Lab-01: Write in Cryptography

Student Name	Avery Yong
Student #	059789115
Course Code	SPR200
Section Number	NAA
Professor	Prof. Wei Huang

1 Math equation 1

$$\int_0^\infty \frac{x^3}{e^x - 1} dx = \frac{\pi^4}{15}$$

2 Math equation 2

$$\begin{aligned} x &= y & w &= z & a &= b + c \\ 2x &= -y & 3w &= \frac{1}{2}z & a &= b \\ -4 + 5x &= 2 + y & w + 2 &= -1 + w & ab &= cb \end{aligned}$$

3 Cryptographic protocol

1. **Choose two large primes:** Pick primes p and q.
2. **Compute:** $n = p \cdot$ q.
3. **Compute Euler's totient:** $\varphi(n) = (p-1)(q-1)$.
4. **Choose public exponent:** Select e such that $\gcd(e, \varphi(n)) = 1$.
5. **Compute private exponent:** Find d such that $e \cdot d \equiv 1 \pmod{\varphi(n)}$.
6. **Publish:** The public key is (n, e), and the private key is d.

4 Cryptographic proof (Take-home task)

Proof. The private exponent d is chosen so that

$$e \cdot d \equiv 1 \quad (mod \varphi(n)).$$

This implies there exists some integer k such that

$$e \cdot d = 1 + k\varphi(n).$$

Consider the ciphertext $c \equiv m^e \pmod{n}$. When we raise c to the power d, we get

$$c^d \equiv (m^e)^d = m^{ed} \quad \pmod{n}.$$

Substituting $ed = 1 + k\varphi(n)$ into the exponent, we obtain

$$m^{ed} = m^{1+k\varphi(n)} = m \cdot (m^{\varphi(n)})^k.$$

By Euler's theorem (which states that if $gcd(m, n) = 1$, then $m^{\varphi(n)} \equiv 1 \mod n$), we have

$$(m^{\varphi(n))k} \equiv 1^k \equiv 1 \pmod{n}.$$

Therefore,

$$m^{1+k\varphi(n)}) \equiv m \cdot 1 \equiv m \pmod{n}.$$

Hence,

$$m^{ed} \equiv m \pmod{n},$$

which shows that decrypting c with exponent d indeed recovers the original message $\square$