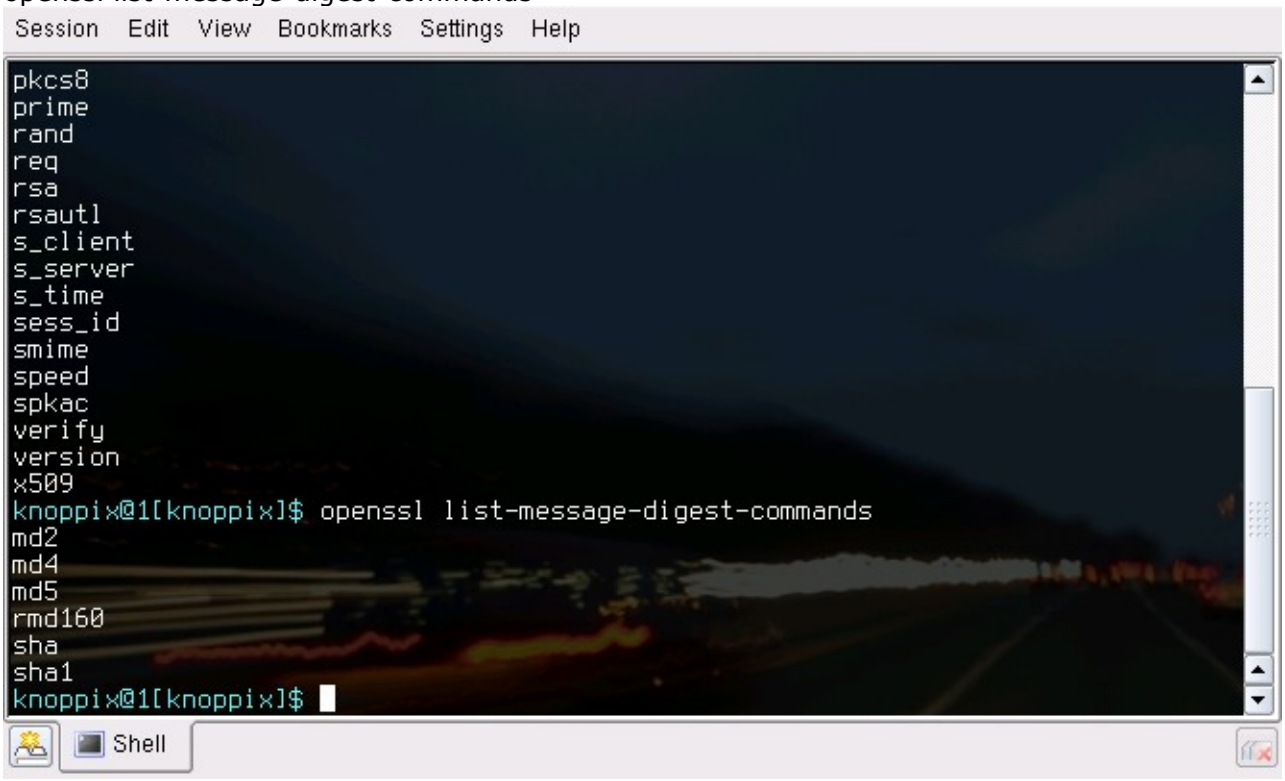
Cryptography Lab

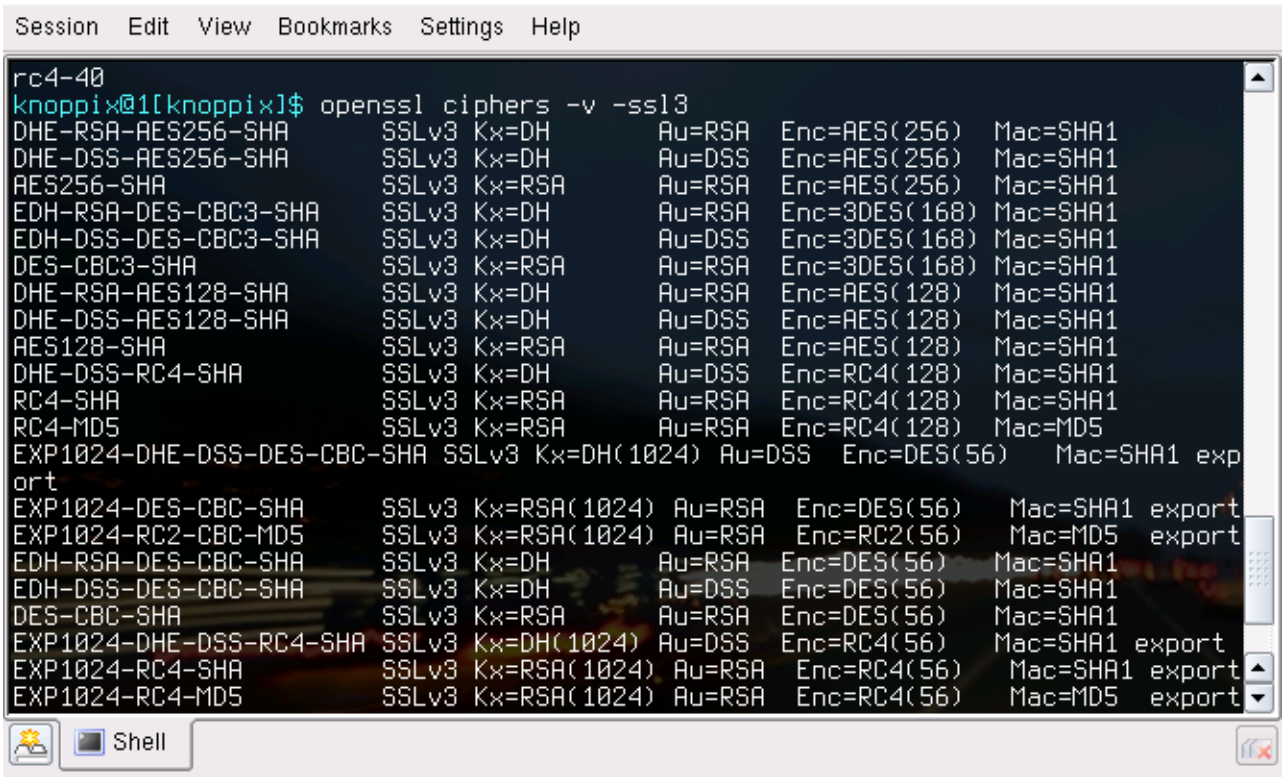
This was a lab involving some of the basics of cryptography.

