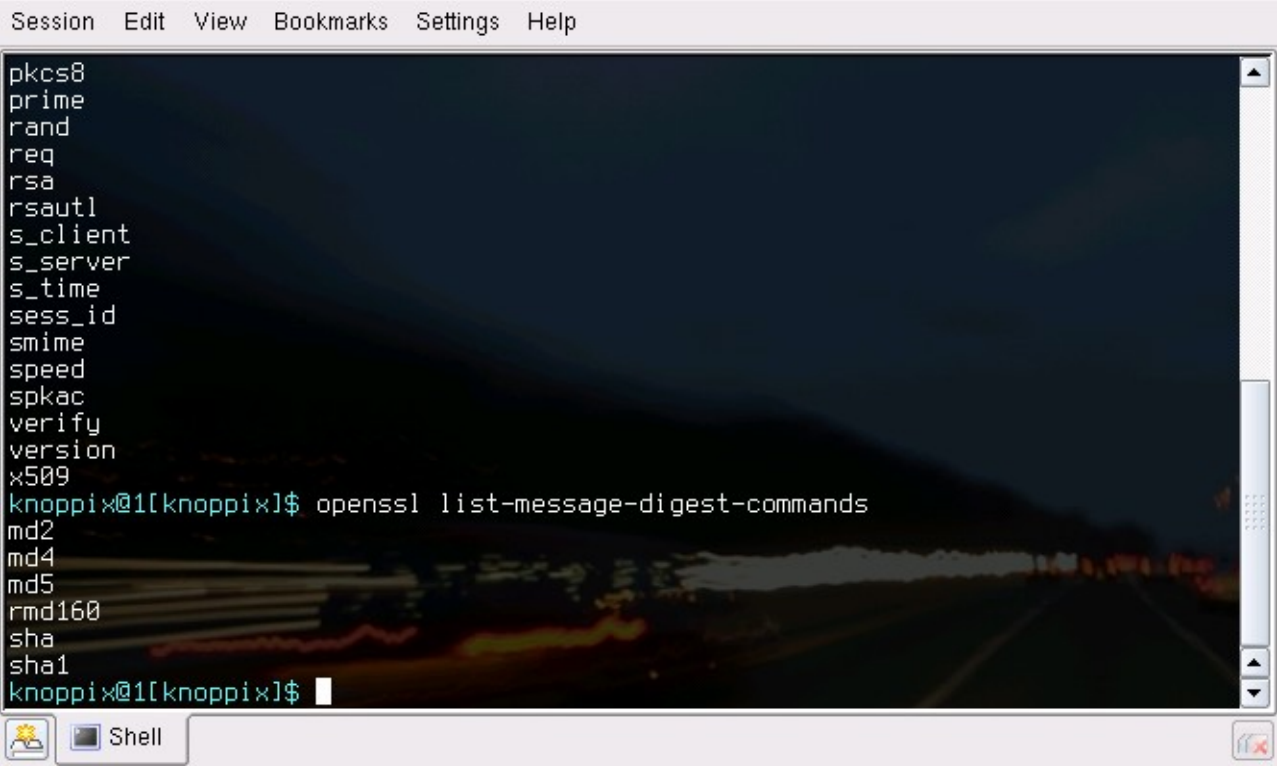


Cryptography Lab

This was a lab involving some of the basics of cryptography.

```
openssl list-standard-commands
```

```
openssl list-message-digest-commands
```

