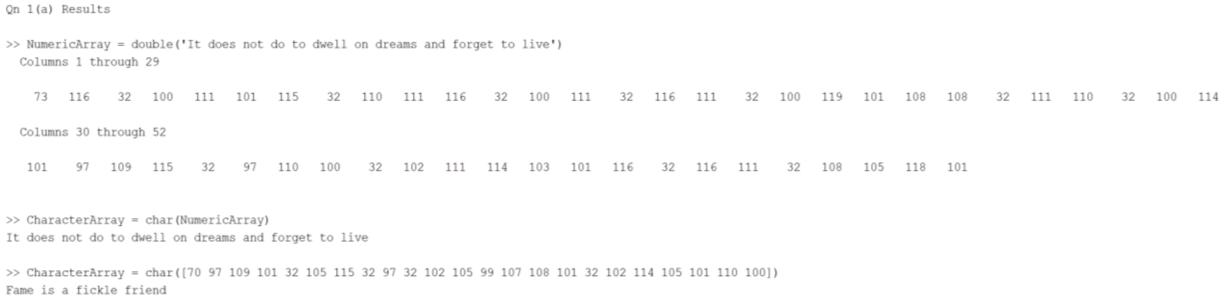
EE3731C CA2 Assignment Report

Name: Just some NUS student **Matric No.:** A1234567Q

Qn 1

1 (a)

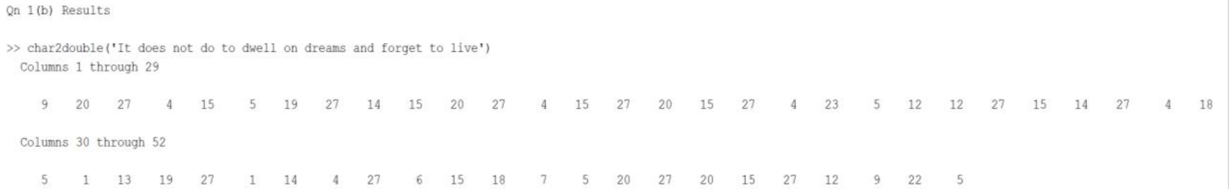
Results



```
Qn 1(a) Results

>> NumericArray = double('It does not do to dwell on dreams and forget to live')
  Columns 1 through 29

    73   116    32   100   111   101   115    32   110   111   116    32   100   111    32   116   111    32   100   119   101   108   108    32   111   110    32   100   114

  Columns 30 through 52

   101    97   109   115    32    97   110   100    32   102   111   114   103   101   116    32   116   111    32   108   105   118   101


>> CharacterArray = char(NumericArray)
It does not do to dwell on dreams and forget to live

>> CharacterArray = char([70 97 109 101 32 105 115 32 97 32 102 105 99 107 108 101 32 102 114 105 101 110 100])
Fame is a fickle friend
```

1 (b)

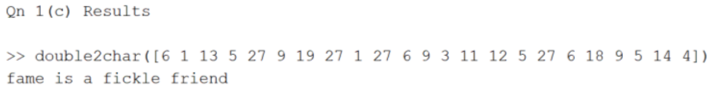
Results



```
Qn 1(b) Results

>> char2double('It does not do to dwell on dreams and forget to live')
  Columns 1 through 29

     9    20    27     4    15     5    19    27    14    15    20    27     4    15    27    20    15    27     4    23     5    12    12    27    15    14    27     4    18

  Columns 30 through 52

     5     1    13    19    27     1    14     4    27     6    15    18     7     5    20    27    20    15    27    12     9    22     5
```

