

## Appendix B Encryption times for spatial files within DBFS

Table B1 shows encryption (*Enc.*) and decryption (*Dec.*) times of different sizes of spatial files using 256-bit AES encryption (32-character key) using three approaches:

- within ECMSDK using DBMS\_CRYPTO\_TOOLKIT,
- within ECMSDK using OpenSSL encryption tool, and
- within Windows NTFS using OpenSSL encryption tool.

The next three subsections include the encryption-decryption performance results from these approaches.

The first two approaches compare the encryption and decryption performance of files within ECMSDK using (a) the DBMS\_CRYPTO\_TOOLKIT within the Oracle 11g database (implemented in PL/SQL) against (b) the performance provided by the OpenSSL tool (a Windows executable, called externally using PL/SQL from our encryption scripts). The third approach compares the encryption of spatial files using the OpenSSL tool within ECMSDK versus those stored directly on the OS (i.e. Windows NTFS).

In all experiments, the tests were performed on a machine with the following specifications: an Intel 1.6 GHz i5-8265u processor with 8GB RAM on Dell Inspiron system and the software utilized consisted of Oracle 11g Database Release 2, running on Windows 10 Operating System.

GIS File	Filesize (Mb)	AES		OpenSSL on CMSDK		OpenSSL on NTFS	
		Enc.	Dec.	Enc.	Dec.	Enc.	Dec.
france-points.shp	1.50	1.13	1.07	0.48	0.17	0.04	0.04
france-waterways.shp	6.32	4.73	4.49	0.55	0.29	0.06	0.05
france-natural.shp	11.67	8.74	8.30	1.15	0.45	0.11	0.07
indonesia-natural.shp	11.95	8.95	8.50	1.20	0.55	0.07	0.07
germany-points.shp	13.89	10.41	9.88	1.25	0.92	0.07	0.14
britain-waterways.shp	16.12	12.08	11.46	1.93	1.31	0.08	0.09
china-buildings.shp	26.53	19.87	18.87	2.25	1.90	0.12	0.34
india-natural.shp	32.13	24.07	22.85	3.81	2.38	0.13	0.37
china-natural.shp	33.75	25.28	24.00	4.08	2.68	0.14	0.48
india-waterways.shp	36.21	27.13	25.75	4.18	2.77	0.15	0.56

**Table B1:** Comparing three approaches of applying AES encryption and decryption of spatial files<sup>1</sup>.

<sup>1</sup> The ESRI shapefiles used in the investigation are sourced from publicly available datasets (<https://mapcruzin.com/download-free-arcgis-shapefiles.htm>).

## B.1 Within ECMSDK using DBMS\_CRYPTO\_TOOLKIT

Figure B1 shows the encryption and decryption time for spatial files in ECMSDK being computed from within PL/SQL code using SQLplus. One by one, each file's ID is passed to the encryption procedure `encrypt()` along with the encryption key. The time capturing has been coded within PL/SQL code.

To retrieve the file id of a file, the following SQL can be used.