A screenshot of a terminal window with a dark background and a light-colored border. The window title bar includes a menu with 'Session', 'Edit', 'View', 'Bookmarks', 'Settings', and 'Help'. The terminal content shows a list of OpenSSL commands: pkcs8, prime, rand, req, rsa, rsautl, s_client, s_server, s_time, sess_id, smime, speed, spkac, verify, version, and x509. Below this list, the command 'openssl list-message-digest-commands' is entered, resulting in a list of message digest commands: md2, md4, md5, rmd160, sha, and sha1. The prompt 'knoppi@1[knoppi]\$' is visible at the end of the command line and again at the bottom of the terminal. The window's taskbar at the bottom shows a 'Shell' icon and standard window controls.

```
openssl ciphers -v -ssl3
```

```

Session Edit View Bookmarks Settings Help
rc4-40
knoppix@1[knoppix]$ openssl ciphers -v -ssl3
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-DSS-AES256-SHA SSLv3 Kx=DH Au=DSS Enc=AES(256) Mac=SHA1
AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
EDH-RSA-DES-CBC3-SHA SSLv3 Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
EDH-DSS-DES-CBC3-SHA SSLv3 Kx=DH Au=DSS Enc=3DES(168) Mac=SHA1
DES-CBC3-SHA SSLv3 Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-DSS-AES128-SHA SSLv3 Kx=DH Au=DSS Enc=AES(128) Mac=SHA1
AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
DHE-DSS-RC4-SHA SSLv3 Kx=DH Au=DSS Enc=RC4(128) Mac=SHA1
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
EXP1024-DHE-DSS-DES-CBC-SHA SSLv3 Kx=DH(1024) Au=DSS Enc=DES(56) Mac=SHA1 export
EXP1024-DES-CBC-SHA SSLv3 Kx=RSA(1024) Au=RSA Enc=DES(56) Mac=SHA1 export
EXP1024-RC2-CBC-MD5 SSLv3 Kx=RSA(1024) Au=RSA Enc=RC2(56) Mac=MD5 export
EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH Au=RSA Enc=DES(56) Mac=SHA1
EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH Au=DSS Enc=DES(56) Mac=SHA1
DES-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1
EXP1024-DHE-DSS-RC4-SHA SSLv3 Kx=DH(1024) Au=DSS Enc=RC4(56) Mac=SHA1 export
EXP1024-RC4-SHA SSLv3 Kx=RSA(1024) Au=RSA Enc=RC4(56) Mac=SHA1 export
EXP1024-RC4-MD5 SSLv3 Kx=RSA(1024) Au=RSA Enc=RC4(56) Mac=MD5 export

```

www.OpenSSL.org

File Edit View Go Bookmarks Tools Help

http://www.openssl.org/

CD-Inhaltsverzei... KNOPPIX - Webse...

Google Docs & Spreadsheets (All) OpenSSL: The Open Source tool...

OpenSSL

- Title
- FAQ
- About
- News
- Documents
- Source
- Contribution
- Support
- Related

Welcome to the OpenSSL Project

The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and **Open Source** toolkit implementing the **Secure Sockets Layer** (SSL v2/v3) and **Transport Layer Security** (TLS v1) protocols as well as a full-strength general purpose cryptography library. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation.

OpenSSL is based on the excellent SSLeay library developed by Eric A. Young and Tim Hudson. The OpenSSL toolkit is **licensed** under an Apache-style licence, which basically means that you are free to get and use it for commercial and non-commercial purposes subject to some simple license conditions.

Why buy a **SS** toolkit a black-box you can get open one for free

http://www.opensource.org/

```
Session Edit View Bookmarks Settings Help
drwxr-xr-x  4 knoppix knoppix   140 Mar 29 17:58 .kde
-rw-r--r--  1 knoppix knoppix   409 Jun 28  2002 .kderc
drwxr-xr-x  2 knoppix knoppix   100 Aug 28  2005 .links
drwxr-xr-x  3 knoppix knoppix    60 May  3  2004 .local
drwxr-xr-x  2 knoppix knoppix    60 Mar 29 17:58 .mcp
drwxr-xr-x  4 knoppix knoppix   100 Aug 28  2005 .mozilla
-rw-r--r--  1 knoppix knoppix   752 Dec 16  1999 .nessusrc
drwxr-xr-x  5 knoppix knoppix   140 Mar 29 17:58 .netscape
drwxr-xr-x  2 knoppix knoppix   160 Mar 29 17:58 .qt
drwx----- 4 knoppix knoppix    80 Mar 29 18:19 .thumbnails
drwxr-xr-x  2 knoppix knoppix    80 Aug 28  2005 .xine
-rw-----  1 knoppix knoppix   1513 Mar 29 18:44 .xsession-errors
-rw-r--r--  1 knoppix knoppix  64908 Mar 29 18:28 1a.png
-rw-r--r--  1 knoppix knoppix  81752 Mar 29 18:30 1b.png
-rw-r--r--  1 knoppix knoppix 190061 Mar 29 18:32 1c.png
lrwxrwxrwx  1 knoppix knoppix    9 Mar 29 18:36 AdobeFnt.lst -> /dev/null
drwxr-xr-x  2 knoppix knoppix   160 Mar 29 18:44 Desktop
-rw-r--r--  1 knoppix knoppix 1466246 Mar 29 18:37 fips1402.pdf
-rw-r--r--  1 knoppix knoppix  55939 Mar 29 18:42 rfc3766hp.txt
drwxr-xr-x  2 knoppix knoppix    40 Apr 19  2004 tmp
knoppix@1[knoppix]$ openssl rand -out des_keyhp 56
knoppix@1[knoppix]$ cat des_keyhp
óç
+%l'æ½àWbu, ßè<[ü9.!fâpG³HùpKäÜø`ø×ð7kál+«bÉ!jknoppix@1[knoppix]$
```

