ΕΠΛ326: Εργαστήριο 2 / CS326: Lab 2

Στο σημερινό εργαστήριο θα χρησιμοποιήσουμε το εργαλείο openssl για να κρυπτογραφήσουμε και να αποκρυπτογραφήσουμε δεδομένα χρησιμοποιώντας συμμετρική κρυπτογράφηση. Στο τέλος αυτού του εργαστήριου οι φοιτητές θα μπορούν να:

- κρυπτογραφούν ένα αρχείο από δεδομένά χρησιμοποιώντας συμμετρικά κρυπτογραφήματα, DES/AES
- αποκρυπτογραφούν κρυπτογραφήματα
- καταλαβαίνουν το ASCII coding
- χρησιμοποιούν τον αλγόριθμο DES/AES με διαφορετικούς διακόπτες

In today's lab we are going to use the openssl tool for encrypting and decrypting data using symmetric encryption. You should:

- Learn how to encrypt with DES/AES
- Learn how to decrypt with
- Understand the ASCII encoding
- Use options in DES/AES

Βήμα 1:

Σχεδιάστε το Feistel Network του DES, χωρίς να αναλύσετε τη συνάρτηση *f*. Δείξτε με ποια μαθηματική σχέση συνδέονται τα R_i, L_i με τα R_{i-1}, L_{i-1} και το κλειδί k_i.

Step 1:

Draw the Feistel Network of DES, without further analyzing the *f* function. Show the mathematical expression that connects R_i, L_i with R_{i-1}, L_{i-1} and the key k_i.

Βήμα 2:

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Για το παραπάνω S-box βρείτε την έξοδο των: 100101, 100110, 011110, 111111.

Step 2:

For the above S-box, find the outputs of 100101, 100110, 011110, 111111.

Βήμα 3/Step 3:

Περισσότερες πληροφορίες για το OPENSSL μπορείτε να βρείτε στον σύνδεσμο, https://www.openssl.org/docs/manmaster/man1/enc.html.

Κατά την διάρκεια του εργαστηρίου μπορείτε να χρησιμοποιείτε τον πιο πάνω σύνδεσμο για καλύτερη κατανόηση του εργαλείου openssl.

You can find more for openssl in the following link, https://www.openssl.org/docs/manmaster/man1/enc.html.

You can always use the above link during the lab exercises.

Βήμα 4/Step 4:

Πληκτρολογήστε την πιο κάτω εντολή/Type the command

```
$ openssl help
openssl:Error: 'help' is an invalid command.

Standard commands
asn1parse      ca             ciphers        crl            crl2pkcs7
dgst           dh             dhparam        dsa            dsaparam
ec             ecparam        enc            engine         errstr
gendh          gendsa         genrsa         nseq           ocsp
passwd         pkcs12         pkcs7          pkcs8          prime
rand           req            rsa            rsautl         s_client
s_server       s_time         sess_id        smime          speed
spkac          verify         version        x509

Message Digest commands (see the `dgst' command for more details)
md2            md4            md5            mdc2           rmd160
sha            sha1

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    base64         bf             bf-cbc         bf-cfb
bf-ecb         bf-ofb         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
```

```
(will be dealing with the 2nd part, i.e., the 'enc' command)
```

