.bin>  <IBE_Private_Key_file_name.bin>
```

For example, in order to decrypt the encrypted file generated in Step-4, using the Private-Key generated in Step-3, under the IBE-Parameters generated in Step-2, use the following command:-

```
./aass_ibe_decrypt ciphertext.bin encrypted_key.bin ibeparams.bin private_key.bin
```

This will generate ‘output.jpeg’. Check whether the generated output is correct or not.

Additionally: you may run the VerifyKey Command to check whether a given Private-Key is correct against a given User-ID or not:-

Use the command:-

```
./aass_ibe_verifykey <IBE_Params_ile_name.bin> <IBE_Private_Key_file_name.bin>
<User-ID>
```

For example, in order to verify whether the private-key generated in Step-3 is correct against User-ID “soumyadev@iiita.ac.in” under the IBE-Parameters generated in Step-1 or not, use the following command:-

```
./aass_ibe_verifykey ibeparams.bin private_key.bin soumyadev@iiita.ac.in
```

*** END ***