**********Draft**********

This example is from test_crypto.lpr to compare with openssl

06/12/20

**********Draft**********

Legend:

Key

IV

Encrypted

This example is from test_crypto.lpr to compare with openssl
test0612.txt
Key Ascii Now we are engaged in a great ci

Key Hex 4e6f772077652061726520656e676167656420696e2061206772656174206369

IV 000102030405060708090A0B0C0D0E0F

openssl enc -v -P -p -nosalt -aes-256-cbc -K 4e6f772077652061726520656e676167656420696e2061206772656174206369 -iv 000102030405060708090A0B0C0D0E0F -in text.plain -out some.secret.enc

This from test_crypto.lpr
cat text.plain
Four score and s

openssl enc -v -P -p -nosalt -aes-256-cbc -K
4e6f772077652061726520656e676167656420696e2061206772656174206369 -iv
000102030405060708090A0B0C0D0E0F -in text.plain -out some.secret.enc
bufsize=8192
key=4E6F772077652061726520656E676167656420696E2061206772656174206369
iv =000102030405060708090A0B0C0D0E0F
bytes read   :   17
bytes written: 32

some.secret.enc
00000000 23 AE 14 F4 A7 B2 DC 7F 1D D8 9C F6 F0 7E 40 48 #.....~@H
00000010 F6 55 F7 54 99 D6 0A 89 06 69 6E E8 52 05 01 26 .U.T.....in.R..&

test0612.txt
StrEnc
23ae14f4a7b2dc7f1dd89cf6f07e4048
501eb0abb52fd1ad788cec4d154b9fd6

openssl enc -d -v -P -p -nosalt -aes-256-cbc -K
4e6f772077652061726520656e676167656420696e2061206772656174206369 -iv
000102030405060708090A0B0C0D0E0F -in some.secret.enc -out text.plaindec

bufsize=8192
key=4E6F772077652061726520656E676167656420696E2061206772656174206369
iv =000102030405060708090A0B0C0D0E0F
bytes read   :   32
bytes written: 17

