

# Cryptography Lab

## Group Members

Harris Verdun  
Pablo Hernandez  
Ramier McIntyre  
Heber Paz

## Objectives

- To do a hands on activity to encrypt our data
- Learn how to use symmetric cryptography to encrypt and decrypt a message
- Learn how to transfer files with a lab partner

## Executive Summary

This lab focused on symmetric cryptography. We first created a key with a 56 bit encryption. Then we encrypted a file with that key, and transferred the file and the key with our lab partner. Our lab partner then downloaded the encrypted file, and with the key that we created. Then we decrypted the partners file with the respective key.

```
Shell - Konsole
Session Edit View Bookmarks Settings Help

OPENSSL(1)                                OpenSSL
NAME
  openssl - OpenSSL command line tool

SYNOPSIS
  openssl command [ command_opts ] [ command_args ]

  openssl [ list-standard-commands | list-message-digest-commands | list-cipher-commands ]

  openssl no-XXX [ arbitrary options ]

DESCRIPTION
  OpenSSL is a cryptography toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport
  Security (TLS v1) network protocols and related cryptography standards required by them.

  The openssl program is a command line tool for using the various cryptography functions of the
  crypto library from the shell. It can be used for

  o Creation of RSA, DH and DSA key parameters
  o Creation of X.509 certificates, CSRs and CRLs
  o Calculation of Message Digests
  o Encryption and Decryption with Ciphers
  o SSL/TLS Client and Server Tests
  o Handling of S/MIME signed or encrypted mail

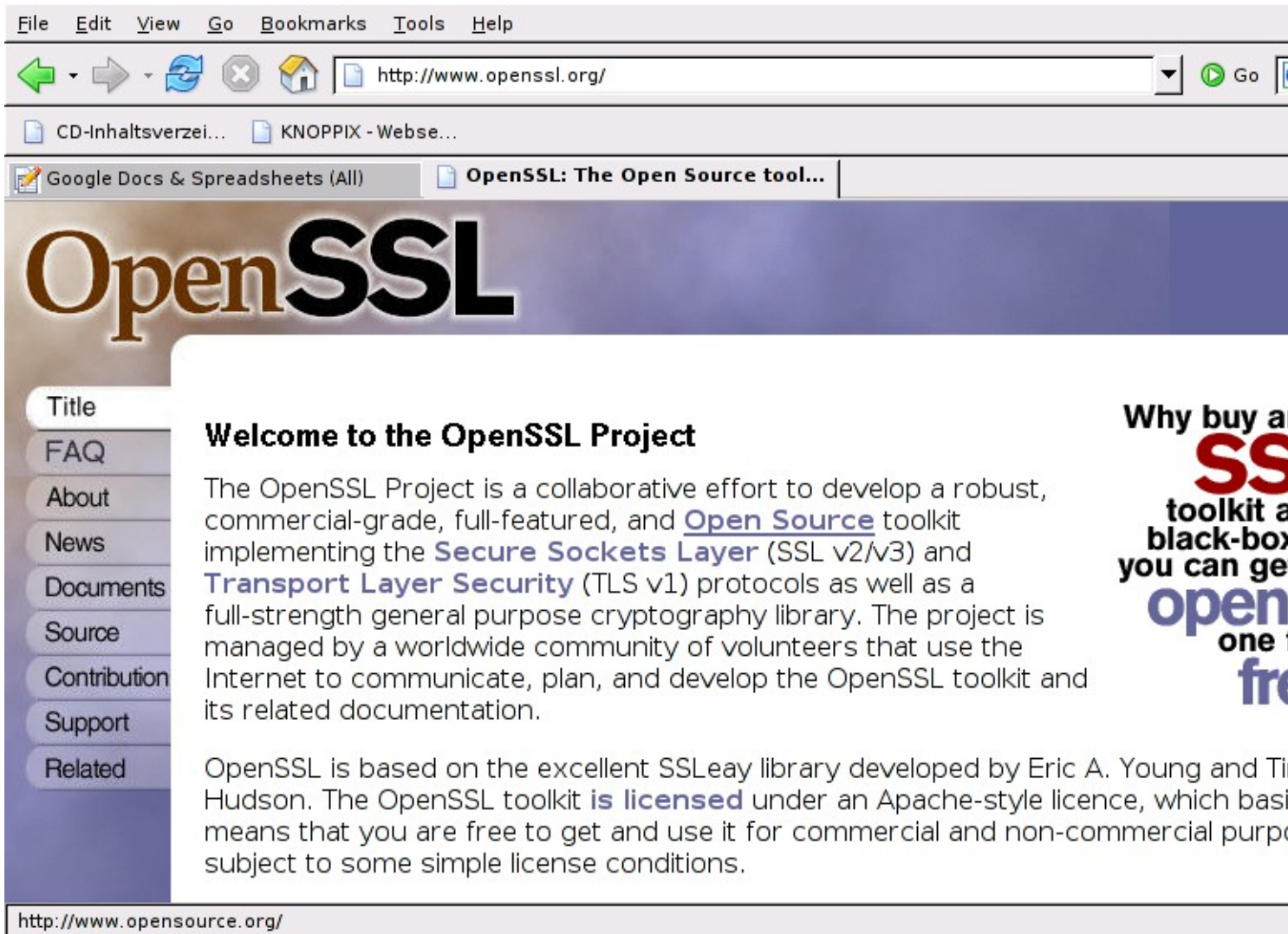
COMMAND SUMMARY
  The openssl program provides a rich variety of commands (command in the SYNOPSIS above),
  often has a wealth of options and arguments (command_opts and command_args in the SYNOPSIS
  above).

  The pseudo-commands list-standard-commands, list-message-digest-commands, and list-cipher-
  commands put a list (one entry per line) of the names of all standard commands, message digest
  commands, and cipher commands, respectively, that are available in the present openssl utility.

  The pseudo-command no-XXX tests whether a command of the specified name is available. If
  the command named XXX exists, it returns 0 (success) and prints no-XXX; otherwise it returns 1 and prints
  no-XXX. In both cases, the output goes to stdout and nothing is printed to stderr. Additional
  options and arguments are always ignored. Since for each cipher there is a command of the same
  name, this is an easy way for shell scripts to test for the availability of ciphers in the
  openssl program. (The openssl program is not able to detect pseudo-commands such as quit,
  list-...-commands, or no-XXX itself.)

Manual page openssl(1ssl) line 1
```