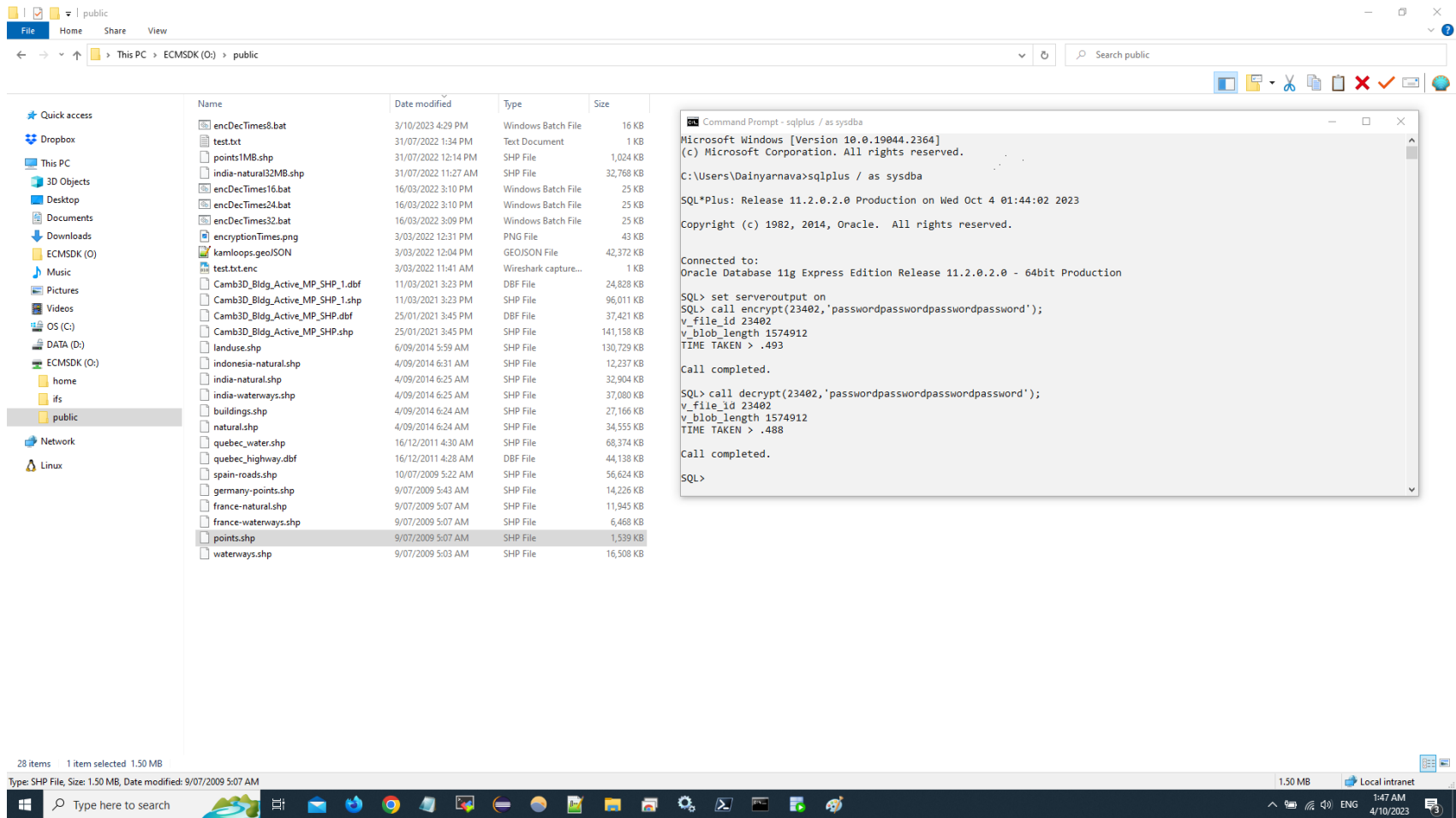
```
SELECT co.content, doc.name
FROM ecmsdk.odmv_document doc, ecmsdk.odm_contentobject co
WHERE doc.name LIKE '%.shp' AND doc.CONTENTOBJECT = co.id;
```

The id of files retrieved using the above query is used as parameter in the encryption and decryption processes:

```
set echo on
set serveroutput on

call encrypt(23402, 'passwordpasswordpasswordpassword');
commit;
call decrypt(23402, 'passwordpasswordpasswordpassword');
commit;
```

This PL/SQL encryption and decryption procedure is available within the “[performanceResults\Approach1\\_WithinECMSDKUsingDBMSCrypto\\_PLSQL](https://github.com/sharmapn/DBFSFileCrypto/)” folder in the GitHub project repository: <https://github.com/sharmapn/DBFSFileCrypto/>



**Figure B1:** Encryption and Decryption time for spatial files in ECMSDK being computed using SQLPlus.

## B.2 Within ECMSDK using OpenSSL Toolkit

Figure B2 shows the encryption and decryption time for spatial files in ECMSDK being computed using the OpenSSL tool. A batch script encrypts and then later decrypts each file one by one for different lengths of the encryption keys. The filename and the encryption key is passed as argument. The time capturing has been coded within the batch script.