1 (c) Results

Results

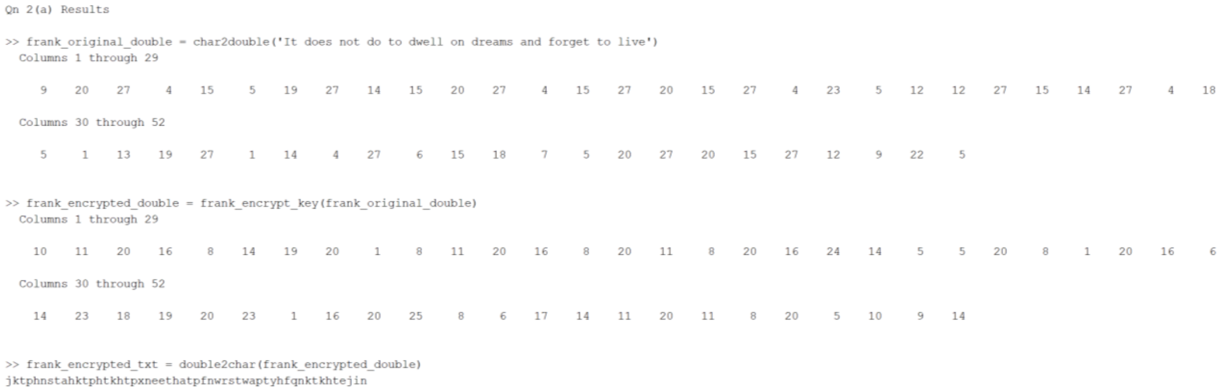


```
Qn 1(c) Results

>> double2char([6 1 13 5 27 9 19 27 1 27 6 9 3 11 12 5 27 6 18 9 5 14 4])
fame is a fickle friend
```

Qn 2

2 (a)

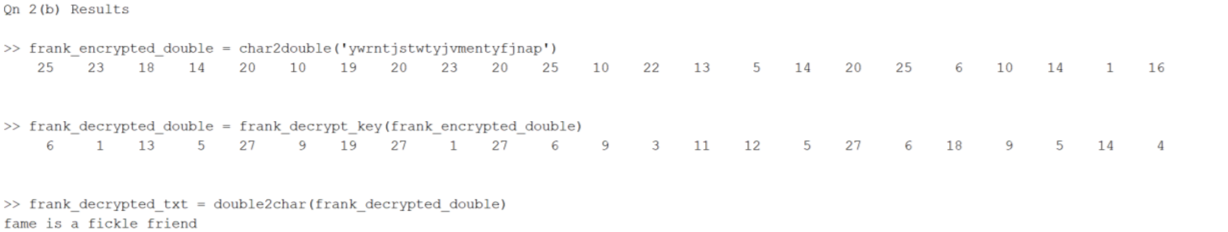
Results



```
Qn 2(a) Results

>> frank_original_double = char2double('It does not do to dwell on dreams and forget to live')
  Columns 1 through 29

     9    20    27     4    15     5    19    27    14    15    20    27     4    15    27    20    15    27     4    23     5    12    12    27    15    14    27     4    18

  Columns 30 through 52

     5     1    13    19    27     1    14     4    27     6    15    18     7     5    20    27    20    15    27    12     9    22     5


>> frank_encrypted_double = frank_encrypt_key(frank_original_double)
  Columns 1 through 29

    10    11    20    16     8    14    19    20     1     8    11    20    16     8    20    11     8    20    16    24    14     5     5    20     8     1    20    16     6

  Columns 30 through 52

    14    23    18    19    20    23     1    16    20    25     8     6    17    14    11    20    11     8    20     5    10     9    14


>> frank_encrypted_txt = double2char(frank_encrypted_double)
jktphnstahktphtkhtpxneethatpfnwrstwaptyhfqnktkhtejin
```

2 (b)

Results

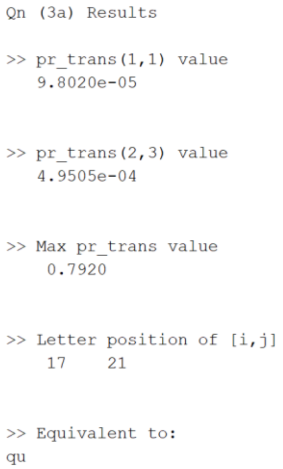


```
Qn 2(b) Results

>> frank_encrypted_double = char2double('ywrntjstwtyjvmentyfjnap')
    25    23    18    14    20    10    19    20    23    20    25    10    22    13     5    14    20    25     6    10    14     1    16


>> frank_decrypted_double = frank_decrypt_key(frank_encrypted_double)
     6     1    13     5    27     9    19    27     1    27     6     9     3    11    12     5    27     6    18     9     5    14     4


>> frank_decrypted_txt = double2char(frank_decrypted_double)
fame is a fickle friend
```