List encrypted file

cat rfc3766hp.enc

```
/H+XiLDMF6fYp12ok1mbjbe5pq5FbHsLH20ciZGoSYJoDcQ0QdWlCTJHBw5PBqRH
WBCNBvK04JHJWu229Y3HsbmB23/h/yWxfhc1g0562hQi amEIbxT0dW4Avk291mJEJ
1x28tgVQamGACdmy4oxtwI2mZ0/HRL9YSAX0LzZ7fngTYeGaRtc1BTb5x0Aw00/n
iMUfiXb2hvX0PoVN9T6JAGC1eUy0133sLH0uHqDDH4rXLfn3/0eeMskOKR8c9KVZ
jtf85C0HpLmScZpjm/x1024mk1nwi jys0Yx6sE89p65B75DyELRnKrCUK1 duIT1b
mGgZa1+wVF1T8WdUX+y1Y0zlvEECyay85/e5o06JRjqS91QJpiv31XAdPs9M10nu
+6cv4Y/tEY3+i169oc7AziCeFaIwXrWdYeUGQCJ1f+LqRN1tqF0frfFpos0He/Ij
j1p1u9tY50Xv0gSosyvKRDunNyUYojGal3jEXk85ulbBezsh8R2JU0wpXA+Fbq1T
WJIxluhI0krSTtzaURK3r0xKXH3KtE8NRwhT+H5p/XUYAKM1aRtEsUjiZk2+qDLx
rDptjIL3ZoxMdSAb9grud/TCsmlapLP1a8sGNLktJef096iQq3Ac1mPSNHfZkXp
JG7FToGR63m/swCYns6zn/vFA+TjHYiyw8nBVI BuzkEwGyhSKFs1HKt12G1daLk1
z9e7/hKnI5reCHh3xV5BEa/3F4ku8Pi q6cSa7BE1s0UaU3HN6si t83Xxb0IA9wdx
/BGNNTQ0dBppYxqYZ1ekXQuCC7RCw2qd41s1TEa4NCdZ90ZRO3fxQsK87bDdQ1/
+5fy/SHVAF0AZALQjPv4IKLGLFqmCPw5C4cNI NwZGqf0drdrs8VAuWrvjlg2eYL
gySkrTE6RH+i x50xub4vUcWoNcb6jNd8mwf16uofDi oSh07Fg108gUrMf60LDQe4
zGTHBSKPEdMKPCnbCw8qZ1jVWRgiwDFitZ1n0nuyumLZhfgACiz66rWjW3qUpvVK
YfABun3EsR/vVfpYxAjvQ58hsqCYVvd7y0Za1qbdofj+XK71c7ka0BCEcyv96Q6
gJexJBG2yGfyjiH1Gx+JJ8Yz2YN64FPYgG8WJWE2iNB2TvBxR+xRt8QI80A4/u
F0xWbfbuKeskgy1XcgnXHwT21QWnpHzE/54dsggLuJbxWszKHEITmUuGWxSMq3
e8C7wojaz0pPLM/12tMez1Fz15uPrvcv+AG/7917oqDUf5P9qVqPUIx0JDcnMvB3z
6jnvY4ndu1xApVzHnnVEQGVA5E+DHAor5vp6xvYb9y+w1jjGopC61YCckIQY20mI
QjvZDjaYP/1JFelxN6rSYPCF8TRILy//T7rqDUNQXqJ9gi377/oyjsoespWibej
LoqeBV47XGbhj0kEDI4JiRNT/VWwHs1zU1wun9xTznnoySU4UTaE+pBB02rCp2F
87hiF7faglDVS87hMtymbj40Sng4n54mk03Y622kN6AME9o6TaN0uaVuusiFJ5Gg
MtXhfI2Pp4yMCLXbnWepZArRjv1GxUZSYjtfR10nPuZd/MzNNQwF9h120+xLJWsb
UPqblkqLe+g6Bs07A2UMUzMNHUKQPH4yKpZWLWHTHaD/X3QzhTo7jhSarkSZSHUJ
y11d74LTt5n0ARdPERcqZnp1JdQbaj4MFir1CjKxhUCIvQVwfbpeMpyFfEcCZZJf
iT0yp9vdXYkZqTFK1cyJTXdW3RmiB3P6QKuy5jRWg1VumI1PM/t14VqAQR Iexb4F
ApUsIUE30Upw7kWzA+qhYBp8PudyQtqVk0H+tv0/v6A18t99o3bqVJMqKxZ8w11Q