Επίσης δοκιμάστε την εντολή/Try also the command:

```
OpenSSL> enc help
unknown option 'help'
options are
-in <file>     input file
-out <file>    output file
-pass <arg>    pass phrase source
-e             encrypt
-d             decrypt
-a/-base64     base64 encode/decode, depending on encryption flag
-k             passphrase is the next argument
-kfile         passphrase is the first line of the file argument
-md            the next argument is the md to use to create a key
                 from a passphrase.  One of md2, md5, sha or sha1
-K/-iv         key/iv in hex is the next argument
-[pP]          print the iv/key (then exit if -P)
-bufsize <n>   buffer size
-engine e      use engine e, possibly a hardware device.
Cipher Types
-aes-128-cbc               -aes-128-cfb               -aes-128-cfb1
-aes-128-cfb8              -aes-128-ecb               -aes-128-ofb
-aes-192-cbc               -aes-192-cfb               -aes-192-cfb1
-aes-192-cfb8              -aes-192-ecb               -aes-192-ofb
-aes-256-cbc               -aes-256-cfb               -aes-256-cfb1
-aes-256-cfb8              -aes-256-ecb               -aes-256-ofb
-aes128                    -aes192                    -aes256
-bf                        -bf-cbc                    -bf-cfb
-bf-ecb                    -bf-ofb                    -blowfish
-cast                      -cast-cbc                  -cast5-cbc
-cast5-cfb                 -cast5-ecb                 -cast5-ofb
-des                       -des-cbc                   -des-cfb
-des-cfb1                  -des-cfb8                  -des-ecb
-des-ede                   -des-ede-cbc               -des-ede-cfb
-des-ede-ofb               -des-ede3                  -des-ede3-cbc
-des-ede3-cfb              -des-ede3-cfb1             -des-ede3-cfb8
-des-ede3-ofb              -des-ofb                   -des3
-desx                      -desx-cbc                  -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
error in enc
```

για να τρέξετε το openssl/for running openssl:

```
$ openssl
```

```
OpenSSL> version
OpenSSL 0.9.8zh 14 Jan 2016
```

Βήμα 5:

Χρησιμοποιείστε την εντολή **cat** για να δείτε τα περιεχόμενα του αρχείου secret-file/
Use cat to inspect the contents of the file

```
$ cat secret-file
Achille-Claude Debussy (French: [aÊƒil klod dÉ™bysi], 22 August 1862
â€“ 25 March 1918), known since the 1890s as Claude-Achille Debussy or
Claude Debussy, was a French composer. He and Maurice Ravel were the
most prominent figures associated with Impressionist music, though
Debussy disliked the term when applied to his compositions. He was
made Chevalier of the Legion of Honour in 1903. He was among the most
influential composers of the late 19th and early 20th centuries, and
his use of non-traditional scales and chromaticism influenced many
composers who followed.

$ openssl aes-256-cbc -e -in secret-file -out secret-file.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:

$ file secret-file.enc
secret-file.enc: data


$ cat secret-file.enc
```

Το αρχείο που έχει δημιουργηθεί είναι σε **binary** μορφή/
The new file is now binary