**This is the OpenSSL website**



**This is what our file looked like once it was encrypted.**

Session Edit View Bookmarks Settings Help

```
ttJNdEBDaSS9M1K7sQ8vAdmDX0n0K9Cw8NY4VLYdnXs4hfXhcxABrc5dtYdpMHi6
xooRmuczPsYSJIouU4/tLrCjYEt0Av0Nrkn94W1n0a95qIT1SoVy2SPWjne9ZMXY
0Gom1m4VCVuzab1iKPDgyocZPI3kXekCpge2ADFI+5Y1vm/jUI0JH013FS+MLLgV
XYxygo0juR9XJVM0nuV80/SgLLbVgA/SerE/kiZ5RpuYmitqCDpezYDs
K0YMgd665oaDdYhfZqVWfSGR1rF0ihBD37+NLtW5/E1giyiMmdDAwWuBQw2p4TLA
siftfHpXfmJz2LPWgNacaYGz1KFUcRqiT2ohVVKzKJpC43q9cN1cWfH+8g22b2iCK
Id7Zf48PtHjt1TqFcaNIiy7JowQ3sbzv27jAInbRN7U16e/AZ5qbELqX101TUE/F
/E7DzyyC69K107Gty8vpi+Nk0h//dSkqRxaUCY16k867w8LAG/TMm2zsDsW2yvJ
bLwkjaeMa328SpWHfbrCocjMLtLhezQ8jhL7YfxkqFZiemXocuJN0p02F22NVoUq
vfgSck17Tfu4HKAQZYU4p3K9+TpfclnkF6WbYjXnDTByIiIuFoyKI5jgURR1Bejs
R60q+MSx0SQ1beyhJeVNDT+wJ76eszgdmIaz8d2Ct++XBad6H+HGQVL3RQ5vqTEj
R0KHgBo1fhIrRDtyAfksawAoh1V4k5aAh466EfjZRIUq+qAfHBtQ/wf2Hj1h4vs
6UpoIIMTEyp0y0WGX3oRoEJd4XmTvCqT2G0ReZbUU8o3gA0IJ7658HIFcmU9kceK
02u4Dqqqtqy5VUNTxBhXRZqK+hzpQmiGswsoRFHMv5n6HUPK/vMBrm3Hxb86cvxjJ
7VRIEeBpG36eJVRHdqNMfMLPw9HGw8E090fqpYMHJ1mpTD1rBoxlwM3r4ZYTT2Kw
KSeQRLObFhu0XZjW6QpFMMwgjclA/dXepwn7iDaxko916xqInt7Xu/HVZMSxX0BY
41XavBrxG01dyaXERWAdgJjQsJVf8A6Hg+LpzKHrIe6Gseys/1QstgZSU5Z/dsq
cJAc2REncvg+QQJkRPba3hLCFaurf68eyKgN3wDPwHLGo8mD2GfbQ290LPqBwcRn
qyTb10a495NPT15w9Tk740TulxMVCCPtjiMX1VzDfLKqYV7K+SzEKDJpF3mgNtX3
W5cJXLbStgVeaf78tgxeZUHsUuZMMgAHqPcKaKBZjGp7jiZTcU5cyHe1bxuQ4op5
KHvpGiJf7JysUUU8sYz7IH/aBNk3EJg8NcbLYffGjEjcv+uSjQPLz0+3Zst5y4/r
VqnG+3bv0C1mYMdEVEHSrIMcR+TMABUOFXsNzLpVBxW8+Umz+YaqefGibg98dunT
1FC3B/IB4Qc/vQN05bi2fWfVuEEqdWLEUV/fE/pUAXndPbZUGk1+faJ8/8HhN1yH
0Ah+KdWHBUrNFow0r8CqCYF+15+18LVBtp61SSHIhK47161p9SgJKYJLU6fm0K6q
rHbkj82u8CBHbcY7QJQg6FLbhDY2+jBQIG37mxRGT+N+8NkfW4ec4IuzVQk1RWq/