openssl list-standard-commands

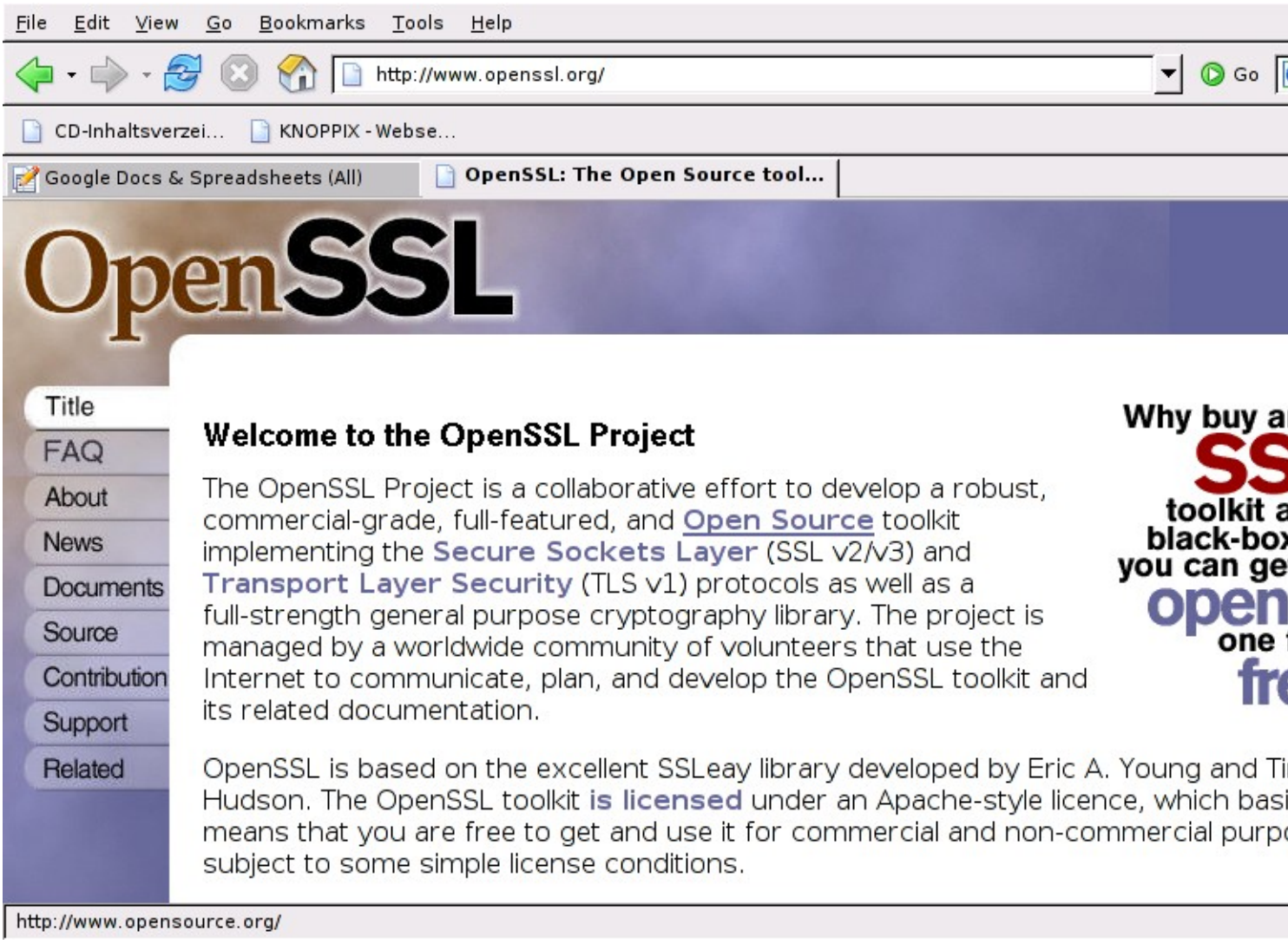
openssl list-message-digest-commands

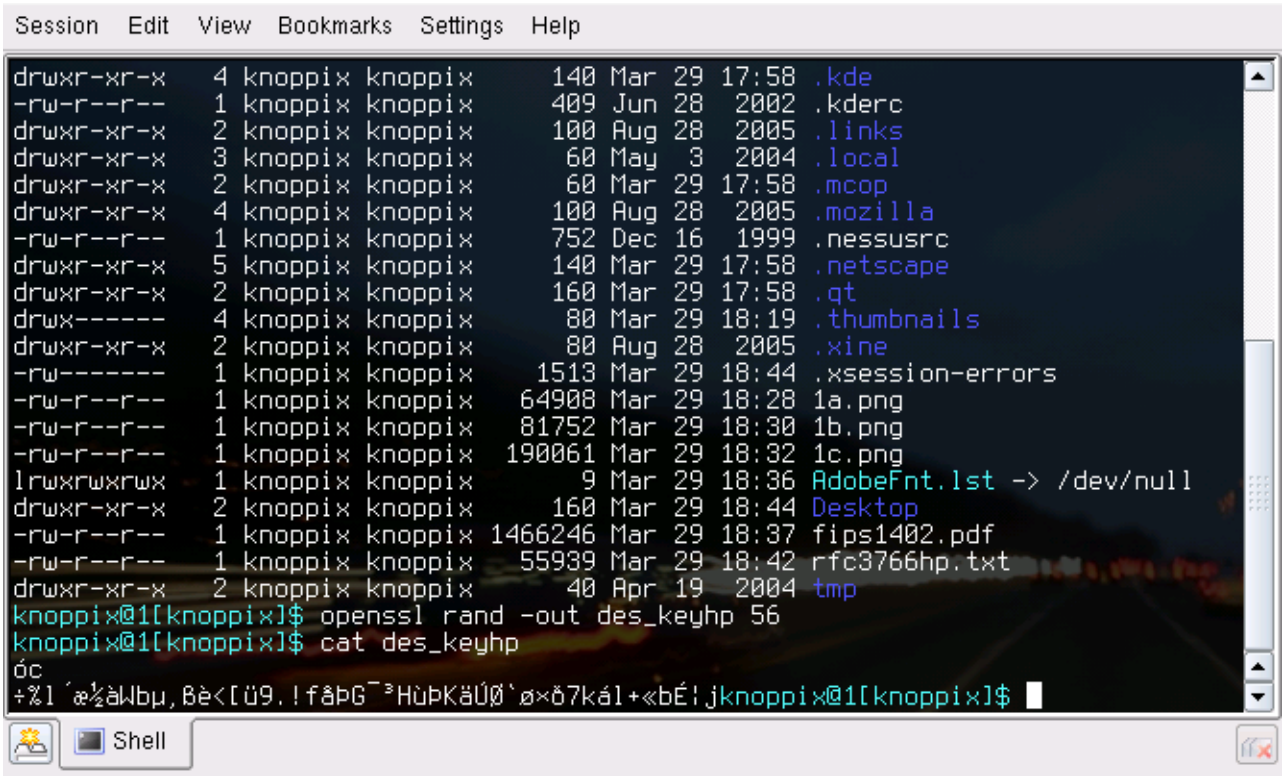


openssl ciphers -v -ssl3



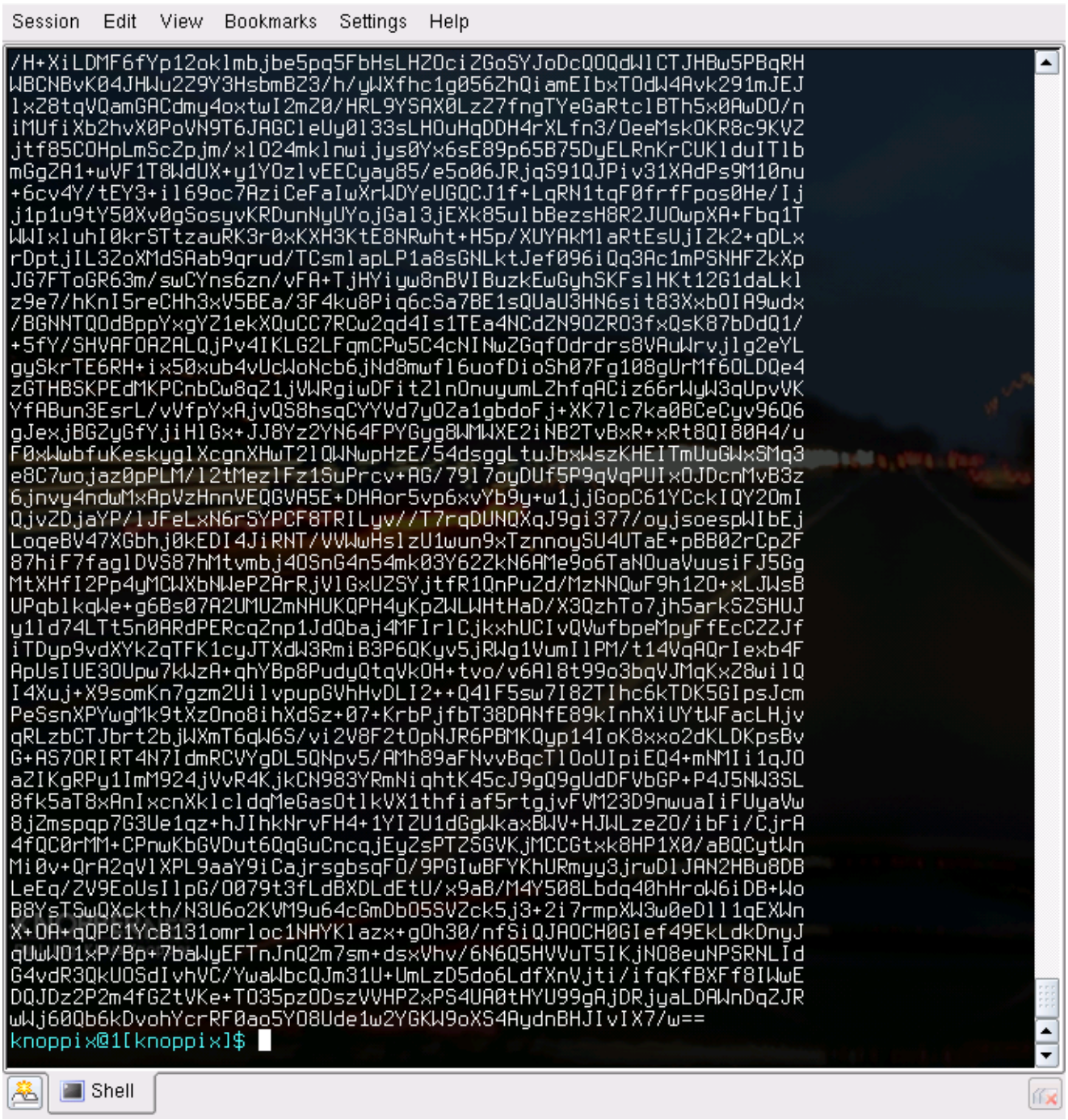
www.OpenSSL.org





List encrypted file

cat rfc3766hp.enc


Session Edit View Bookmarks Settings Help
/H+XiLDMF6fYp12oklmbjbe5pq5FbHsLHZOciZGoSYJoDcQOQdWlCTJHBw5PBqRH
WBCNBvK04JHWu2Z9Y3HsbmBZ3/h/yWXfhc1g056ZhQiamEIbxTOdW4Avk291mJEJ
lxZ8tqVQamGACdmy4oxtwI2mZ0/HRL9YSAX0LzZ7fngTYeGaRtclBTh5x0AwDO/n
iMUfiXb2hvX0PoVN9T6JAGCleUy0l33sLHOuHqDDH4rXLfn3/OeeMskOKR8c9KVZ
jtf85COHpLmScZpjm/xlO24mklnwijys0Yx6sE89p65B75DyELRnKrCUKlduIT1b
mGgZA1+wVF1T8WdUX+y1YOzlvEECyay85/e5o06JRjqS91QJPiv31XAdPs9M10nu
+6cv4Y/tEY3+il69oc7AziCeFaIwXrWDYeUGQCJ1f+LqRN1tqF0frfFpos0He/Ij
j1p1u9tY50Xv0gSosyvKRDunNyUYojGal3jEXk85ulbBezsH8R2JUOwpXA+Fbq1T