Here is one encryption and decryption pair of code:

```
echo "Encryption Time"

set "startTime=%time: =0%"
openssl enc -aes-256-cbc -in O:\public\points.shp -out O:\public\points.shp.enc -k
password -pbkdf2
set "endTime=%time: =0%"
set "end=!endTime:%time:~8,1%=%100)*100+1!" & set
"start=!startTime:%time:~8,1%=%100)*100+1!"
set /A "elap=((10!end:%time:~2,1%=%100)*60+1!%100)-
(((10!start:%time:~2,1%=%100)*60+1!%100), elap==(elap>>31)*24*60*60*100"
set /A
"cc=elap%100+100,elap/=100,ss=elap%60+100,elap/=60,mm=elap%60+100,hh=elap/60+100"
echo points.shp Elapsed:
%hh:~1%%time:~2,1%mm:~1%%time:~2,1%ss:~1%%time:~8,1%cc:~1%;

echo "Decryption Time"

set "startTime=%time: =0%"
openssl enc -d -aes-256-cbc -in O:\public\points.shp.enc -out O:\public\pointsX.shp -k
password -pbkdf2
set "endTime=%time: =0%"
rem Get elapsed time:
set "end=!endTime:%time:~8,1%=%100)*100+1!" & set
"start=!startTime:%time:~8,1%=%100)*100+1!"
set /A "elap=((10!end:%time:~2,1%=%100)*60+1!%100)-
(((10!start:%time:~2,1%=%100)*60+1!%100), elap==(elap>>31)*24*60*60*100"
rem Convert elapsed time to HH:MM:SS:CC format:
set /A
"cc=elap%100+100,elap/=100,ss=elap%60+100,elap/=60,mm=elap%60+100,hh=elap/60+100"
rem echo Start:      %startTime%
rem echo End:        %endTime%
echo points.shp Elapsed:
%hh:~1%%time:~2,1%mm:~1%%time:~2,1%ss:~1%%time:~8,1%cc:~1%
```

The full batch scripts for the encryption and decryption procedures are available within the “[performanceResults/Approach2\\_WithinECMSDKUsingOpenSSL](#)” folder at the GitHub project repository: <https://github.com/sharmapn/DBFSFileCrypto/>

The screenshot shows a Windows File Explorer window with the address bar set to "This PC > ECMSDK (O:) > public". The left sidebar shows the "public" folder selected. The main pane displays a list of files and folders. The "encDecTimes8.bat" file is selected, showing a size of 16 KB and a date modified of 3/10/2023 4:29 PM.

Name	Date modified	Type	Size
india-waterwaysX.shp	3/10/2023 5:19 PM	SHP File	37,080 KB
naturalX.shp	3/10/2023 5:19 PM	SHP File	34,555 KB
india-naturalX.shp	3/10/2023 5:19 PM	SHP File	32,904 KB
buildingsX.shp	3/10/2023 5:19 PM	SHP File	27,166 KB
waterwaysX.shp	3/10/2023 5:19 PM	SHP File	16,508 KB
germany-pointsX.shp	3/10/2023 5:19 PM	SHP File	14,226 KB
indonesia-naturalX.shp	3/10/2023 5:19 PM	SHP File	12,237 KB
france-naturalX.shp	3/10/2023 5:19 PM	SHP File	11,945 KB
france-waterwaysX.shp	3/10/2023 5:19 PM	SHP File	6,468 KB
pointsX.shp	3/10/2023 5:19 PM	SHP File	1,539 KB
india-waterways.shp.enc	3/10/2023 5:19 PM	Wireshark capture...	37,080 KB
natural.shp.enc	3/10/2023 5:18 PM	Wireshark capture...	34,555 KB
india-natural.shp.enc	3/10/2023 5:18 PM	Wireshark capture...	32,904 KB
buildings.shp.enc	3/10/2023 5:18 PM	Wireshark capture...	27,166 KB
waterways.shp.enc	3/10/2023 5:18 PM	Wireshark capture...	16,508 KB
germany-points.shp.enc	3/10/2023 5:18 PM	Wireshark capture...	14,226 KB
indonesia-natural.shp.enc	3/10/2023 5:18 PM	Wireshark capture...	12,237 KB
france-natural.shp.enc	3/10/2023 5:18 PM	Wireshark capture...	11,945 KB
france-waterways.shp.enc	3/10/2023 5:18 PM	Wireshark capture...	6,468 KB
points.shp.enc	3/10/2023 5:18 PM	Wireshark capture...	1,539 KB
encDecTimes8.bat	3/10/2023 4:29 PM	Windows Batch File	16 KB
test.txt	31/07/2022 1:34 PM	Text Document	1 KB
points1MB.shp	31/07/2022 12:14 PM	SHP File	1,024 KB
india-natural32MB.shp	31/07/2022 11:27 AM	SHP File	32,768 KB
encDecTimes16.bat	16/03/2022 3:10 PM	Windows Batch File	25 KB
encDecTimes24.bat	16/03/2022 3:10 PM	Windows Batch File	25 KB
encDecTimes32.bat	16/03/2022 3:09 PM	Windows Batch File	25 KB
encryptionTimes.png	3/03/2022 12:31 PM	PNG File	43 KB
kamloops.geoJSON	3/03/2022 12:04 PM	GEOJSON File	42,372 KB
test.txt.enc	3/03/2022 11:41 AM	Wireshark capture...	1 KB
Camb3D_Bldg_Active_MP_SHP_1.dbf	11/03/2021 3:23 PM	DBF File	24,828 KB
Camb3D_Bldg_Active_MP_SHP_1.shp	11/03/2021 3:23 PM	SHP File	96,011 KB
Camb3D_Bldg_Active_MP_SHP.dbf	25/01/2021 3:45 PM	DBF File	37,421 KB
Camb3D_Bldg_Active_MP_SHP.shp	25/01/2021 3:45 PM	SHP File	141,158 KB
landuse.shp	6/09/2014 5:59 AM	SHP File	130,729 KB
indonesia-natural.shp	4/09/2014 6:31 AM	SHP File	12,237 KB
india-natural.shp	4/09/2014 6:25 AM	SHP File	32,904 KB
india-waterways.shp	4/09/2014 6:25 AM	SHP File	37,080 KB
buildings.shp	4/09/2014 6:24 AM	SHP File	27,166 KB
natural.shp	4/09/2014 6:24 AM	SHP File	34,555 KB

