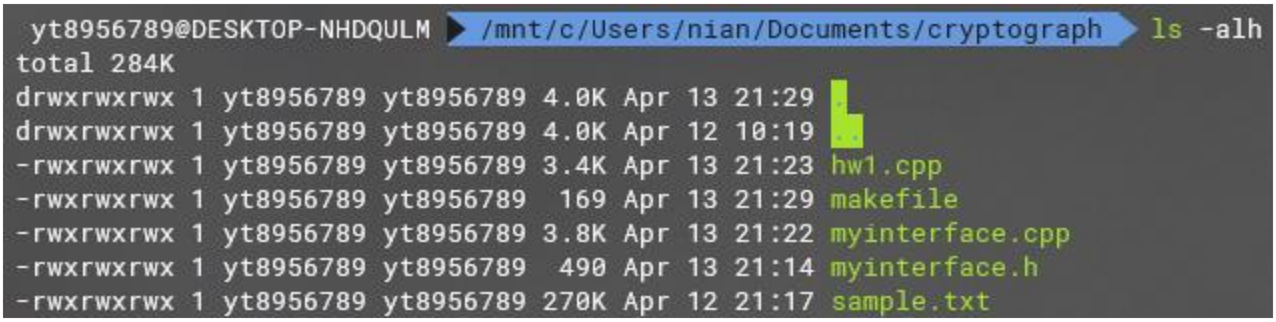
Cryptography and Security Protocols

Homework 1

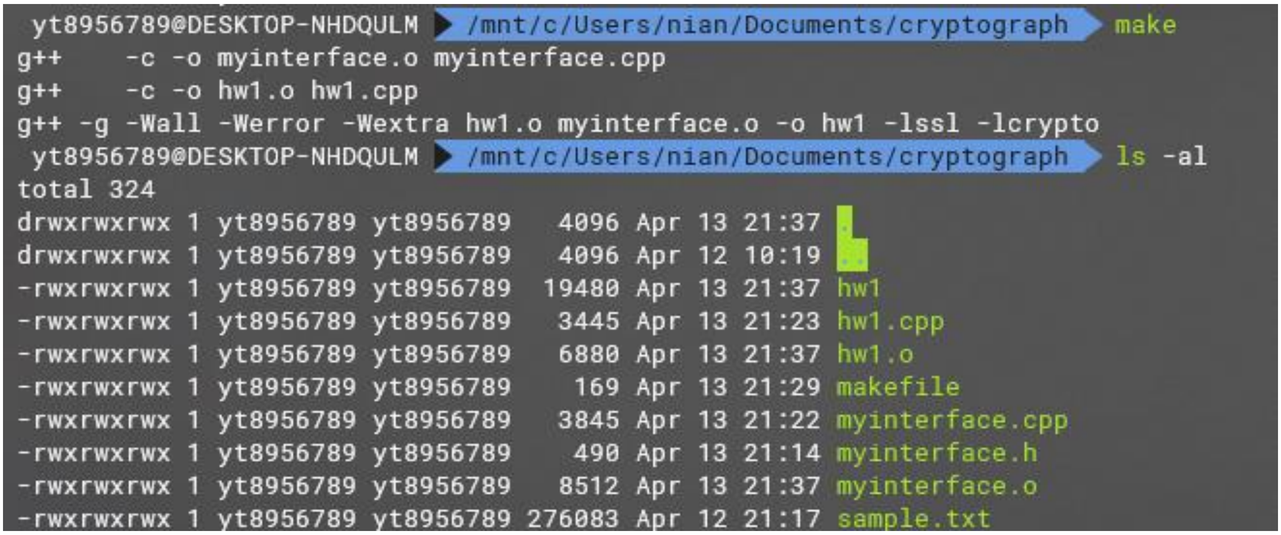
資工四 毛胤年 405410010

- 壓縮檔會有以下程式碼以及demo文檔sample.txt



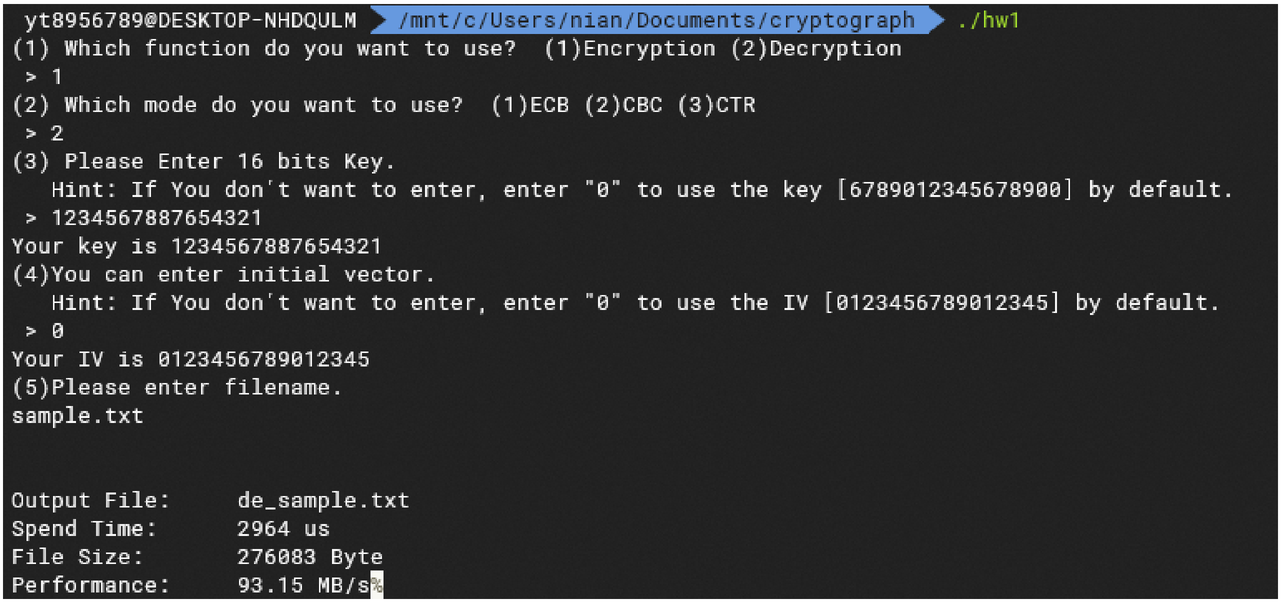
```
 yt8956789@DESKTOP-NHDQULM  /mnt/c/Users/nian/Documents/cryptograph  ls -alh
total 284K
drwxrwxrwx 1 yt8956789 yt8956789 4.0K Apr 13 21:29 .
drwxrwxrwx 1 yt8956789 yt8956789 4.0K Apr 12 10:19 ..
-rwxrwxrwx 1 yt8956789 yt8956789 3.4K Apr 13 21:23 hw1.cpp
-rwxrwxrwx 1 yt8956789 yt8956789  169 Apr 13 21:29 makefile
-rwxrwxrwx 1 yt8956789 yt8956789 3.8K Apr 13 21:22 myinterface.cpp
-rwxrwxrwx 1 yt8956789 yt8956789  490 Apr 13 21:14 myinterface.h
-rwxrwxrwx 1 yt8956789 yt8956789 270K Apr 12 21:17 sample.txt
```

- 使用make編譯主程式，產生執行檔hw1



```
 yt8956789@DESKTOP-NHDQULM  /mnt/c/Users/nian/Documents/cryptograph  make
