CS6500 - Network Security

Assignment 1: OpenSSL interface and performance analysis

M. Uday Theja
CS14B044

Parameters Varied:

Operations:

- Enc
- Dec

Algorithms:

- AES
- DES
- 3DES

Modes:

- CBC
- ECB

Key Sizes :

- AES
  - 128
  - 192
  - 256
- DES
  - 56
- 3DES
  - 112
  - 168

File Sizes:

- 10KB

- 100KB

System Specifications:

```
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                4
On-line CPU(s) list:   0-3
Thread(s) per core:    2
Core(s) per socket:    2
Socket(s):             1
NUMA node(s):          1
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 61
Stepping:              4
CPU MHz:               500.000
BogoMIPS:              4788.78
Virtualization:        VT-x
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              4096K
NUMA node0 CPU(s):     0-3
```

Observations:

Algorithm : AES

File Size	Mode	Key Size (Bits)	Operation	Time (Micro Secs)	Brute Force Time (years)
10KB	CBC	128	Enc	0.038400	4.14346869919e+23
10KB	CBC	128	Dec	0.031949	3.44738753829e+23
10KB	CBC	192	Enc	0.070400	1.40128095564e+43
10KB	CBC	192	Dec	0.035144	6.99525822515e+42
10KB	CBC	256	Enc	0.078400	2.87864656146e+62
10KB	CBC	256	Dec	0.038339	1.40770957295e+62
10KB	ECB	128	Enc	0.022400	2.41702340786e+23
10KB	ECB	128	Dec	0.022364	2.41313890596e+23
10KB	ECB	192	Enc	0.028800	5.73251300035e+42
10KB	ECB	192	Dec	0.027157	5.40548109551e+42
10KB	ECB	256	Enc	0.024000	8.81218335139e+61
10KB	ECB	256	Dec	0.027157	9.97135263641e+61
100KB	CBC	128	Enc	0.046080	4.97216243903e+23
100KB	CBC	128	Dec	0.014238	1.53632050362e+23
100KB	CBC	192	Enc	0.049760	9.90450857283e+42
100KB	CBC	192	Dec	0.025596	5.09477092906e+42
100KB	CBC	256	Enc	0.084480	3.10188853969e+62
100KB	CBC	256	Dec	0.029755	1.09252714842e+62
100KB	ECB	128	Enc	0.014560	1.57106521511e+23
100KB	ECB	128	Dec	0.014398	1.55358495653e+23
100KB	ECB	192	Enc	0.016160	3.21657673909e+42
100KB	ECB	192	Dec	0.015198	3.02509488123e+42
100KB	ECB	256	Enc	0.016640	6.10978045697e+61
100KB	ECB	256	Dec	0.018557	6.81365360216e+61

Algorithm : DES

File Size	Mode	Key Size (Bits)	Operation	Time (Micro Secs)	Brute Force Time (years)
10KB	CBC	56	Enc	0.182400	416.771472365
10KB	CBC	56	Dec	0.174261	398.17441637
10KB	ECB	56	Enc	0.157600	360.105175684
10KB	ECB	56	Dec	0.157474	359.817274338
100KB	CBC	56	Enc	0.174560	398.857610834
100KB	CBC	56	Dec	0.179506	410.158881132
100KB	ECB	56	Enc	0.189680	433.405772359
100KB	ECB	56	Dec	0.182225	416.371609385

Algorithm : 3DES

File Size	Mode	Key Size (Bits)	Operation	Time (Micro Secs)	Brute Force Time (years)
10KB	CBC	112	Enc	0.411200	6.77027038378e+19
10KB	CBC	112	Dec	0.403677	6.6464067065e+19
10KB	CBC	168	Enc	0.451200	5.35305561655e+36
10KB	CBC	168	Dec	0.441247	5.23497280948e+36
10KB	ECB	112	Enc	0.488800	8.04792841341e+19
10KB	ECB	112	Dec	0.522782	8.60743067066e+19
10KB	ECB	168	Enc	0.582400	6.90961788803e+36
10KB	ECB	168	Dec	0.578737	6.86615990327e+36
100KB	CBC	112	Enc	0.442560	7.28660228854e+19
100KB	CBC	112	Dec	0.438525	7.22016736393e+19
100KB	CBC	168	Enc	0.403440	4.7864289848e+36
100KB	CBC	168	Dec	0.394688	4.68259489181e+36
100KB	ECB	112	Enc	0.416400	6.8558866435e+19
100KB	ECB	112	Dec	0.396368	6.5260664676e+19
100KB	ECB	168	Enc	0.444640	5.27522750298e+36
100KB	ECB	168	Dec	0.461163	5.47125706404e+36

Brute Force Attack Time = 2^(key size) * (encryption time or decryption time)

- 3DES is more secure than DES and AES is the most secure
- AES is the fastest, followed by DES and 3DES is the slowest