cat text.plaindec
Four score and s

Key Ascii Now we are engaged in a great ci

Key Hex 4e6f772077652061726520656e676167656420696e2061206772656174206369

IV 23ae14f4a7b2dc7f1dd89cf6f07e4048

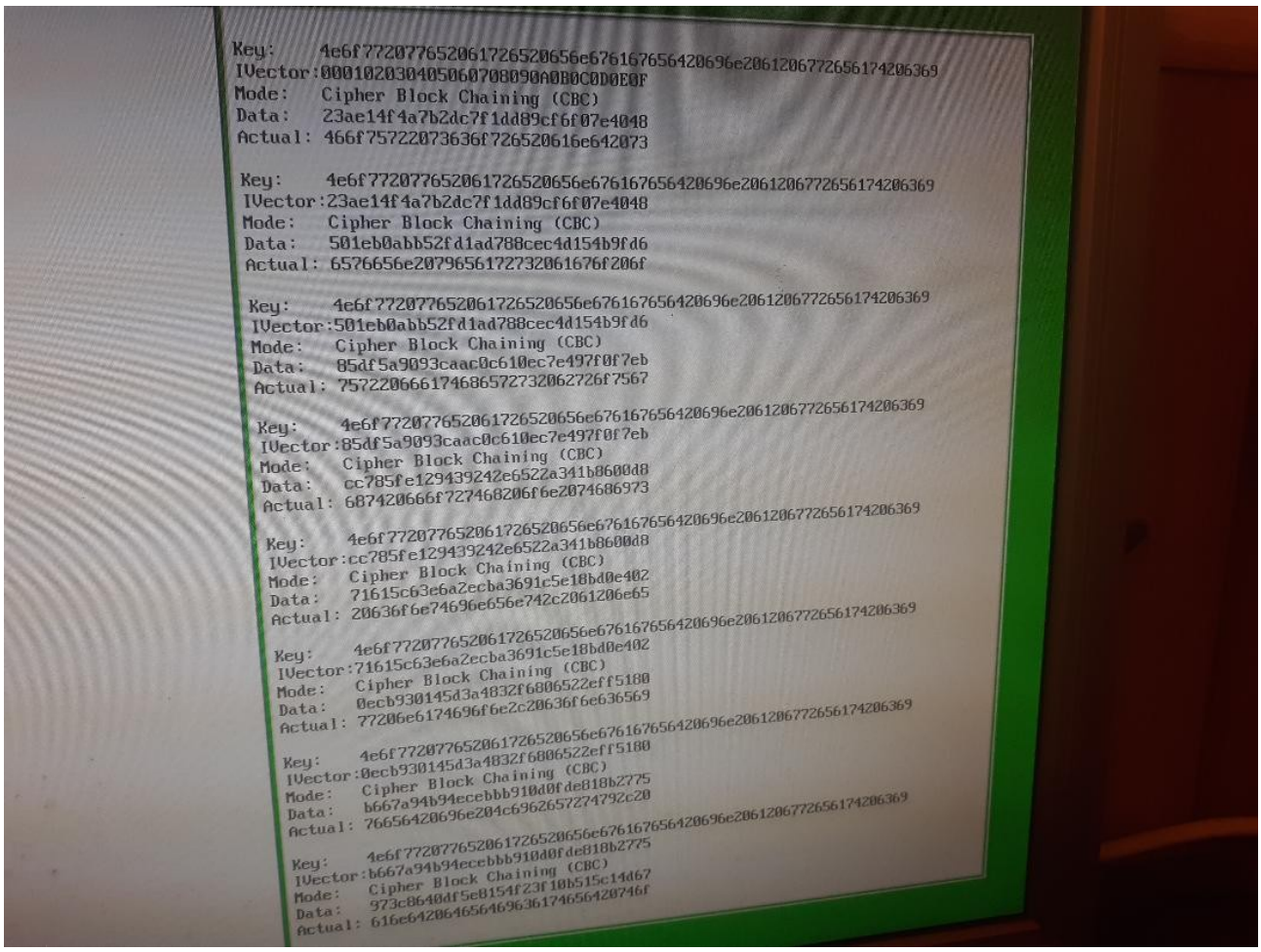
cat text.plain1
even years ago o

openssl enc -v -P -p -nosalt -aes-256-cbc -K 4e6f772077652061726520656e676167656420696e2061206772656174206369 -iv 23ae14f4a7b2dc7f1dd89cf6f07e4048 -in text.plain1 -out some.secret1.enc
bufsize=8192
key=4E6F772077652061726520656E676167656420696E2061206772656174206369
iv =23AE14F4A7B2DC7F1DD89CF6F07E4048
bytes read   :   17
bytes written: 32
some.secret1.enc
00000000 50 1E B0 AB B5 2F D1 AD 78 8C EC 4D 15 4B 9F D6 P..../..x..M.K..
00000010 ED 65 F5 09 E7 2A F1 6E 3E 7D 49 2B 88 D1 DB 79 .e...*.n>}I+...y

test0612.txt
StrEnc
23ae14f4a7b2dc7f1dd89cf6f07e4048
501eb0abb52fd1ad788cec4d154b9fd6

openssl enc -d -v -P -p -nosalt -aes-256-cbc -K 4e6f772077652061726520656e676167656420696e2061206772656174206369 -iv 23ae14f4a7b2dc7f1dd89cf6f07e4048 -in some.secret1.enc -out text.plain1dec
bufsize=8192
key=4E6F772077652061726520656E676167656420696E2061206772656174206369
iv =23AE14F4A7B2DC7F1DD89CF6F07E4048
bytes read   :   32
bytes written: 17

cat text.plain1dec
even years ago o



The file was converted to a single line cat plain.txt
Four score and seven years ago our fathers brought forth on thiscontinent, a new nation, conceived in Liberty, and dedicated to
From file written by Ultibo
ASC & Hex key
Now we are engaged in a great ci
4e6f772077652061726520656e676167656420696e2061206772656174206369
Strplaintext
Four score and s
even years ago o
ur fathers broug
ht forth on this
continent, a ne
w nation, concei
ved in Liberty,
and dedicated to
StrIV
000102030405060708090A0B0C0D0E0F
23ae14f4a7b2dc7f1dd89cf6f07e4048
501eb0abb52fd1ad788cec4d154b9fd6
85df5a9093caac0c610ec7e497f0f7eb
cc785fe129439242e6522a341b8600d8
71615c63e6a2ecba3691c5e18bd0e402
0ecb930145d3a4832f6806522eff5180
b667a94b94ecebbb910d0fde818b2775