M/RdKZf6UpXc9Eud9YhU15/k50pDfMbvqm4Bot59zy/NgtijcQE01GTiFMHwr82
XnUKezYGSspQZFj8Dbi+5Xx2RC1FBwMDaJIYdEFU7telUJqo7kLze3ouHh/qoh0qh
oyjxgwzG3MTmv6NNf0dsp60Ik78vGfDXhHBY3wGIx6pNfrLJdW+VSiSvPYTiMqAp
8Uhl17xWbGeFI3UuqqcYoFbnQci/WAK7G/J2veY51GvV5dLvrB2Rig4MRsbGp21G
F1GaJV2Jav0FYdV4TYcJm+Ub7U1r0FqTkfZexRzuJHouNwcmWDaRpnC0U86tcPUM5
z133jnp1cEKbc+4TgsVGo6CRt1Qq9MFfLZdY3d7Sbs93IFn6tm/DbV20nQGrHdHe
ZbDTjTXZqmuwxhrsA/7zPdUavMIKTBa+MJx0rcrQQkFJYGnaOCM7gogrKiynaQF2
yCVSFUBLEjF+1XdImTf1Sm123myZP3sR16Hw/Cz8FLi1jBwJ+2CEi9bosk3CnYWz
InFDFF9QUFVXZu60C2293WCXLdr+udBadN40kkaL8aoTn4HFkwDL152aXTCXpm
EPnJK++2V00H6C1B42KR261uxFhcuG+KuxorrGyn6Ppzi1k5T1HTrMIrVSHczI2w
xUyreg0Dj0dgeppDCsQ0IaQDLBoIKEYz52TRK+3ztX6Kt0reKcoV/AxXnAdeydk5
EtnkMSj+XK75NSuDRVv+IJu3GVBezmFY01TdNa3HgZLwNpIkLZhhQx8BebRY0WYC
vXfAU51+fDXHoKf6v2r+djWjWuzfkQsnezHDtPBr1YMNYkPJd+KwBP1UvkPIV71i
7RcUcRuyXXJixmA38jPwSEitHI1DcROMENyZqn/d0igztzv/rhgMj/8CM1ZxRCUn
xdfZB601aJLQCnkAvd0SRD0jdG9FoyPZVXD2tBCo6w0sZ53mMTUuHkxLdESrhBs
eiblg8KekqEAcej9XqZpPzjyXjxVH6ZqW126I3e11Rvm23d4DGA3mVMI5i+2+QDj
7zm62mfJ3FEmpbjR4TUbhHw/QzXYxBzRjQkiXmPv7Y4T+Ws0WkrsH9BUEQEomR57
Sf81rmSbcQ2JdkEq1SMNFqtAuVNHJm1kNz0f9w10uoVih2BQB33pnyugheUL6Gy5
c/SjrP+F6Tpy4vDkxqgdglerwIzkDFvUH3o6uekRW+QP7G/CafIay6PSF0LhctQGM
3rwCPL7szsJiLP626mY39aq39ZYsUBtKZqFG1WQS80J0cfayZR01VX6ABHneqFJm
woEimkTxxxyEbnclW9ij8Ln1iKaWgvumLTee09d5Zwponu0ceXn6HLnkJBwwQQpoh5
IEahmwqtWnFuZ8mkxwb10mhESYf10y9mybT5Hb/zVBkHsrUyWwXhr8PiDoN+mjn
LI1pu5M10CFxWkVs80B8tgb1DkeuCKIH1ttI7gxs2bs2Rak6mrMiNo4HvN0pJ8G
h0YSLnkhTFwM74GdYF16Ncnv5MLU9kBrIyjTkrFRO/SLLW/RSYXaZZJ+g1hHIjg64
6h2FH38bzK7X6WekMDZ80HR83JLCxKXJDYhTUp2B2QM6bA3IOVfkPSsNk2diMS8/
1C8D+Dp/wJtbjpc9V+kygV5gRoBX5SFvLFuTBjNfzLYJdsdsf5aoU0bDqFZq3iWM
```



