A Summary of Manger's Padding Oracle Attack

In this document we summarize the implementation details of Mangers's PKCS1 OAEP padding oracle attack. We assume that the reader is acquainted with the attack and only aim to summarize its implementation and provide some basic details; of course, for details about the attack, refer to the original article.

We denote the public modulus by N, the public exponent by e, the private exponent by d, and the given ciphertext to be decrypted by $c = m^e \bmod N$. We denote by O the Manger oracle which determines whether an encrypted message is smaller than $B = 2^{8(k-1)}$ or not, where k is the byte-length of N; in other words, the oracle returns 1 if and only if the first byte of the plaintext is zero.

Step 1: Finding f_1

This part of the attack is used to find a value f_1 which is a power of two for which $O\left(f_1^e \cdot c \bmod N\right) = 0$, i.e. for which $f_1 \cdot m \bmod N \geq B$. The minimal such value of f_1 is returned — the algorithm searches for such values in order, starting from 2.

Algorithm 1 Step 1

```
1: procedure STEP_1(c, N, e, O)
2:     f_1 ← 2
3:     while O(f_1^e · c mod N) = 1 do
4:         f_1 ← 2f_1
5:     end while
6:     return f_1
7: end procedure
```

Step 2: Finding f_2

In this step, the algorithm searches for a value f_2 that is a multiple of $\frac{f_1}{2}$ such that $f_2 \cdot m$ is in the interval $[N, N + B)$.

Algorithm 2 Step 2

```
1: procedure STEP_2(c, N, e, O, f_1)
2:     f_2 ← ⌊(N+B)/B⌋ + f_1/2
3:     while O(f_2^e · c mod N) = 0 do
4:         f_2 ← f_2 + f_1/2
5:     end while
6:     return f_2
7: end procedure
```

Step 3: Find the message m

In the final step, the algorithm searches for the message m, which is to be found in the interval $\left[\left\lceil \frac{N}{f_2} \right\rceil, \left\lfloor \frac{N+B}{f_2} \right\rfloor\right)$, by narrowing the interval until it contains a single value.

Algorithm 3 Finding m

procedure STEP_3(c, N, e, O, f_1, f_2)
  $m_{min} \leftarrow \left\lceil \frac{N}{f_2} \right\rceil$
  $m_{max} \leftarrow \left\lfloor \frac{N+B}{f_2} \right\rfloor$
  while $m_{min} \neq m_{max}$ **do**
    $i \leftarrow \left\lfloor \frac{\left\lfloor \frac{2B}{m_{max}-m_{min}} \right\rfloor \cdot m_{min}}{N} \right\rfloor$
    $f_3 \leftarrow \left\lceil \frac{i \cdot N}{m_{min}} \right\rceil$
    if $O\left(f_3^e \cdot c \bmod N\right) = 1$ **then**
      $m_{max} \leftarrow \left\lfloor \frac{i \cdot N + B}{f_3} \right\rfloor$
    else
      $m_{min} \leftarrow \left\lceil \frac{i \cdot N + B}{f_3} \right\rceil$
    end if
  end while
  return m_{min}
end procedure