AES from OpenSSL

Cache side-channel leak in AES, cache = 32KB, 2-way (observation via miss count)

