ctaes

Simple C module for constant-time AES encryption and decryption.

Features: * Simple, pure C code without any dependencies. * No tables or data-dependent branches whatsoever, but using bit sliced approach from https://eprint.iacr.org/2009/129.pdf. * Very small object code: slightly over 4k of executable code when compiled with -Os. * Slower than implementations based on precomputed tables or specialized instructions, but can do ~15 MB/s on modern CPUs.

Performance

Compiled with GCC 5.3.1 with -O3, on an Intel(R) Core(TM) i7-4800MQ CPU, numbers in CPU cycles:

Algorithm	Key schedule	Encryption per byte	Decryption per byte
AES-128	2.8k	154	161
AES-192	3.1k	169	181
AES-256	4.0k	191	203

Build steps

Object code:

```
$ gcc -O3 ctaes.c -c -o ctaes.o
```

Tests:

```
$ gcc -O3 ctaes.c test.c -o test
```

Benchmark:

```
$ gcc -O3 ctaes.c bench.c -o bench
```

Review

Results of a formal review of the code can be found in http://bitcoin.sipa.be/ctaes/review.zip