Catalogue of RSA Attacks: From Various CTFs

by Sam Gunter

1 Cube-Root Attack

Low Public Exponent Attack

Given N, e, c where e is very small
Finding m

More explanation will be given in future edits

```
# since e is small, found m by finding cube root
def CubeRootNec(N, e, c):
    upper = N
    lower = 1
    while True:
        mid = (upper + lower) // 2
        if (mid ** e <= c):
            lower = mid
        else:
            upper = mid
        if upper ** e == c:
            sol = upper
            break
        if lower ** e == c:
            sol = lower
            break
    return bytes.fromhex(hex(sol)[2:])
```