AES from OpenSSL

Cache side-channel leak in AES, cache = 8KB, 4-way (observation via miss count)