WWIxluhI0krSTtzauRK3r0xKXH3KtE8NRwht+H5p/XUYAkM1aRtEsUjIZk2+qDLx
rDptjIL3ZoXMdSAab9qrud/TCsmlapLP1a8sGNLktJef096iQq3Ac1mPSNHFZkXp
JG7FToGR63m/swCYns6zn/vFA+TjHYiyw8nBVIBuzkEwGyhSKFslHKt12G1daLkl
z9e7/hKnI5reCHh3xV5BEa/3F4ku8Piq6cSa7BE1sQUaU3HN6sit83XxbOIA9wdx
/BGNNTQOdBppYxgYZ1ekXQuCC7RCw2qd4Is1TEa4NCdZN9OZRO3fxQsK87bDdQ1/
+5fY/SHVAFOAZALQjPv4IKLG2LFqmCPw5C4cNINwZGqfOdrdrs8VAuWrvjlg2eYL
gySkrTE6RH+ix50xub4vUcWoNcb6jNd8mwfl6uofDioSh07Fg108gUrMf60LDQe4
zGTHBSKPEdMKPCnbCw8qZ1jVWRgiwDFitZlnOnuyumLZhfqACiz66rWyW3qUpvVK
YfABun3EsrL/vVfpYxAjvQS8hsqCYYVd7yOZa1gbdoFj+XK7lc7ka0BCeCyv96Q6
gJexjBGZyGfYjiHlGx+JJ8Yz2YN64FPYGyg8WMWXE2iNB2TvBxR+xRt8QI80A4/u
F0xWwbfuKeskyglXcgnXHwT2lQWNwpHzE/54dsggLtuJbxWszKHEITmUuGWxSMq3
e8C7wojaz0pPLM/l2tMezlFz1SuPrcv+AG/79l7oyDUf5P9qVqPUIxOJDcnMvB3z
6jnvy4ndwMxApVzHnnVEQGVA5E+DHAor5vp6xvYb9y+w1jjGopC61YCckIQY2OmI