The Command Prompt window shows the output of the "encDecTimes8.bat" script. It displays the encryption and decryption times for various spatial files. The encryption times are as follows:

- points.shp Elapsed: 00:00:00.36
- france-waterways.shp Elapsed: 00:00:00.57
- france-natural.shp Elapsed: 00:00:01.36
- indonesia-natural.shp Elapsed: 00:00:01.09
- germany-points.shp Elapsed: 00:00:01.29
- waterways.shp Elapsed: 00:00:02.08
- buildings.shp Elapsed: 00:00:02.01
- india-natural.shp Elapsed: 00:00:02.58
- natural.shp Elapsed: 00:00:04.85
- india-waterways.shp Elapsed: 00:00:05.68

The decryption times are as follows:

- points.shp Elapsed: 00:00:00.45
- france-waterways.shp Elapsed: 00:00:00.59
- france-natural.shp Elapsed: 00:00:01.91
- indonesia-natural.shp Elapsed: 00:00:01.21
- germany-points.shp Elapsed: 00:00:01.66
- waterways.shp Elapsed: 00:00:01.28
- buildings.shp Elapsed: 00:00:04.65
- india-natural.shp Elapsed: 00:00:02.50
- natural.shp Elapsed: 00:00:01.29
- india-waterways.shp Elapsed: 00:00:02.02

**Figure B2:** Encryption and Decryption time for spatial files in ECMSDK using OpenSSL command line tool.

## B.3 Within NTFS using OpenSSL Toolkit

Figure B3 shows the encryption and decryption time for spatial files in ECMSDK being computed from within PL/SQL code using SQLplus. One by one, each file's ID is passed to the encryption procedure `encrypt()` along with the encryption key. The time capturing has been coded within PL/SQL code.