Qn 3

3 (a)

Results

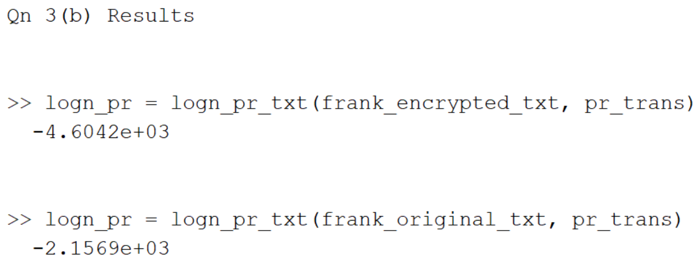


```
Qn (3a) Results

>> pr_trans(1,1) value
   9.8020e-05


>> pr_trans(2,3) value
   4.9505e-04


>> Max pr_trans value
    0.7920


>> Letter position of [i,j]
    17    21


>> Equivalent to:
qu
```

Position i=17, j=21 has highest probability. Since "q" corresponds to position I and "u" corresponds to position j, transitioning from "q" to "u" has the highest transition probability.

3 (b)

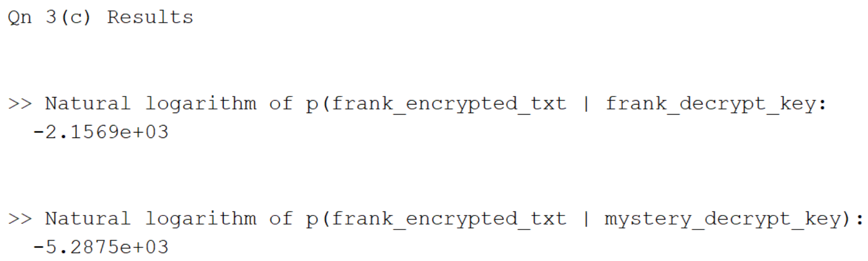
Results



```
Qn 3(b) Results


>> logn_pr = logn_pr_txt(frank_encrypted_txt, pr_trans)
  -4.6042e+03


>> logn_pr = logn_pr_txt(frank_original_txt, pr_trans)
  -2.1569e+03
```

3 (c)

Results

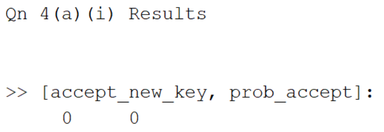


```
Qn 3(c) Results


>> Natural logarithm of p(frank_encrypted_txt | frank_decrypt_key:
  -2.1569e+03


>> Natural logarithm of p(frank_encrypted_txt | mystery_decrypt_key):
  -5.2875e+03
```

Qn 4

4 (a)(i)

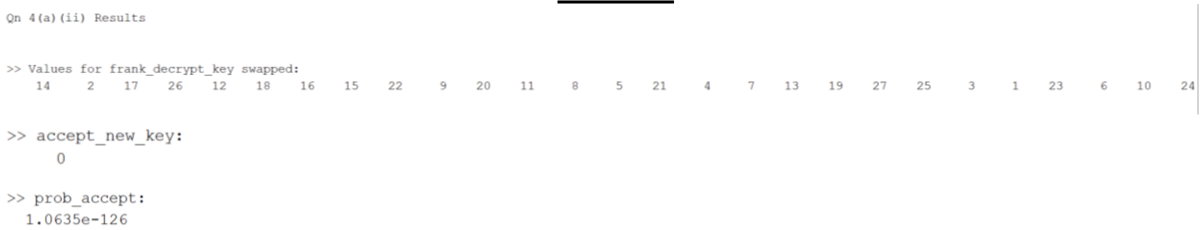
Results



```
Qn 4(a)(i) Results


>> [accept_new_key, prob_accept]:
     0      0
```

4 (a)(ii)

Results

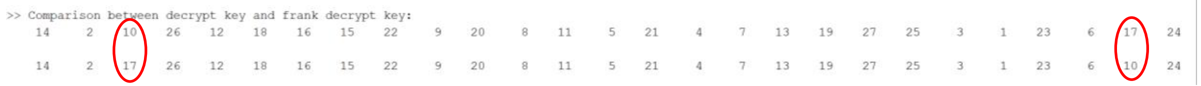


```
Qn 4(a)(ii) Results


>> Values for frank_decrypt_key swapped:
    14     2    17    26    12    18    16    15    22     9    20    11     8     5    21     4     7    13    19    27    25     3     1    23     6    10    24

>> accept_new_key:
     0

>> prob_accept:
  1.0635e-126
```

4 (b)

Results

```
Run 15000: log probability = -2161.1152
```



```
>> Comparison between decrypt key and frank decrypt key:
    14     2    10    26    12    18    16    15    22     9    20     8    11     5    21     4     7    13    19    27    25     3     1    23     6    17    24

    14     2    17    26    12    18    16    15    22     9    20     8    11     5    21     4     7    13    19    27    25     3     1    23     6    10    24
```

Decrypted	Original
morning dawned before i arrived at the village of chamounix i took no rest but returned immediately to geneva even in my own heart i could give no expression to my sensations they weighed on me with a mountain s weight and their excess destroyed my agony beneath them thus i returned home and entering the house presented myself to the family my haggard and wild appearance awoke intense alarm but i answered no juestion scarcely did i speak i felt as if i were placed under a ban as if i had no right to claim their sympathies as if never more might i enqoy companionship with them yet even thus i loved them to adoration and to save them i resolved to dedicate myself to my most abhorred task the prospect of such an occupation made every other circumstance of existence pass before me like a dream and that thought only had to me the reality of life	morning dawned before i arrived at the village of chamounix i took no rest but returned immediately to geneva even in my own heart i could give no expression to my sensations they weighed on me with a mountain s weight and their excess destroyed my agony beneath them thus i returned home and entering the house presented myself to the family my haggard and wild appearance awoke intense alarm but i answered no question scarcely did i speak i felt as if i were placed under a ban as if i had no right to claim their sympathies as if never more might i enjoy companionship with them yet even thus i loved them to adoration and to save them i resolved to dedicate myself to my most abhorred task the prospect of such an occupation made every other circumstance of existence pass before me like a dream and that thought only had to me the reality of life

Remarks

How are the keys different?

- Above is the decrypted text and original text as compared side by side. The letters highlighted in orange and green shows the wrong and right values.

How does the differences show up in the final decrypted text?

Column	Wrong word	Correct word
Column 3 (circled above)	“juestion”	“question”
Column 26 (circled above)	“enqoy”	“enjoy”

Explain why the algorithm does not give exactly the correct answer?

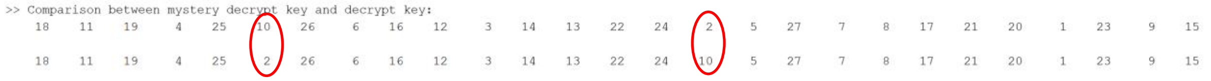
- This is likely because acceptance of the new key is dependent on the new log values and current log values from the function log_pr().
- It depends on the training_txt used because different training texts yield different results for pr_trans.

- This training text already gives a sufficiently accurate result based on the decrypted result. However, evidently the results are still not 100% accurate. This shows that the training text may not be the best representation of the alphabets.