Περιεχόμενα κρυπτογραφημένου αρχείου/The contents of the encrypted file:

```
$ hexdump secret-file.enc
0000000 53 61 6c 74 65 64 5f 5f b0 22 30 66 19 20 cf 1a
0000010 f1 6b 0c cf 36 59 4a 05 0c 1b d7 1d 75 5f a1 ff
0000020 e8 33 95 cd b5 da c7 cb fb 58 f6 09 17 14 c7 48
0000030 bf e6 ae 6d 2a f3 36 95 a8 12 70 52 d1 af 0c 6b
0000040 28 49 2b 5b 99 db da ff f3 54 f7 e3 af fd 75 64
0000050 cd b8 f5 e2 59 e9 25 44 f4 dd bb db 2f 3d 2b 19
0000060 71 1d d2 6f 34 72 26 be 98 1b 3d b8 81 e4 40 4d
0000070 66 74 de 87 13 18 a6 f0 f3 26 9f 24 87 2f 24 8c
0000080 7e 6c 8b 94 d3 87 48 7e 31 18 eb 2f c4 cf c8 74
0000090 cf 9b 6c 4b 76 1b 23 15 66 90 04 df 44 34 d9 b8
00000a0 de 91 56 cc 5f 23 1f 3d 13 39 09 a1 69 ba 12 ca
00000b0 21 28 c7 ff 4f d2 63 ba 5d bd e4 b1 c5 b5 5b a1
00000c0 27 f8 3f f9 f7 12 04 7e f7 c3 61 4e df f0 9b 65
00000d0 3d d3 59 2b 94 23 2a e3 ea 3c 12 68 95 0a b9 b2
00000e0 bd f1 81 91 5f 0d 36 33 4a 62 36 a4 96 af 0a 0a
```

```
00000f0 55 0a f0 72 09 2e b1 da 29 c4 df af 4b 76 af 05
0000100 0f 8c 1c 6f f7 b2 08 dc cb fa b5 7c 31 d9 52 5f
0000110 ac 8b 35 b3 9f 0c d7 4a 42 10 c4 68 e0 a4 fc 88
0000120 89 ad 31 f4 e6 de 94 95 aa d7 8f 60 b4 81 1a 70
0000130 5d 38 f4 14 73 49 7b a6 07 9c b4 57 7b f1 e9 d2
0000140 08 4f 6b 67 8d 41 4e 67 0b e4 b9 20 3b 94 e3 9d
0000150 b1 82 09 6a 16 fb 66 14 60 b1 63 9e 7f 4d d9 44
0000160 1d c8 08 a0 29 5e 48 1b d1 42 51 63 fe 8f 9c cd
0000170 27 73 62 f8 2d 0a 9a 50 0c af d4 59 2e 16 5c 1e
0000180 4e 62 07 5c 81 83 9f 67 84 cc 71 fc 33 a7 29 54
0000190 c7 14 0f e6 48 f8 77 f9 a9 de 68 e8 4f da 16 7e
00001a0 cc e0 0a 67 2e f7 26 51 78 fb e5 e3 d8 bc 84 c5
00001b0 be d2 72 4e e8 fb 48 cf e1 87 de fd c8 57 8c b5
00001c0 74 bc 10 61 19 17 e9 ae 39 04 d5 6e a4 18 96 f1
00001d0 ac 3b b5 44 80 41 38 47 7d f2 36 0b f3 e5 82 11
00001e0 34 d1 b8 3e 41 90 52 6f 6d 76 49 d2 b3 2c 6f fe
00001f0 be c7 a4 ee a4 05 49 16 85 c0 bf 56 12 6b 9b 74
0000200 db 8c 42 27 40 7b ea 18 41 f4 a5 fd f8 5a 51 27
0000210 d1 e4 d4 f8 56 d6 b1 ba e4 5a 95 04 63 21 92 d0
0000220 27 9a a3 d3 50 cf bc 12 4c d5 04 89 c2 ee b4 04
0000230 a0 fd ad 0d 8f c8 c3 77 c4 7d b8 b8 73 4b 66 30
0000240 81 1b 88 18 e4 8c 2f 69 f6 0e 07 25 a7 5e f3 b3
0000250
```

Αποκρυπτογράφηση κρυπτογραφημένου αρχείου/Decrypt the file:

```
$ openssl aes-256-cbc -d -in secret-file.enc -out secret-
file.decrypted
enter aes-256-cbc decryption password: xxxxxxx

$ cat secret-file.decrypted
Achille-Claude Debussy (French: [aÊƒil klod dÉ™bysi], 22 August 1862
â€“ 25 March 1918), known since the 1890s as Claude-Achille Debussy or
Claude Debussy, was a French composer. He and Maurice Ravel were the
most prominent figures associated with Impressionist music, though
Debussy disliked the term when applied to his compositions. He was
made Chevalier of the Legion of Honour in 1903. He was among the most
influential composers of the late 19th and early 20th centuries, and
his use of non-traditional scales and chromaticism influenced many
composers who followed.
```

Βήμα 6/Step 6:

Να επαναλάβετε τα πιο πάνω βήματα αλλά να χρησιμοποιείστε τον διακόπτη **-a** για την κρυπτογράφηση. Με την επιλογή **–a** θα δημιουργήσετε ASCII αρχείο. Αυτό γίνετε γιατί χρησιμοποιούμε Base64 (an encoding to translate binary to printable characters).

