FCC200 Report
Affine Cipher and S-DES Implementation

Connor Beardsmore - 15504319

Curtin University
Science and Engineering
Perth, Australia
April 2017

Affine Cipher

Compute Eligible Keys

There are two keys required, a and b. The first is required to be *coprime* with the length of the alphabet, in this scenario *26*. The second key representing the linear shift must be both positive and less than the length of the alphabet.

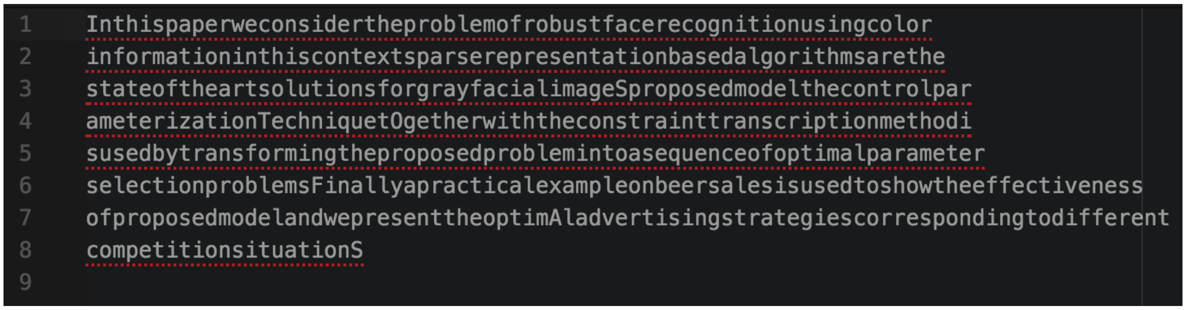
???

There are a total of 12 possible a values that are coprime with *26*. Each of these values can have a shift value (b) of 0 to 25. Thus, the total number of eligible keys is:

$$12 * 26 = 312$$

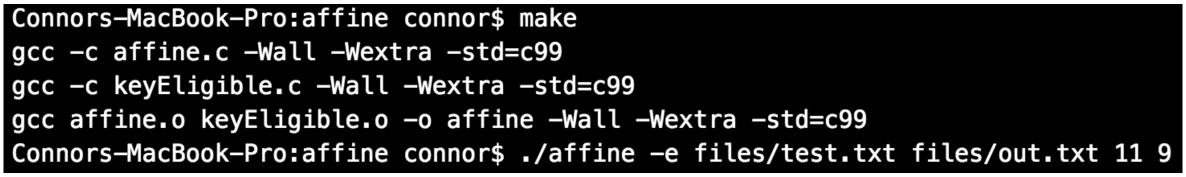
Of these, 26 keys are trivial Caesar ciphers and 286 are non-trivial.

Recovered Plaintext



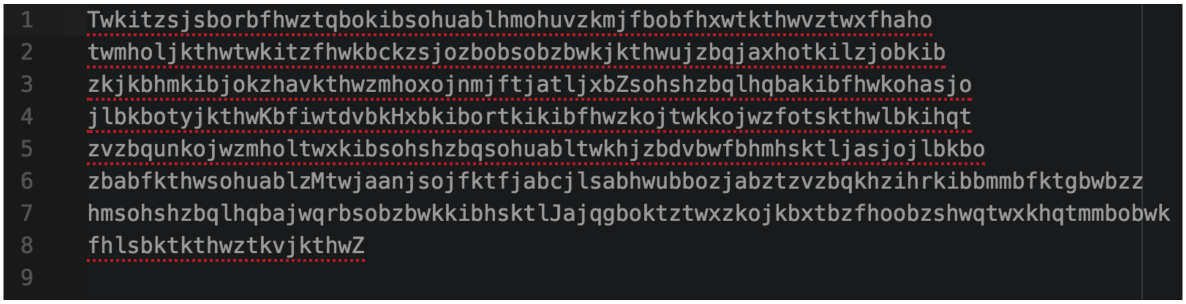
```
Inthispaperweconsidertheproblemofrobustfacerecognitionusingcolor
informationinthiscontextsparserepresentationbasedalgorithmsarethe
stateoftheartsolutionsforgrayfacialimageSproposedmodelthecontrolpar
ameterizationTechniquetOgetherwiththeconstrainttranscriptionmethodi
susedbytransformingtheproposedproblemintoasequenceofoptimalparameter
selectionproblemsFinallyapracticalexampleonbeersalesisusedtoshowtheeffectiveness
ofproposedmodelandwepresenttheoptimAladvertisingstrategiescorrespondingtodifferent
competitionsituationS
```

