Cryptography

Lab 2

1. Perform a timing-attack [2] on the following RSA implementation.
2. Imlement blind signature scheme [1].
3. Modify decryption algorithm in such a way that it is computed on random (blinded) input. Apply the attack from Problem 1 to that implementation.

Naive RSA

```python
from sympy import randprime, mod_inverse

def GenModulus(w):
    n = len(w) // 2
    p = randprime(2 ** n, 2 ** (n+1))
    q = randprime(2 ** n, 2 ** (n+1))
    N = p * q
    return N, p, q

def GenRSA(w):
    N, p, q = GenModulus(w)
    m = (p-1) * (q-1)
    e = 2 ** 16 + 1
    d = mod_inverse(e, m)
    return N, e, d, p, q

def enc(x, N, e):
    return fast_pow(x, N, e) #x ** e % N

def dec(c, N, d):
    return fast_pow(c, N, d) #c ** d % N

def fast_pow(c, N, d):
    d_bin = "{0:b}".format(d)
    d_len = len(d_bin)
    reductions = 0
    h = 0
    x = c
    for j in range(1, d_len):
        x, r = mod_reduce(x ** 2, N)
        reductions = reductions + r
        if d_bin[j] == "1":
            x, r = mod_reduce(x * c, N)
            reductions = reductions + r
            h = h + 1
    return x, h, reductions

def mod_reduce(a, b):
    reductions = 0
    if a >= b:
        a = a % b
        reductions = 1
    return a, reductions
```

References

[1] David Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology – CRYPTO'83*, pages 199–203. Springer, 1983.

[2] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Advances in Cryptology – CRYPTO'96*, pages 104–113, 1996.