4 (c)

Results

```
Run 15000: log probability = -1204.8648
```



```
>> Comparison between mystery decrypt key and decrypt key:
    18    11    19     4    25    10    26     6    16    12     3    14    13    22    24     2     5    27     7     8    17    21    20     1    23     9    15

    18    11    19     4    25     2    26     6    16    12     3    14    13    22    24    10     5    27     7     8    17    21    20     1    23     9    15
```

Mystery Decrypted text

when we got to the house the street in front of it was packed and the three girls was standing in the door mary bane was red headed jut that don t make no difference she was most awful jeautiful and her face and her eyes was all lit up like glory she was so glad her uncles was come the king he spread his arms and mary bane she bumped for them and the hare lip bumped for the duke and there they had it everyjody most leastways women cried for boy to see them meet again at last and have such good times

Remarks

How are the keys different?

- If we compare decrypt key and mystery key as shown above (circled in red), column 6 and column 16 are swapped respectively.
- If we infer based on the mystery decrypted text, it seems like ‘b’ and ‘j’ are swapped.

How does the differences show up in the final decrypted text?

Letter Affected	Words Affected by	“Correct Answer”
“b” (highlighted in orange)	**“bane”**	**“jane”**
	“bumped”	**“jumped”**
	“boy”	**“joy”**
“j” (highlighted in yellow)	**“jut”**	**“but”**
	“jeautiful”	**“beautiful”**
	“everyjody”	**“everybody”**

Explain why the algorithm does not give exactly the correct answer?

- This has a similar situation as qn 4(b) where the new key is dependent on the new log values and current log values from the function log_pr().
- As mentioned under Remarks of qn 4(b), the training text might not have the most sufficient information for pr_trans which is a variable affecting the actual outcome.

Qn 5

Suggestions for improvements

1) Modifying rand(1)

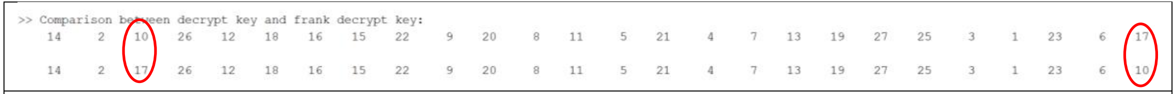
- To ensure everyone's code behaves the same way, rand(1) is used to accept the decrypt key. rand(1) means that $0 \leq rand(1) \leq 1$ which is can possibly increase the chance of accepting an incorrect decrypt_key which is evident some inaccuracies as shown above.

2) Training Text

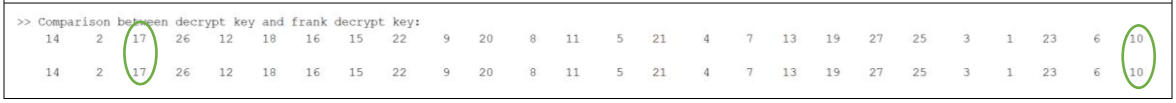
- **Increasing Statistical Accuracy of training text**
  The characters used in training_txt could possibly be modified to give a better representation of pr_trans.
- **Increasing characters in training text**
  An example snippet of a training text is shown. Apostrophe is not included in the training text. If miscellaneous characters like numbers and apostrophe is included in the training text, we could possibly improve the algorithm to fit more characters. We will then not be limited by the accuracy of training text

Example snippet from training text
`he drew near his mother s bedside  and inquired       mother   isn t there something you want me to do`

3) Comment/Remove `rng(9, 'twister')`



```
>> Comparison between decrypt key and frank decrypt key:
    14     2    10    26    12    18    16    15    22     9    20     8    11     5    21     4     7    13    19    27    25     3     1    23     6    17

    14     2    17    26    12    18    16    15    22     9    20     8    11     5    21     4     7    13    19    27    25     3     1    23     6    10
```



```
>> Comparison between decrypt key and frank decrypt key:
    14     2    17    26    12    18    16    15    22     9    20     8    11     5    21     4     7    13    19    27    25     3     1    23     6    10

    14     2    17    26    12    18    16    15    22     9    20     8    11     5    21     4     7    13    19    27    25     3     1    23     6    10
```

- We can evidently see that the decrypt key in 4(b) is corrected once we remove `rng(9, 'twister')`. *However, I will still uncomment it to ensure easier marking*
- What happens if we remove this line?
  More samples will be generated, and we can generate a more accurate decrypt key as shown evidently above.