g++    -c -o myinterface.o myinterface.cpp
g++    -c -o hw1.o hw1.cpp
g++ -g -Wall -Werror -Wextra hw1.o myinterface.o -o hw1 -lssl -lcrypto
 yt8956789@DESKTOP-NHDQULM  /mnt/c/Users/nian/Documents/cryptograph  ls -al
total 324
drwxrwxrwx 1 yt8956789 yt8956789   4096 Apr 13 21:37 .
drwxrwxrwx 1 yt8956789 yt8956789   4096 Apr 12 10:19 ..
-rwxrwxrwx 1 yt8956789 yt8956789  19480 Apr 13 21:37 hw1
-rwxrwxrwx 1 yt8956789 yt8956789   3445 Apr 13 21:23 hw1.cpp
-rwxrwxrwx 1 yt8956789 yt8956789   6880 Apr 13 21:37 hw1.o
-rwxrwxrwx 1 yt8956789 yt8956789    169 Apr 13 21:29 makefile
-rwxrwxrwx 1 yt8956789 yt8956789   3845 Apr 13 21:22 myinterface.cpp
-rwxrwxrwx 1 yt8956789 yt8956789    490 Apr 13 21:14 myinterface.h
-rwxrwxrwx 1 yt8956789 yt8956789   8512 Apr 13 21:37 myinterface.o
-rwxrwxrwx 1 yt8956789 yt8956789 276083 Apr 12 21:17 sample.txt
```