QjvZDjaYP/lJFeLxN6rSYPCF8TRILyv//T7rqDUNQXqJ9gi377/oyjsoespWIbEj
LoqeBV47XGbhj0kEDI4JiRNT/VVWwHslzU1wun9xTznnoySU4UTaE+pBB0ZrCpZF
87hiF7faglDVS87hMtvmbj4OSnG4n54mk03Y62ZkN6AMe9o6TaNOuaVuusiFJ5Gg
MtXHfI2Pp4yMCWXbNWePZArRjVlGxUZSYjtfR1QnPuZd/MzNNQwF9h1ZO+xLJWsB
UPqblkqWe+g6Bs07A2UMUZmNHUKQPH4yKpZWLWHtHaD/X3QzhTo7jh5arkSZSHUJ
y1ld74LTt5n0ARdPERcqZnp1JdQbaj4MFIrlCjkxhUCIvQVwfbpeMpyFfEcCZZJf
iTDyp9vdXYkZqTFK1cyJTXdW3RmiB3P6QKyv5jRWg1VumIlPM/t14VqAQrIexb4F
ApUsIUE3OUpw7kWzA+qhYBp8PudyQtqVkOH+tvo/v6Al8t99o3bqVJMqKxZ8wilQ
I4Xuj+X9somKn7gzm2UilvpupGVhHvDLI2++Q4lF5sw7I8ZTIhc6kTDK5GIpsJcm
PeSsnXPYwgMk9tXzOno8ihXdSz+07+KrbPjfbT38DANfE89kInhXiUYtWFacLHjv
qRLzbCTJbrt2bjWXmT6qW6S/vi2V8F2tOpNJR6PBMKQyp14IoK8xxo2dKLDKpsBv
G+AS7ORIRT4N7IdmRCVYgDL5QNpv5/AMh89aFNvvBqcTlOoUIpiEQ4+mNMIi1qJO
aZIKgRPy1ImM924jVvR4KjkCN983YRmNiqhtK45cJ9gQ9gUdDFVbGP+P4J5NW3SL