I4Xuj+X9somKn7gzm2UilvpupGVhHvDLI2++Q41F5sw7I8ZTIhc6kTDK5GipsJcm
PeSsnXPYwgMk9tXz0no8ihXdSz+07+KrbPjfbT38DANfE89kInhXiUYtWFacLHjv
qRLzbCTJbrt2bjWxmT6qW6S/vi2V8F2t0pNJR6PBMKQyp14IoK8xxo2dKLDKpsBv
G+AS70RIRt4N7IdmRCVYgDL5QNpv5/AMh89afNvvBqcT10oUIpiEQ4+mNMIi1qJ0
aZIKgRPy1ImM924jVvR4KjkCN983YRmNi qhtK45cJ9gQ9gUdDFVbGP+P4J5NW3SL
8fk5aT8xAnIxcnXk1cldqMeGas0t1kVX1thfi af5rtgJvFVM23D9nwuaIiFUyaWw
8jZmspqp7G3Ue1qz+hJihknrvFH4+1YI2U1dGgWkaxBwV+HJWLzeZ0/ibfi/CjrA
4fQC0rMM+CPnwKbGVDut6QqGuCncqjEyZsPTZSGVKjMCCGtxk8HP1X0/aBQCytWn
Mi0v+QrA2qV1XPL9aaY9iCajrsgbsqF0/9PG1wBFYKhURmyy3jrwD1JAN2HBu8DB
LeEq/ZV9EoUsI1pG/0079t3fLdBXDLdEtU/x9aB/M4Y508Lbdq40hHroW6iDB+Wo
B8YsT5WQXckth/N3U6o2KVM9u64c6mDb05SVZck5j3+2i7rmpXW3w0eD111qEXWn
X+0A+gQPC1YcB131omr1oc1NHYK1azx+g0h30/nfSiQJA0CH0GIef49EkLdkDnyJ
qUwW01xP/Bp+7baWjEFTnJnQ2m7sm+dsxVhw/6N6Q5HVWuT5IKjN08euNPSRNLId
G4vdr3QkU0SdiVhVC/YwaWbcQJm31U+UmLzD5do6LdfXnVjti/ifiqKfBXf8IiWwE
DQJDz2P2m4fG2tVKe+T035pz0DszVWHP2xPS4UA0tHYU99gAjDRjyaLDAWnDqZJR
wWj60Qb6kDvohYcrRF0ao5Y08Ude1w2YGKW9oXS4AydnBHJIvIX7/w==
knoppix@1[knoppix]$
```

Alpha 500 MHz compiled with Digital's C compiler, optimized, no platform specific code:

group	modulus	exponent	time
type	size	size	
mod	768	~150	12 msec
mod	1024	~160	24 msec
mod	1536	~180	59 msec
ecn	155	~150	20 msec
ecn	185	~200	27 msec

The following two tables (computed by Eric Young) were originally for RSA signing operations, using the Chinese Remainder representation. For ease of understanding, the parameters are presented here to show the interior calculations, i.e., the size of the modulus and exponent used by the software.

Dual Pentium II-350:

equiv	equiv	equiv
modulus	exponent	time
size	size	
256	256	1.5 ms
512	512	8.6 ms
1024	1024	55.4 ms
2048	2048	387 ms

KNOPPIX
Dipl.-Ing. Klaus Knopper

Alpha 264 600mhz:

equiv	equiv	equiv
modulus	exponent	time



Shell



Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to 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.