- 執行程式後會詢問加解密、模式、key、IV以及欲處理的檔案名稱

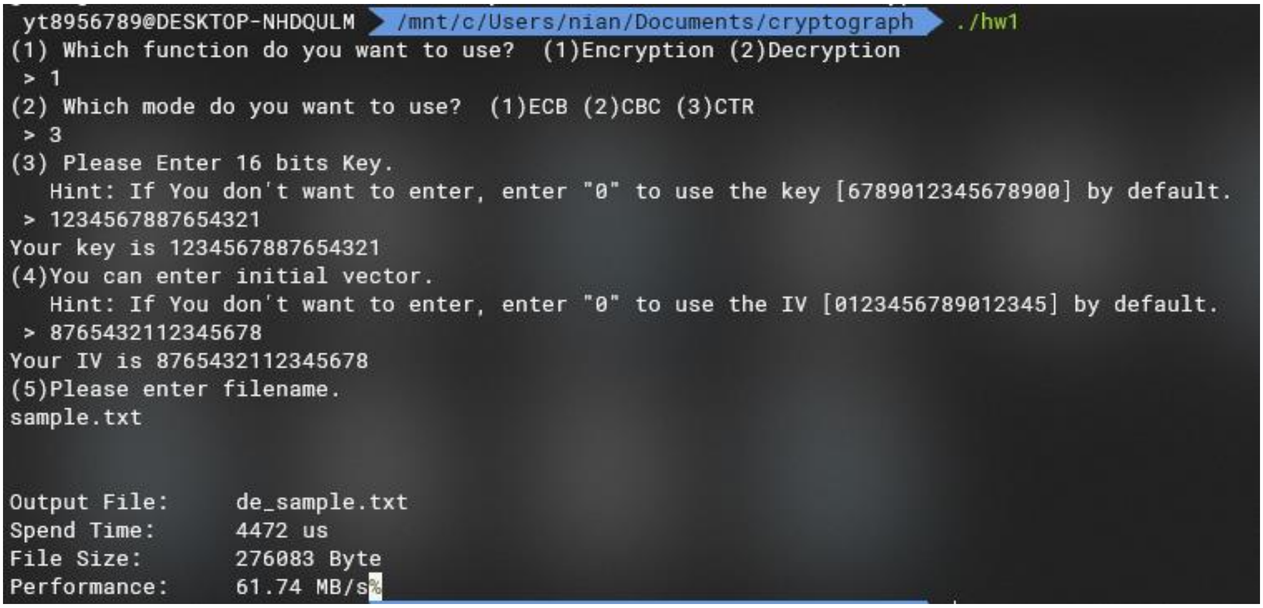


```
 yt8956789@DESKTOP-NHDQULM  /mnt/c/Users/nian/Documents/cryptograph  ./hw1
(1) Which function do you want to use?  (1)Encryption (2)Decryption
 > 1
(2) Which mode do you want to use?  (1)ECB (2)CBC (3)CTR
 > 2
(3) Please Enter 16 bits Key.
   Hint: If You don't want to enter, enter "0" to use the key [6789012345678900] by default.
 > 1234567887654321
Your key is 1234567887654321
(4)You can enter initial vector.
   Hint: If You don't want to enter, enter "0" to use the IV [0123456789012345] by default.
 > 0
Your IV is 0123456789012345
(5)Please enter filename.
sample.txt


Output File:     de_sample.txt
Spend Time:      2964 us
File Size:       276083 Byte
Performance:     93.15 MB/s%
```