Shell

```
Shell - Konsole <3>
Session Edit View Bookmarks Settings Help

rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any
assurances of licenses to be made available, or the result of an
attempt made to obtain a general license or permission for the use
of such proprietary rights by implementers or users of this
specification can be obtained from the IETF on-line IPR repository
at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention
any copyrights, patents or patent applications, or other
proprietary rights that may cover technology that may be required
to implement this standard. Please address the information to the
IETF at ietf-ipr@ietf.org.

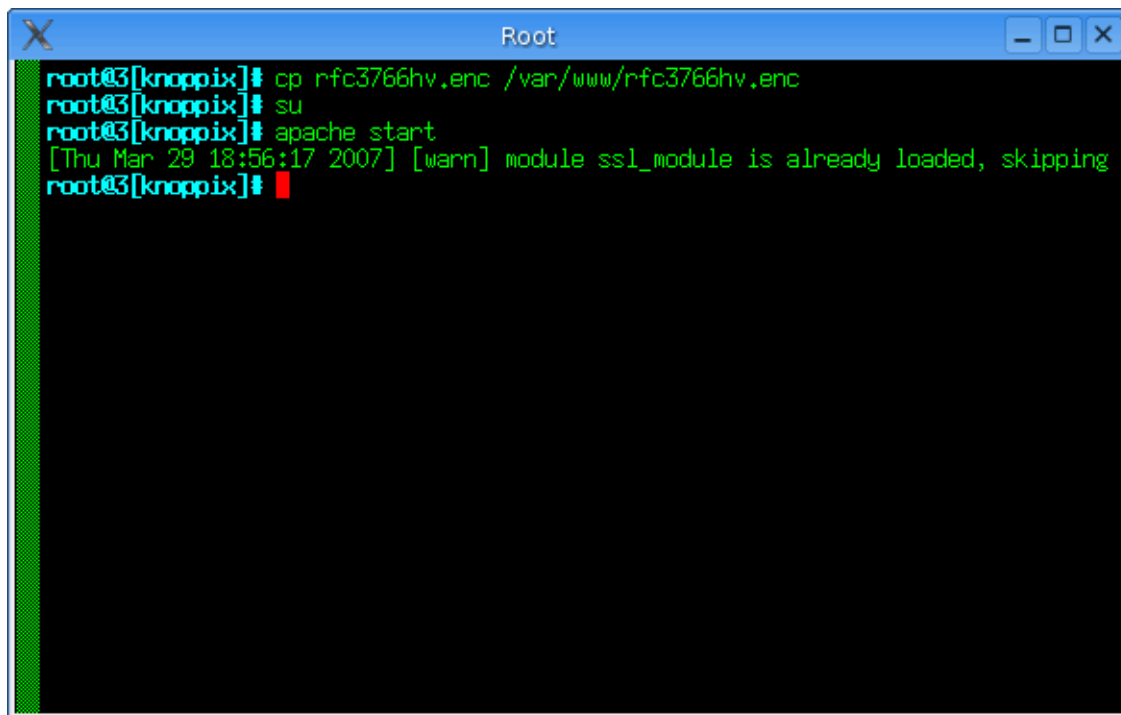
Acknowledgement

Funding for the RFC Editor function is currently provided by the
Internet Society.

Orman & Hoffman                Best Current Practice                [Page 23]

knoppix@2[knoppix]$ openssl md5 rfc3766hv.txt
MD5(rfc3766hv.txt)= 046d557e7127a9fcfaa9d016d130fd80
knoppix@2[knoppix]$ openssl md5 rfc3766hv.dec
MD5(rfc3766hv.dec)= 046d557e7127a9fcfaa9d016d130fd80
knoppix@2[knoppix]$ ls -l
total 204
lrwxrwxrwx  1 knoppix knoppix    9 Mar 29 18:33 AdobeFnt.lst -> /dev/null
drwxr-xr-x  2 knoppix knoppix  200 Mar 29 18:50 Desktop
-rw-r--r--  1 knoppix knoppix   56 Mar 29 18:41 des_keyXX
-rw-r--r--  1 knoppix knoppix   56 Mar 29 18:42 des_keyhv
-rw-r--r--  1 knoppix knoppix 55939 Mar 29 18:49 rfc3766hv.dec
-rw-r--r--  1 knoppix knoppix 75782 Mar 29 18:45 rfc3766hv.enc
-rw-r--r--  1 knoppix knoppix 55939 Mar 29 18:40 rfc3766hv.txt
drwxr-xr-x  2 knoppix knoppix   40 Apr 19 2004 tmp
knoppix@2[knoppix]$
```