KNOPPERNET

```
knoppi@1[knoppi]$ openssl md5 rfc3766hp.txt
MD5(rfc3766hp.txt)= 046d557e7127a9fcfaa9d016d130fd80
knoppi@1[knoppi]$ openssl md5 rfc3766hp.dec
MD5(rfc3766hp.dec)= 046d557e7127a9fcfaa9d016d130fd80
knoppi@1[knoppi]$ █
```



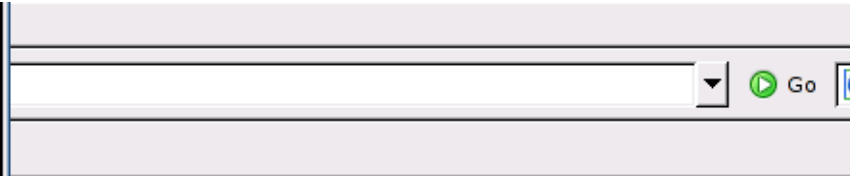
Shell



Start Apache

```
root@1[knoppix]# cp rfc3766hp.enc /var/www/rfc3766hp.enc
root@1[knoppix]# su
root@1[knoppix]# apache start
[Thu Mar 29 19:03:52 2007] [warn] module ssl_module is already loaded, skipping
root@1[knoppix]# █
```

Placeholder Page



Welcome to Your New Home in Cyberspace

This is a placeholder page installed by the [Debian](#) release of the [Apache](#) Web server package, because no home page was installed on this host. You may want to replace this as soon as possible with your own web pages, of course....

This computer has installed the Debian GNU/Linux operating system but has nothing to do with the Debian GNU/Linux project. If you want to report something about this host's behaviour or domain, please contact the ISPs involved directly, **not** the Debian Project.

See the [Network Abuse Clearinghouse](#) for how to do this.

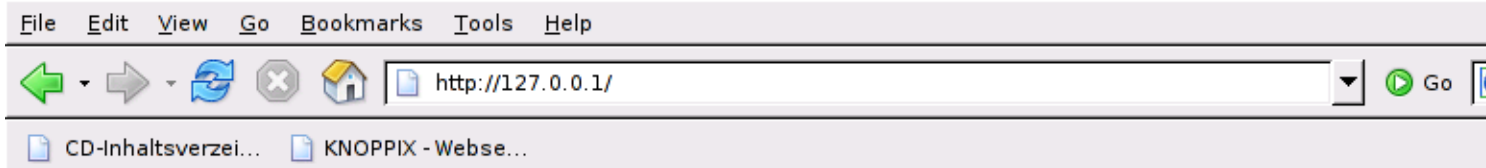
Unless you changed its configuration, your new server is configured as follows:

- Configuration files can be found in `/etc/apache`.

Done



Edited Home Page using Apache



Heber Paz

- Configuration files can be found in `/etc/apache`.
- The DocumentRoot, which is the directory under which all your HTML files should exist, is set to `/var/www`.
- CGI scripts are looked for in `/usr/lib/cgi-bin`, which is where Debian packages will place their CGI scripts.
- Log files are placed in `/var/log/apache`, and will be rotated daily. The frequency of rotation can be changed by editing `/etc/apache/cron.conf`.
- The default directory index is `index.html`, meaning that requests for a directory `/foo/bar/` will return the contents of the file `/var/www/foo/bar/index.html` if it exists (assuming that `/var/www` is your DocumentRoot).
- User directories are enabled, and user documents will be looked for in the `public_html` directories of users' homes. These dirs should be under `/home`, and users will not be able to symlink to files they don't own.

All standard Apache modules are available with this release and can be chosen with the `apachectl` command. Installing a new module on your system is just a matter of compiling it (with the `apache-dev` package) and adding a line to your `httpd.conf` configuration file.

More documentation on Apache can be found on:

- The [RFC3766hp](#) stored on your server.
- The [Apache Project](#) home site.
- The [ApacheWeek](#) newsletter.
- The [Debian Project Documentation](#) which contains HOWTOs, FAQs, and software updates.

Done

Exchange of decrypted files (des_keyhp, des_keyrm)

