Known Plaintext Attack (KPA) -

Output for KPA.java :

```
xuan
ThiJd<!RZyeQjz,05F$K@wB@d^%*2,UqJ
'>;PD#V/]5-rgwvOTBs!!@q7s$t_Dy`Pw(O+<V%X:t_bk2YBm*1M'[1R3^$e'}B%I'_$]^/a--~FWp
aberdeen
Th6r*tzu[A2%bX_[:6:Gn58;(=/wm/Z/=V;I□T,RwD<;jN<xmzfz4KcvKYtYe(vkNjX,Xc.D.Ug^6f'eo|9G
VcM%`]t&aw|5kS7;'}CK3?"gK C=
3ip76k2
Th'□28d\aL\>w2)DK\*a(}ybcj1\sO?DjxsVH$>B\R`$Kc+k&pj=w86qI*33YG8sH:<C$4eD"Xje3AS0□
KO□'P;?,P~OhIOvC:x~M,A,6"HR.{Y;
mocha
This is the plaintext (task 1) for you Akash Ananda Kumar with the ID number = 27681463932 to
decode. Good luck!
```

KEY : mocha

DECODED MESSAGE: This is the plaintext (task 1) for you Akash Ananda Kumar with the ID number = 27681463932 to decode. Good luck!

The code checks using the given first two characters to find the key and plaintext. Here, I have used a while loop to check each word in the passwords and first two characters and decrypting the cipher text using the encdec() method to find the possible key and plaintext. Such an encdec() method in the rotor96crypto file uses substitution cipher technique.

Ciphertext Only Attack (COA) -

Output for COA.java :

```
keith1
This is the second task (Ciphertext Only Attack) of the assignment of the Cryptography and
Secure Development course. Akash Ananda Kumar - you are expected to decode it with the
assumption that this plaintext is English sentences. This plaintext contains this random number
8097 so that you cannot guess it from the others :) Finger-crossed
```

KEY: keith1

DECODED MESSAGE: This is the second task (Ciphertext Only Attack) of the assignment of the Cryptography and Secure Development course. Akash Ananda Kumar - you are expected to decode it with the assumption that this plaintext is English sentences. This plaintext contains this random number 8097 so that you cannot guess it from the others :) Finger-crossed

In this code, I used the regex pattern condition to find the possible key and plaintext using the given ciphertext and all other possible keys in the password file.

And for the experiment result, total ciphertext letters needed to decode the message:

$N = \log_2(K)$, where k is the total number of possible keys

So, $K = 10000$

$N = \log_2(10000)$

$N = 13.29$

So, here are approximately 14 ciphertext letters needed to decode the message.

And, Unicity distance :

$H(k)/D = \log_2(9473)/3.2$

$= 4.13$