To retrieve the file id of a file, the following SQL can be used.

```
echo "Encryption Time"

set "startTime=%time: =0%"
openssl enc -aes-256-cbc -in D:\OpenSSLencryptionTimes\points.shp -out
D:\OpenSSLencryptionTimes\points.shp.enc -k password -pbkdf2
set "endTime=%time: =0%"
rem Get elapsed time:
set "end=!endTime:%time:~8,1%=%100)*100+1!" & set
"start=!startTime:%time:~8,1%=%100)*100+1!"
set /A "elap=((10!end:%time:~2,1%=%100)*60+1!%100)-
(((10!start:%time:~2,1%=%100)*60+1!%100), elap==(elap>>31)*24*60*60*100"
rem Convert elapsed time to HH:MM:SS:CC format:
set /A
"cc=elap%100+100,elap/=100,ss=elap%60+100,elap/=60,mm=elap%60+100,hh=elap/60+100"
rem echo Start:      %startTime%
rem echo End:        %endTime%
echo points.shp Elapsed:
%hh:~1%%time:~2,1%%mm:~1%%time:~2,1%%ss:~1%%time:~8,1%%cc:~1%;

echo "Decryption Time"

set "startTime=%time: =0%"
openssl enc -d -aes-256-cbc -in D:\OpenSSLencryptionTimes\points.shp.enc -out
D:\OpenSSLencryptionTimes\pointsX.shp -k password -pbkdf2
set "endTime=%time: =0%"
rem Get elapsed time:
set "end=!endTime:%time:~8,1%=%100)*100+1!" & set
"start=!startTime:%time:~8,1%=%100)*100+1!"
set /A "elap=((10!end:%time:~2,1%=%100)*60+1!%100)-
(((10!start:%time:~2,1%=%100)*60+1!%100), elap==(elap>>31)*24*60*60*100"
rem Convert elapsed time to HH:MM:SS:CC format:
set /A
"cc=elap%100+100,elap/=100,ss=elap%60+100,elap/=60,mm=elap%60+100,hh=elap/60+100"
rem echo Start:      %startTime%
rem echo End:        %endTime%
echo points.shp Elapsed:
%hh:~1%%time:~2,1%%mm:~1%%time:~2,1%%ss:~1%%time:~8,1%%cc:~1%
```

The full batch scripts for the encryption and decryption procedures are available within the “[performanceResults/Approach3\\_WithinNTFSUsingOpenSSL](https://github.com/sharmapn/DBFSFileCrypto/)” folder at the GitHub project repository: <https://github.com/sharmapn/DBFSFileCrypto/>

The screenshot displays a Windows File Explorer window titled 'OpenSSLEncryptionTimes' showing a directory of spatial files and their encrypted versions. The files are organized into two main groups: original spatial files and their encrypted counterparts (encDecTimes8.bat, encDecTimes16.bat, etc.). The Command Prompt window shows the output of the 'encDecTimes8.bat' script, which measures the time taken to encrypt and decrypt various spatial files using OpenSSL.