8fk5aT8xAnIxcnXklcldqMeGasOtlkVX1thfiaf5rtgjvFVM23D9nwuaIiFUyaVw
8jZmspqp7G3Ue1qz+hJIhkNrvFH4+1YIZU1dGgWkaxBWV+HJWLzeZO/ibFi/CjrA
4fQC0rMM+CPnwKbGVDut6QqGuCncqjEyZsPTZSGVKjMCCGtxk8HP1X0/aBQCytWn
Mi0v+QrA2qVlXPL9aaY9iCajrsgbsqFO/9PGIwBFYKhURmyy3jrwDlJAN2HBu8DB
LeEq/2V9EoUsIlpG/0079t3fLdBXDLdEtU/x9aB/M4Y508Lbdq40hHroW6iDB+Wo
B8YsTSwQXckth/N3U6o2KVM9u64cGmDbO5SVZck5j3+2i7rmpXW3w0eDll1qEXWn
X+OA+qQPC1YcB131omrloc1NHYKlazx+gOh30/nfSiQJAOCH0GIef49EkLdkDnyJ
qUwWO1xP/Bp+7baWyEFTnJnQ2m7sm+dsxVhv/6N6Q5HVVuT5IKjNO8euNPSRNLId
G4vdR3QkUOSdIvhVC/YwaWbcQJm31U+UmLzD5do6LdfXnVjti/ifqKfBXFf8IWwE
DQJDz2P2m4fGZtVKe+TO35pzODszVVHPZxPS4UA0tHYU99gAjDRjyaLDAWnDqZJR
wWj60Qb6kDvohYcrRF0ao5YO8Ude1w2YGKW9oXS4AydnBHJIvIX7/w==
knoppix@1[knoppix]$
Shell

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

group type	modulus size	exponent size	time
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