Repeat again the steps but now use –a for encryption. By using –a an ASCII file will be created using the Base64 encoding, which maps all binary characters to printable groups of characters.

```
$ openssl aes-256-cbc -a -in secret-file -out secret-file.enc
enter aes-256-cbc encryption password:  xxxxx
Verifying - enter aes-256-cbc encryption password:  xxxxx
```

Χρησιμοποιήστε την εντολή **file** για να ελέγξετε τον τύπο του αρχείου/Use **file** to inspect the format of the file

```
$ file secret-file.enc
secret-file.enc: ASCII text
```

```
$ cat secret-file.enc
U2FsdGVkX1+rcRkyk48lNvzAR2ZHb94ZWxgvVG4r7Da1onTBxdhHCz2z6fMEI9F4
NqGV75W6/zNFwjnCnWXsyCiY1M9DrM6UktkJslNtjFCvJ8tNfpsHlNbsm/xT0D6W
4ZdVZkecfTBaV0ZowFySb6FxyEKXWCZ7aY2pFijsSYnrrP/XU2lL1EBH+QXs6pNz
qScF275BWU+BywNC+eXEot+FJVqKP8CtAIlsgzlxexI7hQOHCn6MNhvLzVtXG+XB
ADAKIykLUOJAH3zS5WnezqkAEYeX4vy7P9iDum/1RhNXTR1BYfYpa1Wes8Fp9qzU
qIbntrX7GTYNyfqxVuaCPZF6Ev7zyhI8meMkOQRl1b55/toRqOSYzALTOeZXI1Rh
qiK/NQagM+Go8iiURIClMFY9fH8P1W9afKviKqxD6722eK/FjD5U6GbOYB/scmr2
NL7H2VPoBsv4BfD0WFiiGLLWZiP+DpooYvRerswK0OlLFLGAf/BUmyjsmR/COWxb
hwgLhKJlDUaXwQvN2uBU1zrIMgnGeZscjaJLT6iBaA7E73rS1dLQ2/Q/sP/WiFsD
cITjmRXWK1QFiRYvYLFBNthiEuVJmyESYotWfWsltXrYgcPoASv9UqlaZGp0SOyf
Wyz6t4Urn6zINcW1AFjqVoQdHqqyO0jzFIY2R2lqpBNhLUEfs8r7aid6TMvh17MX
OBKNWxCQVfwEVxyUehxnxiLucfT9XnVDXLEnMc20w7hs7Ebl8047OU+2n5LiXxdf
oS1zJWbrm3IiPVqx+5pU6g==
```

Μπορείτε να χρησιμοποιήσετε τον σύνδεσμο https://cryptii.com/text/base64 για να κατανοήσετε καλυτέρα πως δουλεύει το Base64.

You can find more for Base64 at https://cryptii.com/text/base64.

Βήμα 7/Step 7:

Κρυπτογράφηση δεδομένων χρησιμοποιώντας τον διακόπτη **-k** για να καθορίσουμε κωδικό/ Encryption of data using **–k** for enabling a password

```
$ echo "Hello world" | openssl aes-256-cbc -a -k mypass
U2FsdGVkX1/QOZ3pdor7y0RU78JJaJx4dnruNJx41fk=
```

Εκτελεστέ την ιδιά εντολή αρκετές φορές/Repeat the command sever times

```
$ echo "Hello world" | openssl aes-256-cbc -a -k mypass
U2FsdGVkX18Qjogwzvti10njjG3YRO+4WLRla1MTqtk=
```

```
$ echo "Hello world" | openssl aes-256-cbc -a -k mypass
U2FsdGVkX18pKL80FU8zUIGj2IrfJVdkKgXHZE/xs9M=
```

```
$ echo "Hello world" | openssl aes-256-cbc -a -k mypass
U2FsdGVkX1+fXpZ+/oTCMHUPG6Ji02uYaUl8BnLGP2U=

$ echo "Hello world" | openssl aes-256-cbc -a -k mypass
U2FsdGVkX1+H8K6LRBPCKE3ZXeCJ8E2CbLOePjQQREA=
```

Αν και ο κωδικός είναι ο ίδιος παρατηρούμε ότι τα αποτελέσματα είναι διαφορετικά. Αυτό συμβαίνει επειδή χρησιμοποιούμε **"salt"**. Μπορούμε να εκτελέσουμε την ιδιά εντολή με τον διακόπτη **-nosalt** για να το απενεργοποιήσουμε.