**We used the root user to start the Apache service**

A terminal window titled "Root" with a blue header bar. The window contains a series of shell commands and their outputs. The commands are: `cp rfc3766hv.enc /var/www/rfc3766hv.enc`, `su`, and `apache start`. The output for the `apache start` command is: `[Thu Mar 29 18:56:17 2007] [warn] module ssl_module is already loaded, skipping`. The prompt `root@3[knoppix]#` is visible at the end of each line.

```
root@3[knoppix]# cp rfc3766hv.enc /var/www/rfc3766hv.enc
root@3[knoppix]# su
root@3[knoppix]# apache start
[Thu Mar 29 18:56:17 2007] [warn] module ssl_module is already loaded, skipping
root@3[knoppix]#
```

**We had also used Ethereal to capture the packets as we were transferring the files between the partners.**

eth0: Capturing - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: ip.addr == 129.7.236.174

| No. | Time       | Source        | Destination   | Protocol | Info                |
|-----|------------|---------------|---------------|----------|---------------------|
| 575 | 104.128014 | 129.7.236.174 | 129.7.236.234 | ICMP     | Echo (ping) request |
| 576 | 104.128041 | 129.7.236.234 | 129.7.236.174 | ICMP     | Echo (ping) reply   |
| 579 | 105.130533 | 129.7.236.174 | 129.7.236.234 | ICMP     | Echo (ping) request |
| 580 | 105.130557 | 129.7.236.234 | 129.7.236.174 | ICMP     | Echo (ping) reply   |
| 583 | 106.132302 | 129.7.236.174 | 129.7.236.234 | ICMP     | Echo (ping) request |
| 584 | 106.132326 | 129.7.236.234 | 129.7.236.174 | ICMP     | Echo (ping) reply   |
| 588 | 107.134070 | 129.7.236.174 | 129.7.236.234 | ICMP     | Echo (ping) request |
| 589 | 107.134095 | 129.7.236.234 | 129.7.236.174 | ICMP     | Echo (ping) reply   |
| 592 | 108.135838 | 129.7.236.174 | 129.7.236.234 | ICMP     | Echo (ping) request |
| 593 | 108.135864 | 129.7.236.234 | 129.7.236.174 | ICMP     | Echo (ping) reply   |