- 加解密完成後，會印出輸出檔的名稱和加解密速率

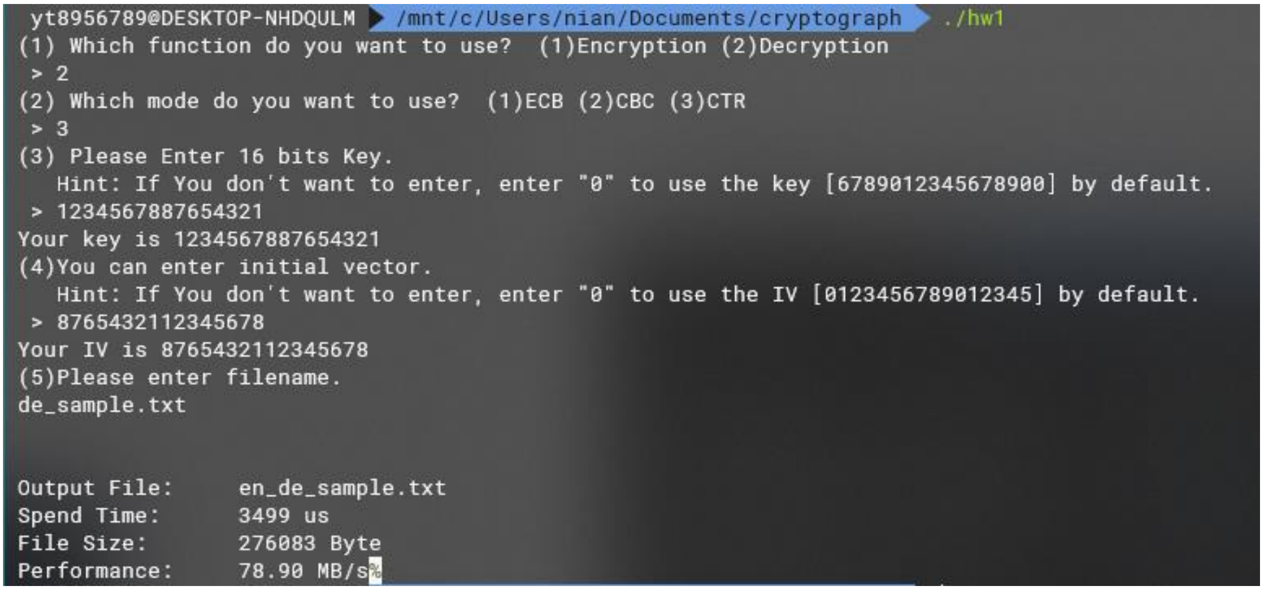
DEMO

- 加密sample.txt後輸出成de_sample.txt

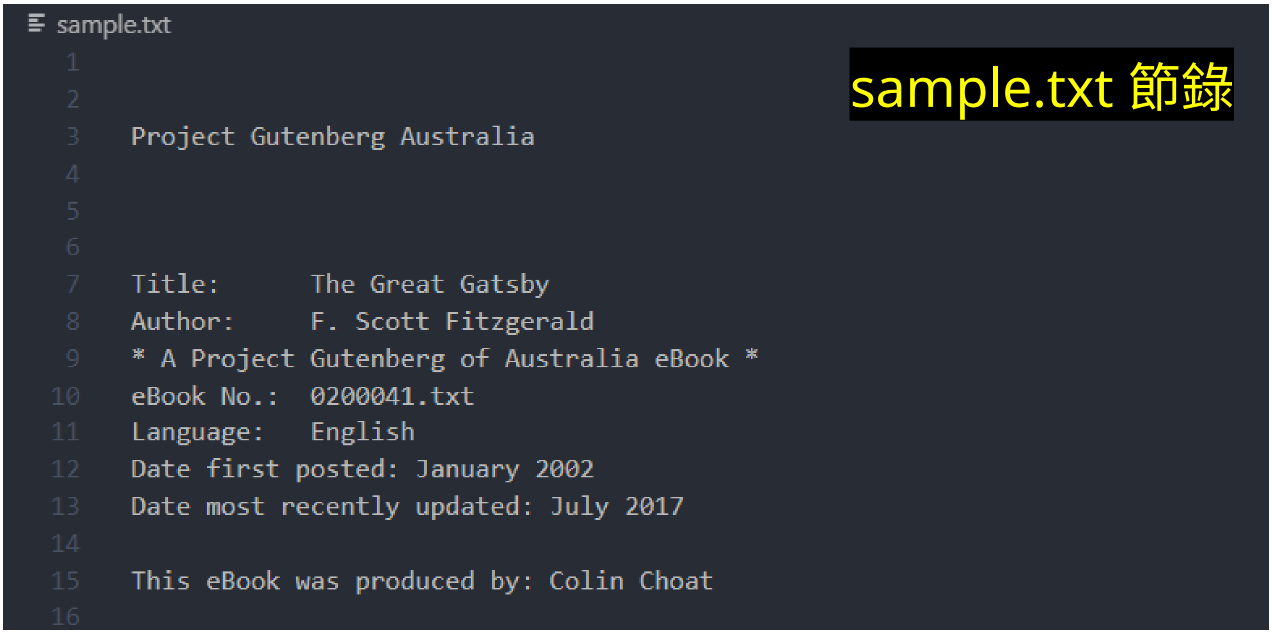


```
 yt8956789@DESKTOP-NHDQULM  /mnt/c/Users/nian/Documents/cryptograph  ./hw1
(1) Which function do you want to use?  (1)Encryption (2)Decryption
 > 1
(2) Which mode do you want to use?  (1)ECB (2)CBC (3)CTR
 > 3
(3) Please Enter 16 bits Key.
   Hint: If You don't want to enter, enter "0" to use the key [6789012345678900] by default.
 > 1234567887654321
Your key is 1234567887654321
(4)You can enter initial vector.
   Hint: If You don't want to enter, enter "0" to use the IV [0123456789012345] by default.
 > 8765432112345678
Your IV is 8765432112345678
(5)Please enter filename.
sample.txt


Output File:     de_sample.txt
Spend Time:      4472 us
File Size:       276083 Byte