Name	Date modified	Type	Size
Camb3D_Bldg_Active_MP_SHPX.shp	3/10/2023 4:30 PM	SHP File	141,158 KB
landuseX.shp	3/10/2023 4:30 PM	SHP File	130,729 KB
Camb3D_Bldg_Active_MP_SHP_1X.shp	3/10/2023 4:30 PM	SHP File	96,011 KB
quebec_waterX.shp	3/10/2023 4:30 PM	SHP File	68,374 KB
spain-roadsX.shp	3/10/2023 4:30 PM	SHP File	56,624 KB
india-waterwaysX.shp	3/10/2023 4:30 PM	SHP File	37,080 KB
naturalX.shp	3/10/2023 4:30 PM	SHP File	34,555 KB
buildingsX.shp	3/10/2023 4:30 PM	SHP File	27,166 KB
india-naturalX.shp	3/10/2023 4:30 PM	SHP File	32,904 KB
germany-pointsX.shp	3/10/2023 4:30 PM	SHP File	14,226 KB
indonesia-naturalX.shp	3/10/2023 4:30 PM	SHP File	12,237 KB
waterwaysX.shp	3/10/2023 4:30 PM	SHP File	16,508 KB
france-naturalX.shp	3/10/2023 4:30 PM	SHP File	11,945 KB
Camb3D_Bldg_Active_MP_SHP.shp.enc	3/10/2023 4:30 PM	WireShark capture...	141,158 KB
france-waterwaysX.shp	3/10/2023 4:30 PM	SHP File	6,468 KB
pointsX.shp	3/10/2023 4:30 PM	SHP File	1,539 KB
landuse.shp.enc	3/10/2023 4:30 PM	WireShark capture...	130,729 KB
Camb3D_Bldg_Active_MP_SHP_1.shp.enc	3/10/2023 4:30 PM	WireShark capture...	96,011 KB
quebec_water.shp.enc	3/10/2023 4:30 PM	WireShark capture...	68,374 KB
spain-roads.shp.enc	3/10/2023 4:30 PM	WireShark capture...	56,624 KB
india-waterways.shp.enc	3/10/2023 4:29 PM	WireShark capture...	37,080 KB
natural.shp.enc	3/10/2023 4:29 PM	WireShark capture...	34,555 KB
buildings.shp.enc	3/10/2023 4:29 PM	WireShark capture...	27,166 KB
india-natural.shp.enc	3/10/2023 4:29 PM	WireShark capture...	32,904 KB
waterways.shp.enc	3/10/2023 4:29 PM	WireShark capture...	16,508 KB
germany-points.shp.enc	3/10/2023 4:29 PM	WireShark capture...	14,226 KB
france-natural.shp.enc	3/10/2023 4:29 PM	WireShark capture...	11,945 KB
france-waterways.shp.enc	3/10/2023 4:29 PM	WireShark capture...	6,468 KB
indonesia-natural.shp.enc	3/10/2023 4:29 PM	WireShark capture...	12,237 KB
points.shp.enc	3/10/2023 4:29 PM	WireShark capture...	1,539 KB
encDecTimes8.bat	3/10/2023 4:29 PM	Windows Batch File	25 KB
encDecTimes16.bat	16/03/2022 3:10 PM	Windows Batch File	25 KB
encDecTimes24.bat	16/03/2022 3:10 PM	Windows Batch File	25 KB
encDecTimes32.bat	16/03/2022 3:09 PM	Windows Batch File	25 KB
100mb.json.enc	16/03/2022 1:42 AM	WireShark capture...	94,826 KB
kamloops_7.geoJSON	15/03/2022 9:35 PM	GEOJSON File	200,040 KB
encryptionTimes.png	3/03/2022 12:31 PM	PNG File	43 KB
kamloops_1.geoJSON	3/03/2022 12:27 PM	GEOJSON File	100,020 KB
kamloops.geoJSON	3/03/2022 12:04 PM	GEOJSON File	42,372 KB
test.txt.enc	3/03/2022 11:41 AM	WireShark capture...	1 KB

```

D:\OpenSSLEncryptionTimes>encDecTimes8.bat
"Encryption Time"
points.shp Elapsed: 00:00:00.15
france-waterways.shp Elapsed: 00:00:00.12
france-natural.shp Elapsed: 00:00:00.16
indonesia-natural.shp Elapsed: 00:00:00.14
germany-points.shp Elapsed: 00:00:00.41
waterways.shp Elapsed: 00:00:02.02
buildings.shp Elapsed: 00:00:00.86
india-natural.shp Elapsed: 00:00:00.65
natural.shp Elapsed: 00:00:00.93
india-waterways.shp Elapsed: 00:00:01.09
spain-roads.shp Elapsed: 00:00:01.44
quebec_water.shp Elapsed: 00:00:03.25
Camb3D_Bldg_Active_MP_SHP_1.shp Elapsed: 00:00:03.10
landuse.shp Elapsed: 00:00:03.43
Camb3D_Bldg_Active_MP_SHP.shp Elapsed: 00:00:03.44
"#####"
"Decryption Time"
points.shp Elapsed: 00:00:00.14
france-waterways.shp Elapsed: 00:00:00.17
france-natural.shp Elapsed: 00:00:00.22
indonesia-natural.shp Elapsed: 00:00:01.08
germany-points.shp Elapsed: 00:00:00.20
waterways.shp Elapsed: 00:00:00.22
buildings.shp Elapsed: 00:00:00.83
india-natural.shp Elapsed: 00:00:00.52
natural.shp Elapsed: 00:00:00.82
india-waterways.shp Elapsed: 00:00:00.68
spain-roads.shp Elapsed: 00:00:01.64
quebec_water.shp Elapsed: 00:00:01.32
Camb3D_Bldg_Active_MP_SHP_1.shp Elapsed: 00:00:01.83
landuse.shp Elapsed: 00:00:03.22
Camb3D_Bldg_Active_MP_SHP.shp Elapsed: 00:00:02.92
"#####"
D:\OpenSSLEncryptionTimes>
  
```

**Figure B3:** Encryption and Decryption time for spatial files in Windows NTFS using OpenSSL command line tool.