> Frame 575 (98 bytes on wire, 98 bytes captured)  
 > Ethernet II, Src: DellPcba\_be:ce:22 (00:0d:56:be:ce:22), Dst: 129.7.236.234 (00:0d:56:be:d0:11)  
 > Internet Protocol, Src: 129.7.236.174 (129.7.236.174), Dst: 129.7.236.234 (129.7.236.234)  
 > Internet Control Message Protocol

```

0000  00 0d 56 be d0 11 00 0d 56 be ce 22 08 00 45 00  ..V....V..."..E.
0010  00 54 00 00 40 00 40 01 5f 01 81 07 ec ae 81 07  .T...@. @. ....
0020  ec ea 08 00 c4 44 b3 1f 00 00 46 0c 55 e9 00 0e  ....D...F.U...
0030  f9 94 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  ..
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..!#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  ..()*)+,-./012345
  
```

eth0: <live capture in progress> File: /tmp/etherXXXXPSGZcZ 117 KB P: 840 D: 10 M: 0

**Here you can see where one of our partners after they exchanged the des\_key, and verified the hash.**

```
-rw-r--r-- 1 knoppix knoppix 56 Mar 29 18:41 des_keyXX
-rw-r--r-- 1 knoppix knoppix 56 Mar 29 18:42 des_keyhv
-rw-r--r-- 1 knoppix knoppix 75782 Mar 29 19:09 rfc3766PH.enc
-rw-r--r-- 1 knoppix knoppix 55939 Mar 29 18:49 rfc3766hv.dec
-rw-r--r-- 1 knoppix knoppix 75782 Mar 29 18:45 rfc3766hv.enc
-rw-r--r-- 1 knoppix knoppix 55939 Mar 29 18:40 rfc3766hv.txt
drwxr-xr-x 2 knoppix knoppix 40 Apr 19 2004 tmp
root@5[knoppix]# openssl des -d -a -kfile des_keyPH -in rfc3766PH.enc -out rfc3766PH.dec
root@5[knoppix]# openssl md5 rfc3766PH.txt
rfc3766PH.txt: No such file or directory
root@5[knoppix]# ls -l
total 1004
lrwxrwxrwx 1 knoppix knoppix 9 Mar 29 18:33 AdobeFnt.lst -> /dev/null
drwxr-xr-x 2 knoppix knoppix 280 Mar 29 19:23 Desktop
-rw----- 1 root root 663138 Mar 29 19:21 Part 1A
-rw-r--r-- 1 root root 56 Mar 29 19:20 des_keyPH
-rw-r--r-- 1 knoppix knoppix 56 Mar 29 18:41 des_keyXX
-rw-r--r-- 1 knoppix knoppix 56 Mar 29 18:42 des_keyhv
-rw-r--r-- 1 root root 55939 Mar 29 19:24 rfc3766PH.dec
-rw-r--r-- 1 knoppix knoppix 75782 Mar 29 19:09 rfc3766PH.enc
-rw-r--r-- 1 knoppix knoppix 55939 Mar 29 18:49 rfc3766hv.dec
-rw-r--r-- 1 knoppix knoppix 75782 Mar 29 18:45 rfc3766hv.enc
-rw-r--r-- 1 knoppix knoppix 55939 Mar 29 18:40 rfc3766hv.txt
drwxr-xr-x 2 knoppix knoppix 40 Apr 19 2004 tmp
root@5[knoppix]# openssl md5 rfc3766hv.txt
MD5(rfc3766hv.txt)= 046d557e7127a9fcfaa9d016d130fd80
root@5[knoppix]# openssl md5 rfc3766PH.dec
MD5(rfc3766PH.dec)= 046d557e7127a9fcfaa9d016d130fd80
root@5[knoppix]#
```