Although the password is always the same, the results of the encryption are different. This is because of the use of **"salt".** You can use **-nosalt** to turn off this.

```
$ echo "Hello world" | openssl aes-256-cbc -a -nosalt -k mypass
Y6gOmC3+eJNK6fRJgglxXA==

$ echo "Hello world" | openssl aes-256-cbc -a -nosalt -k mypass
Y6gOmC3+eJNK6fRJgglxXA==

$ echo "Hello world" | openssl aes-256-cbc -a -nosalt -k mypass
Y6gOmC3+eJNK6fRJgglxXA==

$ echo "Hello world" | openssl aes-256-cbc -a -nosalt -k mypass
Y6gOmC3+eJNK6fRJgglxXA==
```

Βήμα 8/Step 8:

Ο Electronic Codebook mode (ECB) αλγόριθμος, είναι πιο ευάλωτος σε σχέση με τον CBC αλγόριθμο, επειδή κάθε μπλοκ κρυπτογραφείται χωρίς να χρησιμοποίει πληροφορίες από άλλα μπλοκ για αυτό το λόγο τα μπλοκ που είναι τα ιδιά παράγουν τα ιδιά κρυπτογραφήματα.

Electronic Codebook mode (ECB) is a weaker mode, since every block is encrypted individually. This is not the case with CBC, where each block is using information from previous block before encryption.

```
$ echo
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAA" | openssl aes-128-ecb -a -nosalt -k mypass
qL6qDyLQqBGzGIhYr2ztg6i+qg8i0KgRsxiIWK9s7YOovqoPItCoEbMYiFivbO2D
qL6qDyLQqBGzGIhYr2ztg6i+qg8i0KgRsxiIWK9s7YMDE+4uheimszaju+hDE0E5
```

Μόνο οι τελευταίοι χαρακτήρες διαφέρουν στο κρυπτογράφημα και αυτό είναι λόγω του padding. Προσθέστε περισσότερα 'A's.

Only the last characters are different due to padding. Add more ‘A’s.

```
$ echo
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAA" | openssl aes-128-ecb -a -nosalt -k
mypass
qL6qDyLQqBGzGIhYr2ztg6i+qg8i0KgRsxiIWK9s7YOovqoPItCoEbMYiFivbO2D
qL6qDyLQqBGzGIhYr2ztg6i+qg8i0KgRsxiIWK9s7YOovqoPItCoEbMYiFivbO2D
uPNkft7kkqukzMnYpm3gpg==
```

Παρατηρούμε ότι και οι δυο γραμμές είναι ιδίες. Αυτό δεν θα συνέβαινε εάν χρησιμοποιούσαμε τον αλγόριθμο Cihper Block Chaining (CBC).

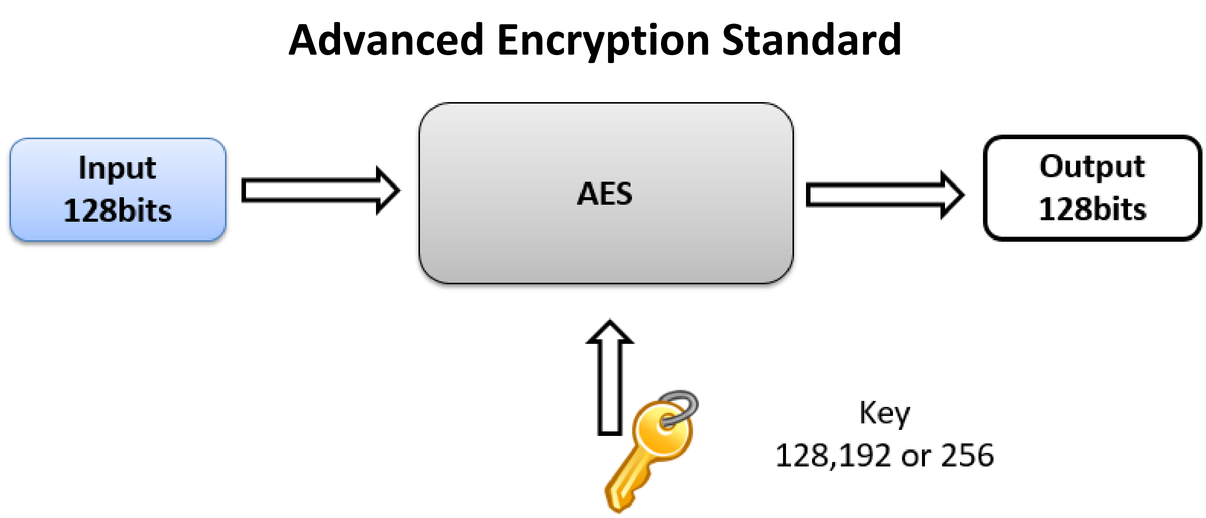
Notice that both lines are equal. We can avoid this using CBC.

```
$ echo
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAA" | openssl aes-128-cbc -a -nosalt -k
mypass
xKapMYSqhDZE4pcQ+Fsi+SqzVmFl+sLavqswlzri2Q9Zdcqeml/lY1hiDFPHawW4
EM76677/oQHv7hRi86PjX1UGbJAseA0BEdB3y5ObTcJvHvu9EtIjb3pTSgJsSJQQ
IYFViIQn+CjtMSZEJ1h+eg==
```