Performance:     61.74 MB/s%
```

- 解密de_sample.txt後輸出成en_de_sample.txt



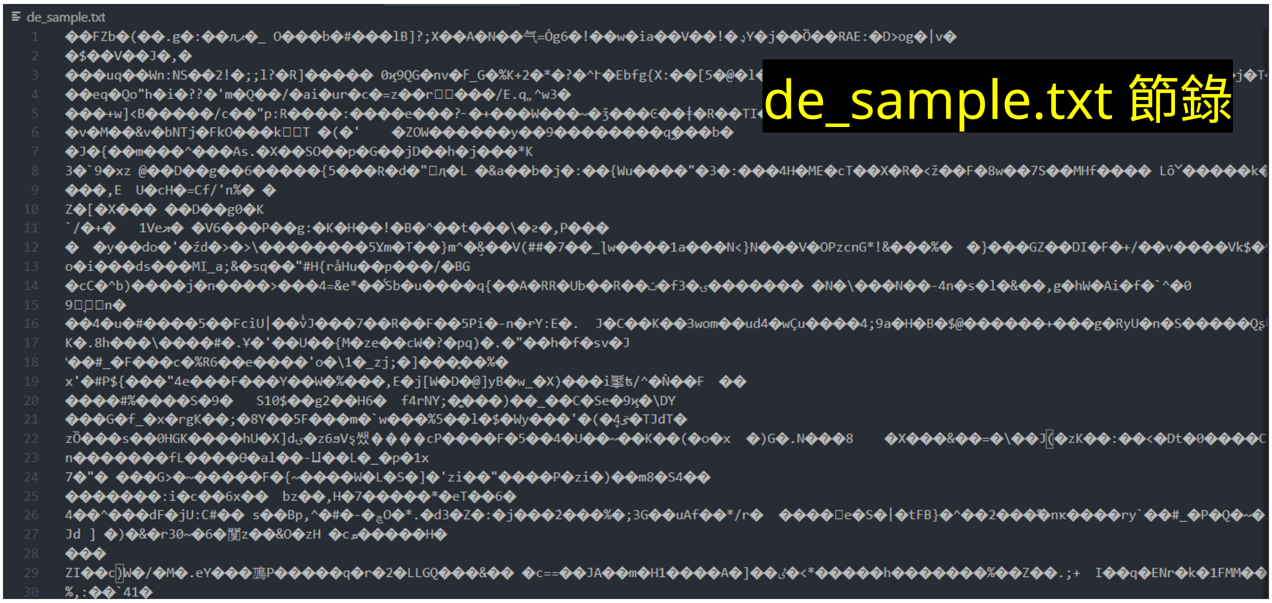
```
 yt8956789@DESKTOP-NHDQULM  /mnt/c/Users/nian/Documents/cryptograph  ./hw1
(1) Which function do you want to use?  (1)Encryption (2)Decryption
 > 2
(2) Which mode do you want to use?  (1)ECB (2)CBC (3)CTR
 > 3
(3) Please Enter 16 bits Key.
   Hint: If You don't want to enter, enter "0" to use the key [6789012345678900] by default.
 > 1234567887654321
Your key is 1234567887654321
(4)You can enter initial vector.
   Hint: If You don't want to enter, enter "0" to use the IV [0123456789012345] by default.
 > 8765432112345678
Your IV is 8765432112345678
(5)Please enter filename.
de_sample.txt


Output File:     en_de_sample.txt
Spend Time:      3499 us
File Size:       276083 Byte
Performance:     78.90 MB/s%
```



