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

This example is from test_crypto.lpr to compare with openssl
06/10/20

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

Legend:
Key
IV
Encrypted

This example is from test_crypto.lpr to compare with openssl
test0513.txt
Key Ascii Now we are engaged in a great ci

Key Hex 4e6f772077652061726520656e676167656420696e20612067726561742063 69

IV 000102030405060708090A0B0C0D0E0F

openssl enc -v -P -p -nosalt -aes-256-cbc -K 4e6f772077652061726520656e676167656420696e206120677265617420636 9 -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..&
```

test0513.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
```

```
test0513.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
```

```
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
4e6f77207765206172652067656e6e6572616c20617661696c6162696c697479
```

```
openssl enc -v -P  -p -nosalt -aes-256-cbc -K
4e6f772077652061726520656e676167656420696e206120677265617420636 -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 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
```