StrEnc
23ae14f4a7b2dc7f1dd89cf6f07e4048
501eb0abb52fd1ad788cec4d154b9fd6
85df5a9093caac0c610ec7e497f0f7eb
cc785fe129439242e6522a341b8600d8
71615c63e6a2ecba3691c5e18bd0e402
0ecb930145d3a4832f6806522eff5180
b667a94b94ecebbb910d0fde818b2775
973c8640df5e8154f23f10b515c14d67

StrDecry
466f75722073636f726520616e642073
6576656e207965617273206167 6f206f
757220666174686572732062726f7567
687420666f727468206f6e2074686973
20636f6e74696e656e742c2061206e65
77206e6174696f6e2c20636f6e636569
76656420696e204c6962657274792c20
616e642064656469636174656420746f

The first 4 lines match the 2nd thru 5th IV. The question is why the 6th thru 8th do not match

openssl enc -v -P -p -nosalt -aes-256-cbc -K
4e6f772077652061726520656e676167656420696e20612067726561742063 69 -iv
000102030405060708090A0B0C0D0E0F -in plain.txt -out encrypted
bufsize=8192
key=4E6F772077652061726520656E676167656420696E20612067726561742063 69
iv =000102030405060708090A0B0C0D0E0F
bytes read : 128
bytes written: 144

```
00000000  23 AE 14 F4  A7 B2 DC 7F  1D D8 9C F6  F0 7E 40 48  #.............~@H
00000010  50 1E B0 AB  B5 2F D1 AD  78 8C EC 4D  15 4B 9F D6  P..../..x..M.K..
00000020  85 DF 5A 90  93 CA AC 0C  61 0E C7 E4  97 F0 F7 EB  ..Z.....a.......
00000030  CC 78 5F E1  29 43 92 42  E6 52 2A 34  1B 86 00 D8  .x_.)C.B.R*4....
00000040  A9 2C 44 DD  D8 D4 3F 8A  6D 45 3E 21  A2 E9 AC F0  .,D...?.mE>!....
00000050  73 92 B1 A2  EC A5 DD 06  A3 EF 57 E2  35 38 CC 3D  s.........W.58.=
00000060  76 06 59 C5  A0 33 21 98  60 D2 06 FB  C3 0E B0 6C  v.Y..3!.`......l
00000070  9F 8A 06 8D  7E 89 34 73  58 D7 FD B3  8B E9 B8 21  ....~.4sX......!
00000080  B3 25 71 10  4D 31 A5 90  18 5F DA C4  AF 3D 56 06
```

~~cat plain.txt~~
~~Four score and s~~
~~even years ago o~~
~~ur fathers broug~~
~~ht forth on this~~
~~ continent, a ne~~
~~w nation, concei~~
~~ved in Liberty,~~

and dedicated to

openssl enc -v -P -p -nosalt -aes-256-cbc -K 4e6f772077652061726520656e676167656420696e2061206772656174206369 -iv 000102030405060708090A0B0C0D0E0F -in plain.txt -out encrypted
bufsize=8192
key=4E6F772077652061726520656E676167656420696E2061206772656174206369
iv =000102030405060708090A0B0C0D0E0F
bytes read   :   136
bytes written: 144

00000000 23 AE 14 F4 A7 B2 DC 7F 1D D8 9C F6 F0 7E 40 48 #.........~@H
00000010 24 83 59 90 D3 29 7C A2 83 50 86 D1 50 DF E4 D1 $.Y..)|..P..P...
00000020 61 1E 3B 24 F3 80 23 24 25 EC 49 F0 1A 9A 40 F8 a.;$..#$%.I...@.
00000030 D6 BC A5 29 77 41 61 F4 2A 0C 66 5D D2 EE CD AE ...)wAa.*.f]....
00000040 D1 1B C6 A2 B4 9D 8C BA 5E D3 CA 7C E3 FF 64 09 ....^..|..d.
00000050 16 20 99 0F EB BD 82 A6 9C 8C 59 29 DD E1 D6 B1 . ...Y)....
00000060 19 08 59 8E E4 4B C4 4B AF E3 50 B0 68 D1 49 26 ..Y..K.K..P.h.I&
00000070 AD 5B 8D B4 7C 44 02 DD D8 CC 1B 59 5E 86 4B D7 .[..|D.....Y^.K.
00000080 AB D6 E5 58 B2 16 77 F2 32 EB 40 38 61 6B 5D 70 ...X..w.2.@8ak]p