sample.txt 節錄

sample.txt

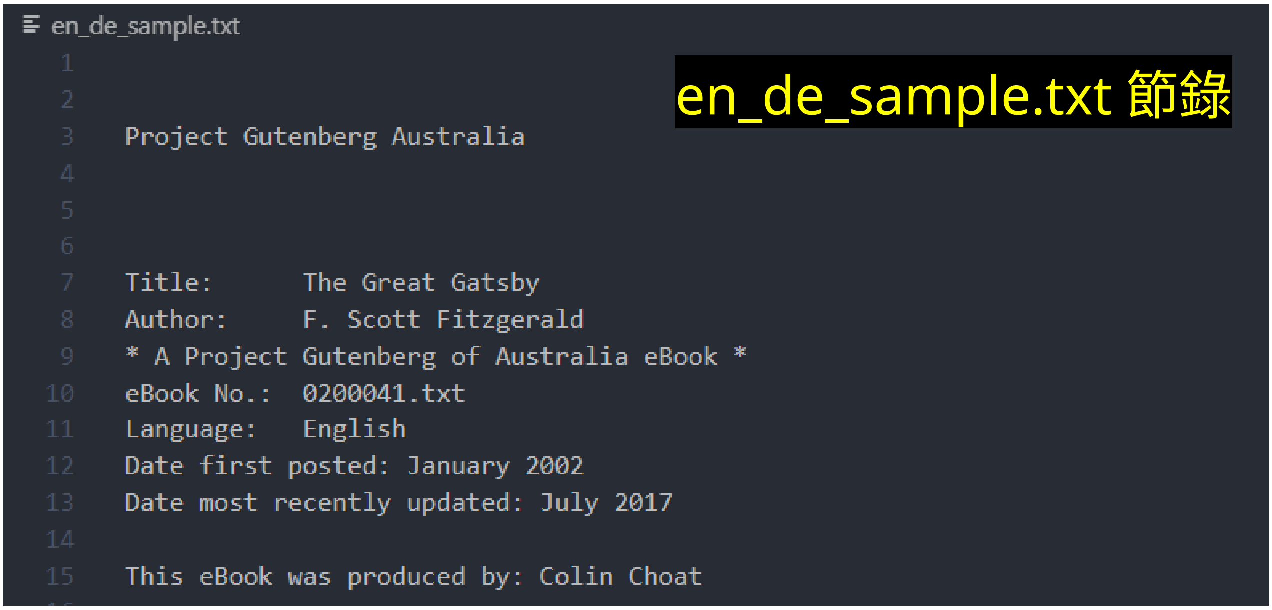
```


Project Gutenberg Australia



Title:       The Great Gatsby
Author:      F. Scott Fitzgerald
* A Project Gutenberg of Australia eBook *
eBook No.:   0200041.txt
Language:    English
Date first posted: January 2002
Date most recently updated: July 2017

This eBook was produced by: Colin Choat