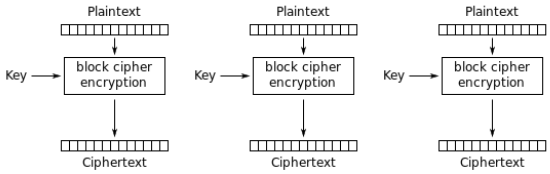
Βήμα 9/Step 9:

Να επαναλάβετε όλα τα πιο πάνω βήματα χρησιμοποιώντας τον DES αλγόριθμο.

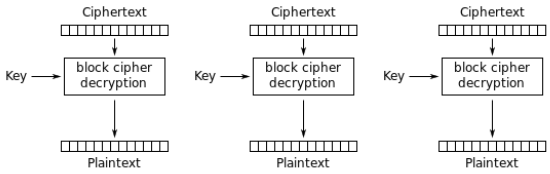
Repeat all the above steps using the DES algorithm



Modes of operation: Electronic Code (ECB) Mode:

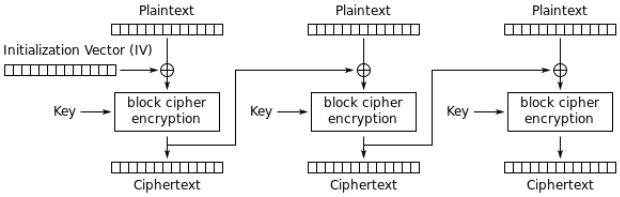


Electronic Codebook (ECB) mode encryption

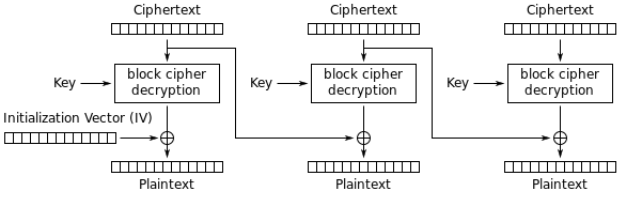


Electronic Codebook (ECB) mode decryption

Cipher-Block Chaining (CBC) Mode



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Summary of Modes

Mode	Formulas	Ciphertext
ECB	Y_i=F(PlainText$_i$,Key)	Y_i
CBC	Y_i=PlainText$_i$ XOR Ciphertext$_{i-1}$	F(Y,key); Ciphertext$_0$=IV
PCBC	Y_i=PlainText$_i$ XOR (Ciphertext$_{i-1}$ XOR PlainText$_{i-1}$)	F(Y,key);Ciphertext$_0$=IV
CFB	Y_i=Ciphertext$_{i-1}$	Plaintext XOR F(Y,key);Ciphertext$_0$=IV
OFB	Y_i=F(Key,I$_{i-1}$);Y_0=IV	Plaintext XOR Y_i
CTR	Y_i=F(Key,IV + g(i));IV=token();	Plaintext XOR Y_i