openssl enc -d -v -P -p -nosalt -aes-256-cbc -K 4e6f772077652061726520656e676167656420696e2061206772656174206369 -iv 000102030405060708090A0B0C0D0E0F -in encrypted -out decrypted
bufsize=8192
key=4E6F772077652061726520656E676167656420696E2061206772656174206369
iv =000102030405060708090A0B0C0D0E0F
bytes read   :   144
bytes written: 136

cat decrypted
Four score and s
even years ago o
ur fathers broug
ht forth on this
 continent, a ne
w nation, concei
ved in Liberty,
and dedicated to

openssl enc -d -v -P -p -nosalt -aes-256-cbc -K 4e6f772077652061726520656e676167656420696e2061206772656174206369 -iv 000102030405060708090A0B0C0D0E0F -in encrypted -out decrypted
bufsize=8192
key=4E6F772077652061726520656E676167656420696E2061206772656174206369
iv =000102030405060708090A0B0C0D0E0F
bytes read   :   144
bytes written: 128

cat decrypted

Four score and seven years ago our fathers brought forth on thiscontinent, a new nation, conceived in Liberty, and dedicated to

openssl help
Standard commands
asn1parse ca ciphers cms
crl crl2pkcs7 dgst dhparam
dsa dsaparam ec ecparam
enc engine errstr gendsa
genpkey genrsa help list
nseq ocsp passwd pkcs12
pkcs7 pkcs8 pkey pkeyparam
pkeyutl prime rand rehash
req rsa rsautl s_client
s_server s_time sess_id smime
speed spkac srp storeutl
ts verify version x509

Message Digest commands (see the `dgst' command for more details)
blake2b512 blake2s256 gost md4
md5 rmd160 sha1 sha224
sha256 sha3-224 sha3-256 sha3-384
sha3-512 sha384 sha512 sha512-224
sha512-256 shake128 shake256 sm3

Cipher commands (see the `enc' command for more details)
aes-128-cbc aes-128-ecb aes-192-cbc aes-192-ecb
aes-256-cbc aes-256-ecb aria-128-cbc aria-128-cfb
aria-128-cfb1 aria-128-cfb8 aria-128-ctr aria-128-ecb
aria-128-ofb aria-192-cbc aria-192-cfb aria-192-cfb1
aria-192-cfb8 aria-192-ctr aria-192-ecb aria-192-ofb
aria-256-cbc aria-256-cfb aria-256-cfb1 aria-256-cfb8
aria-256-ctr aria-256-ecb aria-256-ofb base64
bf bf-cbc bf-cfb bf-ecb
bf-ofb camellia-128-cbc camellia-128-ecb camellia-192-cbc
camellia-192-ecb camellia-256-cbc camellia-256-ecb cast
cast-cbc cast5-cbc cast5-cfb cast5-ecb
cast5-ofb des des-cbc des-cfb
des-ecb des-ede des-ede-cbc des-ede-cfb
des-ede-ofb des-ede3 des-ede3-cbc des-ede3-cfb
des-ede3-ofb des-ofb des3 desx
rc2 rc2-40-cbc rc2-64-cbc rc2-cbc
rc2-cfb rc2-ecb rc2-ofb rc4
rc4-40 seed seed-cbc seed-cfb
seed-ecb seed-ofb sm4-cbc sm4-cfb
sm4-ctr sm4-ecb sm4-ofb

openssl enc --help
Usage: enc [options]
Valid options are:
 -help Display this summary

-ciphers List ciphers
-in infile Input file
-out outfile Output file
-pass val Passphrase source
-e Encrypt
-d Decrypt
-p Print the iv/key
-P Print the iv/key and exit
-v Verbose output
-nopad Disable standard block padding
-salt Use salt in the KDF (default)
-nosalt Do not use salt in the KDF
-debug Print debug info
-a Base64 encode/decode, depending on encryption flag
-base64 Same as option -a
-A Used with -[base64|a] to specify base64 buffer as a single line
-bufsize val Buffer size
-k val Passphrase
-kfile infile Read passphrase from file
-K val Raw key, in hex
-S val Salt, in hex
-iv val IV in hex
-md val Use specified digest to create a key from the passphrase
-iter +int Specify the iteration count and force use of PBKDF2
-pbkdf2 Use password-based key derivation function 2
-none Don't encrypt
-* Any supported cipher
-rand val Load the file(s) into the random number generator
-writerand outfile Write random data to the specified file
-engine val Use engine, possibly a hardware device