Assignment: Project 5

Name 1: Jonathan Smoley

Name 2: Samuel Sovi

GitHub Name: JT2M0L3Y

A Theoretical RSA Problem

Prove that Bob, using RSA, can encrypt a message, which Alice can decrypt, without sharing a key. The task here is to prove the correctness of RSA, in essence, that decrypt will produce the original plaintext.

Proof:

Assume Bob encrypts a message using the public key (n, e) for this cipher, published by Alice. n being the product of two large primes, p and q, as well as e, any integer less than n, ideally a small one.

Bob breaks his message into blocks such that the length of the block is less than n.

Let m be one of these blocks. Bob can encrypt using the following equation:

$$C \equiv m^{e} \ (mod\ n)$$

Then, Alice would have to decrypt the message as follows:

$$m \equiv C^{d} \ (mod\ n)$$

Where d is a key only known by Alice (private), computed by the following equation:

$$d \equiv e^{-1} \ (mod\ (p - 1)(q - 1))$$

m has two possibilities:

1. $gcd(p, m) = gcd(q, m) = 1$

2. m is a multiple of either p or q but not both

Case 2:

By assumption, $m < n$.
Suppose m is a multiple of p and a multiple of q.
So, $p|m$ and $q|m$.
m can be represented as a product of its factors: $m = f_1 f_2 ... f_k$, where f_j for $1 < j < k$ is prime.

Since $p|m$ and p is prime, p is one of these factors, call it f_p.

$m = f_1 ... f_p ... f_q ... f_k$

Which implies, $pq|m$.

So, $m = pqr = nr$ since $n = pq$.

But, this is impossible due to the assumption $m < n$.

Therefore, m is not a multiple of both p and q.

Case 1: $gcd(p, m) = gcd(q, m) = 1$

Encryption:
$C \equiv m^e \,(mod\, n)$
$C^d \equiv (m^e)^d = m^{ed} \,(mod\, n)$

Recall the definition of the private key: $d \equiv e^{-1} \,(mod\, (p - 1)(q - 1))$

$ed \equiv 1(mod\, (p - 1)(q - 1))$

By the division algorithm,

$ed - 1 = k\,(p - 1)(q - 1)$, for some k in the integers

$ed = k\,(p - 1)(q - 1) + 1$

$m^{ed} = m^{k\,(p-1)(q-1)+1} = m^{k\phi\,(p)\phi(q)+1} = m \bullet m^{k\phi\,(p)\phi(q)} = mm^{k\phi\,(pq)} = mm^{k\phi\,(n)}$

So, $m^{ed} = mm^{k\phi(n)}$.

Knowing $gcd(p, m) = gcd(q, m)$, then $n = pq$.

Let $a = m^{k}$.

Since $gcd(a, n) = 1$, $a^{\phi(n)} \equiv 1\ (mod\ n)$.

$m^{ed} \equiv ma^{\phi(n)} \equiv m\ (mod\ n)$

Knowing that $C \equiv m^{e}\ (mod\ n)$, $C^{d} \equiv m^{ed}\ (mod\ n)$.

So, $m \equiv m^{ed} \equiv C^{d}\ (mod\ n)$.

As such, Alice can find m using the congruence $m \equiv C^{d}\ (mod\ n)$.