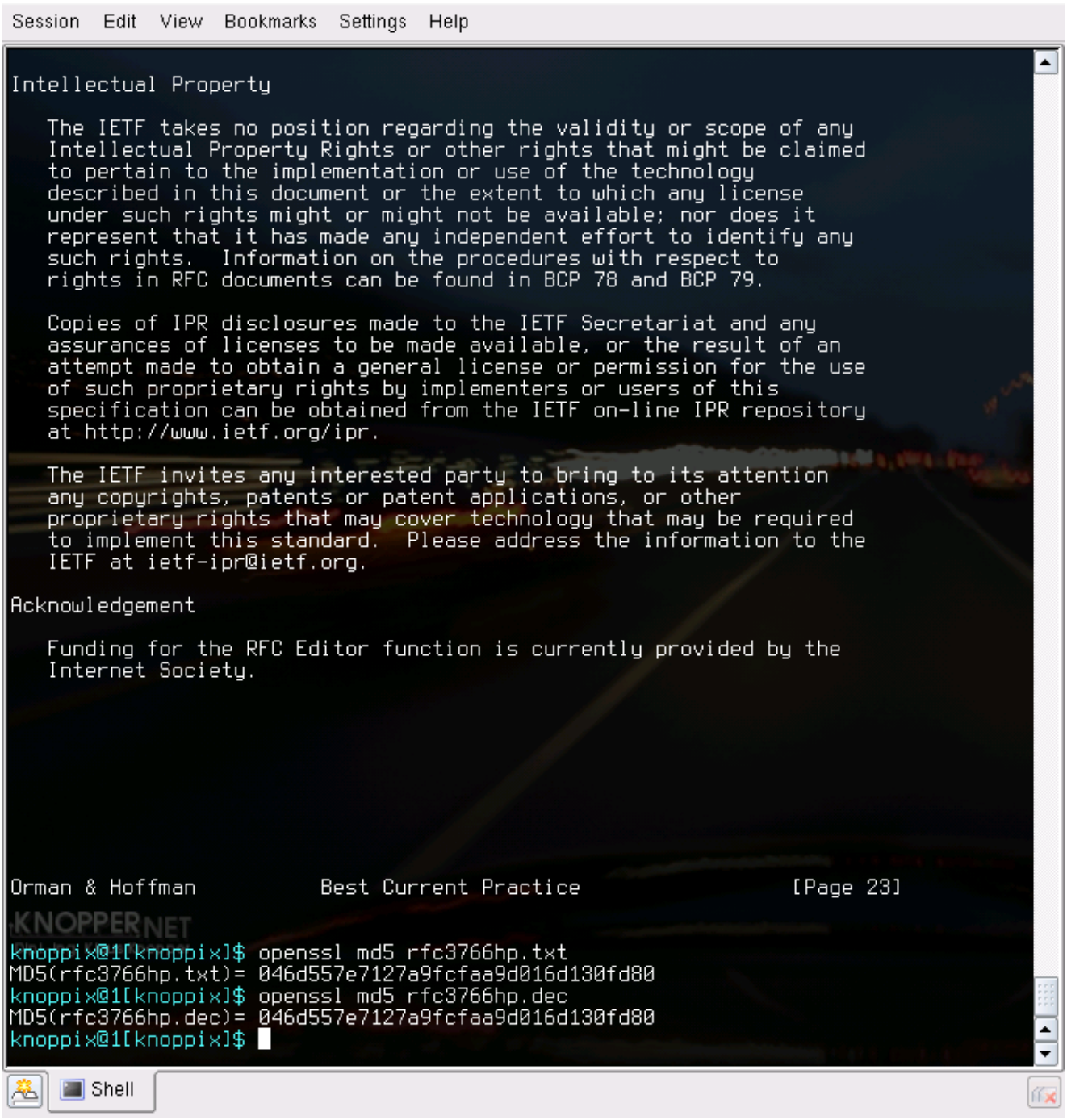
The following two tables (computed by Eric Young) were originally for RSA signing operations, using the Chinese Remainder representation. For ease of understanding, the parameters are presented here to show the interior calculations, i.e., the size of the modulus and exponent used by the software.

