Implementing Daniel Bleichenbacher’s adaptive CCA on PKCS #1

Haukur Óskar Porgeirsson  
hawkuro@engineering.ucsb.edu  
hawkuro@gmail.com

Markús Karl Torfason  
mkt2@cs.ucsb.edu  
markus1993@gmail.com

April 23, 2015

Abstract

We want to implement Daniel Bleichenbacher’s attack on the PKCS #1, as described in [1]. PKCS #1 is a standardization of RSA-OAEP used in SSL v3.0, a protocol which some websites still default to today in absence of support for TLS.

Bleichenbacher’s attack exploits the fact that PKCS compliant (hexadecimal) integers start with the bytes 0x00 and 0x02 to narrow down intervals of possible locations for a message (on a number line) given the corresponding ciphertext and a compliance checking oracle. The algorithm is described mathematically in [1], requiring us to iron out the details of implementation.

In addition to implementing the attack itself, we will also implement an oracle that decodes a ciphertext and returns whether or not it is PKCS compliant. If time allows we’re finally going to simulate a simple attack on SSL.

The implementation will be done in Python. Python provides not only arbitrary-length integers, but also an efficiently implemented powermod function using binary exponentiation which should be very useful in our implementation.

References