Ejercicio I

En el contexto de una comunicación cifrada entre Alice y Bob con RSA, donde la clave pública de Bob es $[n = 187, e = 3]$, respondemos a las siguientes cuestiones:

1. **Cálculo de los valores p y q**

$$n = p \times q$$

$$187 = p \times q$$

Descomponiendo 187 en factores primos:

$$187 = 11 \times 17$$

Por lo tanto, $p = 11$ y $q = 17$.

2. **Clave privada de Bob** La clave privada se calcula determinando el exponente d, que satisface:

$$d \times e \equiv 1 \mod \varphi(n)$$

Donde $\varphi(n) = (p-1) \times (q-1)$:

$$\varphi(187) = (11-1) \times (17-1) = 10 \times 16 = 160$$

Hallamos d resolviendo:

$$d \times 3 \equiv 1 \mod 160$$

El inverso modular de 3 módulo 160 es $d = 107$, por lo que la clave privada de Bob es $(n, d) = (187, 107)$.

3. **Cálculo del criptograma C**

$$C = M^e \mod n$$

$$C = 40^3 \mod 187$$

$$40^3 = 64000$$

$$64000 \mod 187 = 40$$

Por lo tanto, $C = 40$.

4. **Descifrado del criptograma $C = 4$** El atacante debe calcular:

$$M = C^d \mod n$$

$$M = 4^{107} \mod 187$$

Usando exponentiación modular rápida, obtenemos $M = 23$.

Ejercicio II

En el protocolo Diffie-Hellman con $\mathbb{Z}_{73}$ y $\alpha = 2$:

1. **Cálculo de las claves públicas:**

- Alice envía: $A = \alpha^a \mod p = 2^{13} \mod 73 = 61$.
- Bob envía: $B = \alpha^b \mod p = 2^{19} \mod 73 = 24$.

2. **Cálculo de la clave compartida:**

- Alice computa: $K = B^a \mod p = 24^{13} \mod 73 = 39$.
- Bob computa: $K = A^b \mod p = 61^{19} \mod 73 = 39$.

La clave acordada es $K = 39$.

Ejercicio III

1. **Niveles de seguridad postcuántica del NIST**

- **Nivel 1:** Equivalente a AES-128 y SHA-256.
- **Nivel 2:** Equivalente a SHA3-256.
- **Nivel 3:** Equivalente a AES-192 y SHA3-384.
- **Nivel 4:** Equivalente a SHA3-384.
- **Nivel 5:** Equivalente a AES-256 y SHA3-512.

2. **Tabla de algoritmos postcuánticos:**

Algoritmo	Variante	Tamaño de Clave	Tamaño de Firma	Nivel de Seguridad
CRYSTALS-Dilithium	2	1312 bytes	2420 bytes	2
CRYSTALS-Dilithium	3	1952 bytes	3293 bytes	3
CRYSTALS-Dilithium	5	2592 bytes	4595 bytes	5
CRYSTALS-Kyber	512	800 bytes	N/A	1
CRYSTALS-Kyber	768	1184 bytes	N/A	3
CRYSTALS-Kyber	1024	1568 bytes	N/A	5
FALCON	512	897 bytes	666 bytes	1
FALCON	1024	1793 bytes	1280 bytes	5

Table 1: Tabla de algoritmos postcuánticos

3. **Definición de KEM** - Un Key Encapsulation Mechanism (KEM) es un mecanismo criptográfico utilizado para compartir claves de sesión de manera segura, evitando la necesidad de intercambiar claves directamente.

4. **Inconvenientes de reemplazar Diffie-Hellman por Kyber**

- Mayores requerimientos computacionales.
- Tamaños de clave más grandes.
- Adaptación de infraestructuras existentes.
- Posible incompatibilidad con sistemas legados.