1. **upload the aes tool to linux server.**
2. **Demand for encryption**

./aes plaintFile cipherFile key –e

**Demand for decryption**

./aes plaintFile cipherFile key –d

1. **Encrypt files**

the MAC CFG file could be (mac address).cfg,and the names of the Common CFG file for

R1 is ‘a000000000001.cfg’

R2 is ‘a000000000002.cfg’

R3 is ‘a000000000003.cfg’

R4 is ‘a000000000004.cfg’

A1x is ‘a000000000010.cfg’

A2x is ‘a000000000020.cfg’

A41 is ‘a000000000041.cfg’

A48 is ‘a000000000040.cfg’

A68 is ‘a000000000060.cfg’

For example ,encryt 808287032910.cfg and a00000000002.cfg, the key will be 123456789.

./aes 08287032910.cfg 08287032910-e.cfg 123456789 –e

./aes a00000000002.cfg a00000000002-e.cfg 123456789 –e

(08287032910-e.cfg and a00000000002-e.cfg are encrypted files, you could delete 08287032910.cfg and a00000000002.cfg ,then rename the 08287032910-e.cfg and a00000000002-e.cfg to be 08287032910.cfg and a00000000002.cfg)

1. **Decrypt files**

808287032910.cfg and a00000000002.cfg have been encrypted

./aes 08287032910-d.cfg 08287032910.cfg 123456789 –d

./aes a00000000002-d.cfg a00000000002.cfg 123456789 –d

(08287032910-d.cfg and a00000000002-d.cfg are decryted files,you could you could delete 08287032910.cfg and a00000000002.cfg ,then rename the 08287032910-d.cfg and a00000000002-d.cfg to be 08287032910.cfg and a00000000002.cfg)