Figure 1: Original Plaintext File



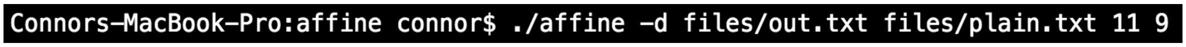
```
Connors-MacBook-Pro:affine connor$ make
gcc -c affine.c -Wall -Wextra -std=c99
gcc -c keyEligible.c -Wall -Wextra -std=c99
gcc affine.o keyEligible.o -o affine -Wall -Wextra -std=c99
Connors-MacBook-Pro:affine connor$ ./affine -e files/test.txt files/out.txt 11 9
```

Figure 2: Encryption Process



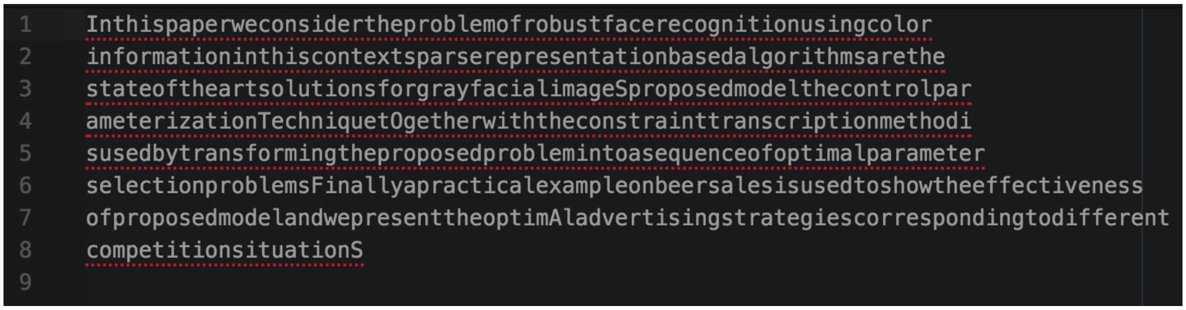
```
Twkitzsjsborbfhwztqbokibsohuablhmohuvzkmjfbobfhxwtkthwvztwxfhaho
twmholjkthwtwkitzfhwkbckzsjozbobsobzbwkjkthwujzbqjaxhotkilzjobkib
zkjkbhmkibjokzhavkthwzmhoxojnmjftjatljxbZsohshzbqlhqbakibfhwkohasjo
jlbkbotyjkthwKbfiwtdvbkHxbkibortkikibfhwzkojtwkkojwzfotskthwlbkihqt
zvzbqunkojwzmholtwxkibsohshzbqsohuabltwkhjzbdvbwfbhmhsktljasjojlbkbo
zbabfkthwsohuablzMtwjaanjsojfktfjabcjlsabhwubbozjabztzvzbqkhzihrkibbmmbfktgbwbzz
hmsohshzbqlhqbajwqrbsobzbwkkibhsktlJajqgboktztwxzkojkbxtbzfhoobzshwqtwxkhqtmmbobwk
fhlsbktkthwztkvjkthwZ
```

Figure 3: Encrypted Ciphertext File



```
Connors-MacBook-Pro:affine connor$ ./affine -d files/out.txt files/plain.txt 11 9
```

Figure 4: Decryption Process



```
Inthispaperweconsidertheproblemofrobustfacerecognitionusingcolor
informationinthiscontextsparserepresentationbasedalgorithmsarethe
stateoftheartsolutionsforgrayfacialimageSproposedmodelthecontrolpar
ameterizationTechniquetOgetherwiththeconstrainttranscriptionmethodi
susedbytransformingtheproposedproblemintoasequenceofoptimalparameter
selectionproblemsFinallyapracticalexampleonbeersalesisusedtoshowtheeffectiveness
ofproposedmodelandwepresenttheoptimAladvertisingstrategiescorrespondingtodifferent
competitionsituationS
```

Figure 5: Recovered Plaintext file

Affine Mathematical Proof

The encryption and decryption functions for the affine cipher are as follows:

$$E(x) = (ax + b)\ mod\ m$$

$$D(x) = a^{-1}(x - b)\ mod\ m$$

Letter Distribution

For the given test file shown in Figure 1, Figure 6 illustrates the letter distributions plotted via GNUPlot.

S-DES

S-DES Mathematical Proof

hello

Pseudo Code Structure

hello

Encrypted Test File

hello

Decrypted Test File

hello

Utilization of an all 1 Key

hello

Modify S-Boxes

hello

Follow up Questions

Threats

hello

Source Coding

hello

Error Coding

hello

S-DES Coding

hello

S-DES Confusion and Diffusion

hello