Anish Banerjee, Shankh Gupta
COL759: Cryptography

Problem 1: RSA with a low-entropy prime generator

Solution: Here, the main idea is that if the prime generator has a low-entropy, it is very likely that two of the sampled N will have a common factor. Since the gcd of two numbers can be calculated efficiently, we can easily factorize the number and thus break RSA.

```
def attack():
    L=[] # A list for storing N
    for i in range(200):
        (N, e), ct = restart_system()
        for i in L:
            p=gcd(i,N)
            if p!=1 and p!=N and p!=N:
                q=N//p
                phiN=(p-1)*(q-1)
                d = inverse(e, phiN)
                return dec(ct, N, d)
        L.append(N)

```

Listing 1: RSA with a low-entropy prime generator

Problem 2: Another Attack on RSA Signatures

Solution:

Problem 3: Attack on RSA PKCS Padding: Bleichenbacher's attack

Solution: