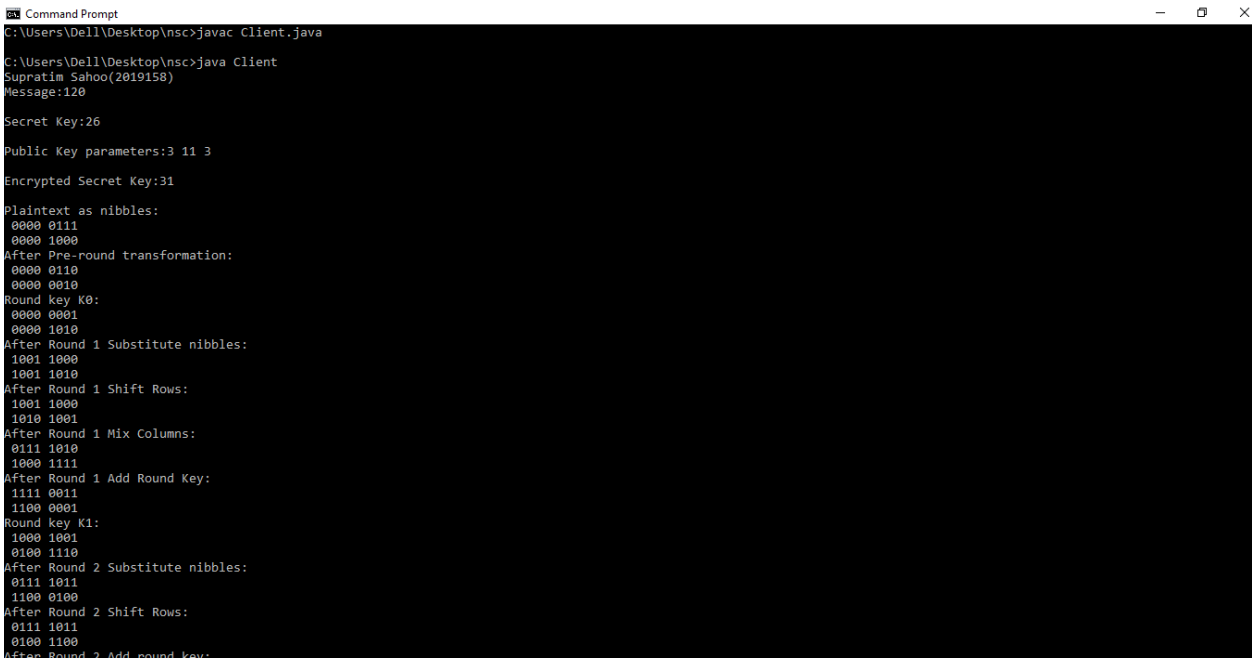
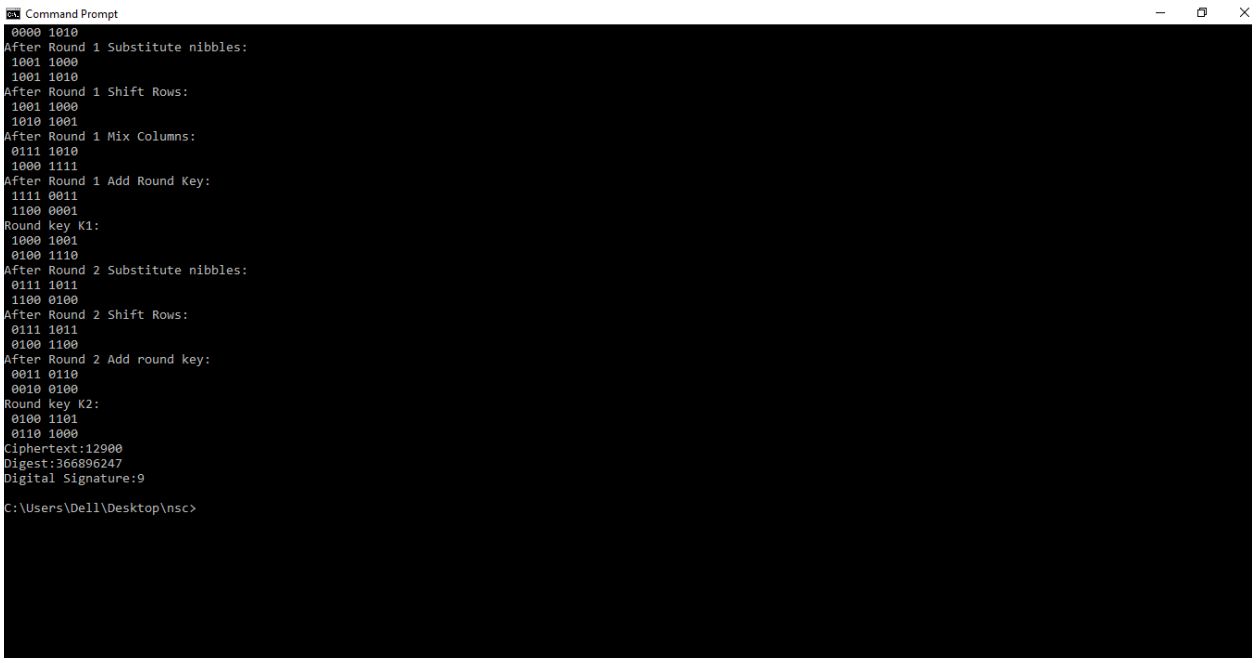
OUTPUT FILE

Client Side:





Server Side:


Command Prompt - java Server
Supratim Sahoo(2019158)
Public key parameters:5 7 11
Decrypted Secret Key:26
Ciphertext nibbles:
0011 0110
0010 0100
After Pre-round transformation:
0111 1011
0100 1100
Round key K2:
0100 1101
0110 1000
After Round 1 InvShift rows:
0111 1011
1100 0100
After Round 1 InvSubstitute nibbles:
1111 0011
1100 0001
After Round 1 InvAdd round key:
0111 1010
1000 1111
Round key K1:
1000 1001
0100 1110
After Round 1 InvMix columns:
1001 1000
1010 1001
After Round 2 InvShift rows:
1001 1000
1001 1010
After Round 2 InvSubstitute nibbles:
0000 0110
0000 0010
After Round 2 Add round key:
0000 0111
0000 1000
Round Key K0:
0000 0001
0000 1010
Decrypted Plaintext:120
Message Digest:366896247
Intermediate verification code:3