```



de_sample.txt 節錄

de_sample.txt

```
��FZb�(��.g�:��л�_ O���b�#���lB]?;X��A�N��气=Ȯg6�!��w�ia��V��!�ږY�j��Ȍ��RAE:�D>og�|v�
�$��V��J�,�
���uq��Wn:NS��2!�;;l?�R]�����  0ɥ9QG�nv�F_G�%K+2�*�?�^Ͱ�Ebfg{X:��[5�@�l�j�T
��eq�Qo"h�i�??�'m�Q��/�ai�ur�c�=z��r□□���/E.q„^w3�
���+w]<B������/c��"p:R�����:����e����?-�+���W����~�ǯ���Ͼ��ɫ�R��TI
�v�M��&v�bNTj�FkO����k□□T �(�'     �ZOW�������y���9���������q̧���b�
�J�{��m����^���As.�X��SO��p�G��jD��h�j����*K
3�`9�xz @���D���g���6������{5����R�d�"□л�L �&a���b�j�:��{Wu�����"�3�:���4H�ME�cT��X�R�<ž��F�8w��7S��MHf���� Lõ̓������k�
���,E  U�cH�=Cf/'n%� �
Z�[�X��� ��D���g0�K
`/�+�   1Veӂ� �V6����P���g:�K�H��!�B�^���t����\�ƨ�,P����
�  �y���do�'�źd�>�>\����������5Ⅹm�T��}m^�&̦��V(##�7��_lw����1a���N<}N���V�OPzcnG*!&���%�  �}����GZ��DI�F�+/��v�����Vk$�
o�i����ds����MI_a;&�sq��"#H{rǡHu��p����/�BG
�cC�^b)�����ǰ�n�����>����4=&e*��Ƽb�u�����q{��A�RR�Ub��R��ٮ�f3�ى�������� �N�\���N��-4n�s�l�&��,g�hW�Ai�f�`^�0
9□̧□□n�
��4�u�#�����5��FciU|��v̈́J����7��R��F���5Pi�-n�ɼY:E�.  J�C��K��3wom��ud4�wÇu�����4;9a�H�B�$@��������+����g�RyU�n�S������Qş
K�.8h���\�����#�.¥�'��U��{M�ze��cW�?�pq)�.�"��h�f�sv�J
ʿ��#_�F����c�%R6��e�����'o�\1�_zj;�]����̜���%�
x'�#P${����"4e����F����Y��W�%����,E�j[W�D�@]yB�w_�X)����i壂ҍ/^�Ň��F  ��
�����#%������S�9�   S10$��g2��H6�  f4rNY;�̭����)��_��C�Se�9ɥ�\DY
����G�f_�x�rgK��;�8Y��5F����m�`w����%5���l�$�Wy����'�(�4̧ڙ�TJdT�
zȌ̀����s���0HGK�����hU�X]dى�z6ɘVş烞����cP������F�5���4�U���~��K��(�o�x  �)G�.N����8    �X���&��=�\��J(�zK��:��<�Dt�0�����C
n���������fL������0�al��-Ш��L�_�p�1x
7�"� ����G>�~�������F�{~�����W�L�S�]�'zi��"�����P�zi�)��m8�S4��
���������:i�c���6x��  bz��,H�7�������*�eT���6�
4��^����dF�jU:C#��  s���Bp,^�#�-�̯O�*.�d3�Z�:�j����2����%�;3G��uAf��*/r�  ����□e�S�|�tFB}�^��2����nк����ry`��#_�P�Q�~�
Jd ] �)�&�r30~�6�閺z��&O�zH �cꟷ������H�
���
ZI��c)W�/�M�.eY����鳭P������q�r�2�LLGQ����&��  �c==��JA��m�H1�����A�]��ۓ�<*������h���������%��Z��.;+  I��q�ENr�k�1FMM��
%,:��`41�
```



en_de_sample.txt 節錄

en_de_sample.txt

```


Project Gutenberg Australia



Title:       The Great Gatsby
Author:      F. Scott Fitzgerald
* A Project Gutenberg of Australia eBook *
eBook No.:   0200041.txt
Language:    English
Date first posted: January 2002
Date most recently updated: July 2017

This eBook was produced by: Colin Choat
```