Dual Pentium II-350:

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

Alpha 264 600mhz:

equiv modulus	equiv exponent	equiv time

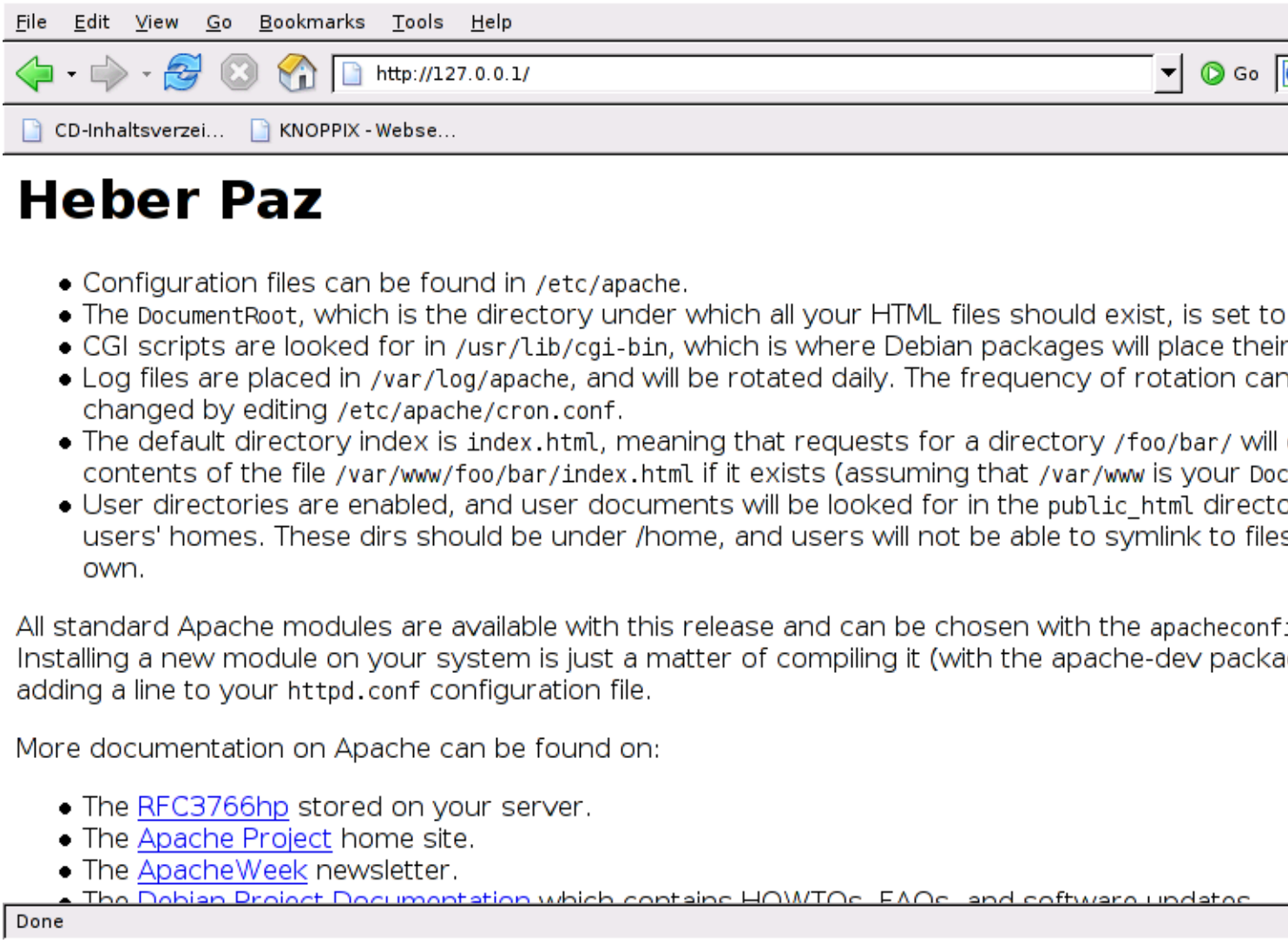


Start Apache

```
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

Edited Home Page using Apache



Exchange of decrypted files (des_keyhp, des_keyrm)