College of Computer and Information Science

Northeastern University

CSG252: Cryptography and Communication Security

Fall 2005

Problem Set 4 - Solutions

Prepared by Tim Morgan

AES Implementation

There are many open source implementations available for reference:
http://www.openssl.org/
http://www.gnupg.org/
http://freshmeat.net/projects/cryptrijndael/
http://jclement.ca/software/pyrijndael/

Benchmarks

In order to roughly compare the speed of AES in different languages, selected implementations were tested on the same hardware platform. All were tested several times on several megabytes of data and the average outcome is listed below. Test was performed on CBC mode with a single key. Where possible, simple optimizations were turned on for student implementations. Keep in mind, speed differences do not necessarily indicate overall language performance, as student implementations are likely non-optimal for their specific languages. Also, when comparing to OpenSSL's performance, note that it likely takes advantage of processor-specific instructions such as those in SSE. (Here, 1Mbyte=2^{20}bytes.)

Implementation	8bit Rate (Mbytes/sec)	32bit Rate (Mbytes/sec)
Python (Eugene Kim)	0.00184	0.00622
Java (Michael Everett)	0.509	0.691
C (Mark Gordon)	4.31	7.57
OpenSSL	N/A	70.1

Other interesting benchmarks can be found at:
http://www.cr0.net:8040/code/crypto/aesbench/
http://www.logix.cz/michal/doc/article.xp/padlock-en

The Python version used was 2.4.2, and Sun's Java VM was from JDK 1.5.0_06. For C, the compiler was gcc 4.0.3. The platform is Debian GNU/Linux with a custom-configured 2.6.12 kernel.

Processor information for test platform:

```
> cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 6
model           : 10
model name      : AMD Athlon(tm) XP 2500+
stepping        : 0
cpu MHz         : 1837.442
cache size      : 512 KB
fdiv_bug        : no
hlt_bug         : no
f00f_bug        : no
coma_bug        : no
fpu             : yes
fpu_exception   : yes
cpuid level     : 1
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 mmx fxsr sse
bogomips        : 3637.24
```