



# UNSA

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA

# Estructuras Discretas II

Docente: Carlo Corrales Delgado

Actividad

Ejercicios de criptografía y clave publica

Escuela:

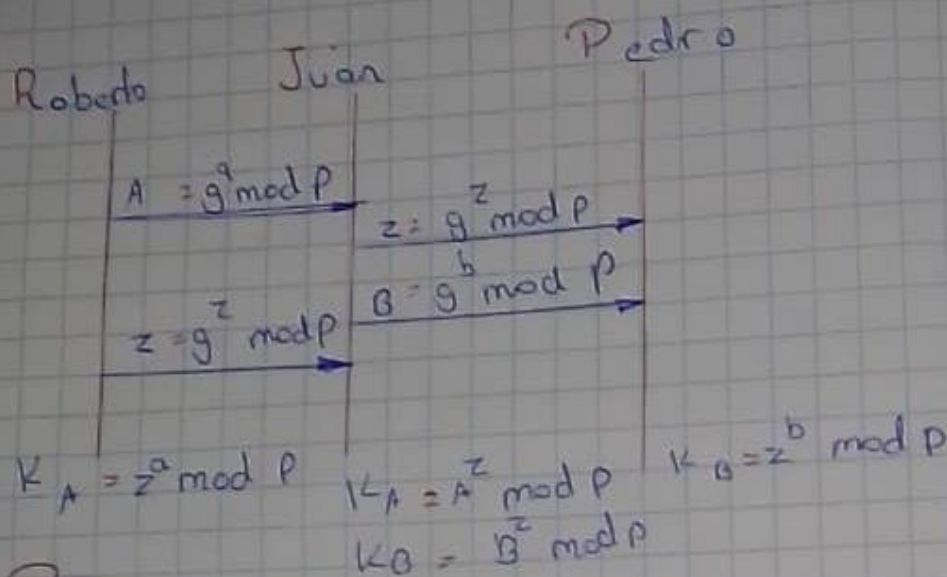
Ciencia de la computación (Primer año)

Alumno:

Josue Gabriel Sumare Uscca

# Criptografía y clave pública

1)



2) Para poder de cifrar la conversación debería hacer muchos cálculos con módulos muy grandes, haciendo este proceso inviable por el costo en tiempo.

3) print("Bienvenido a el programa de cifrado o generación de clave")

Primo = int(input("Ingrese el numero primo"))

raiz = int(input("Ingrese la raiz primitiva del primo"))

clavePr = int(input("Ingrese su clave privada"))

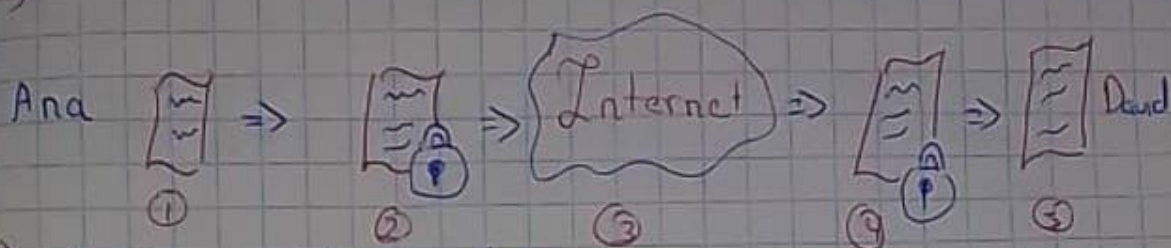
ClavePub = (raiz\*\*clavePr) % primo

print("Su clave publica es" + clavePub)

## Cuestionario

1)  $\ominus$  asimétrico y simétrico

2)



3)  $128/8 = 16$  caracteres

4) Porque al usar códigos con menor peso, facilita la ejecución de códigos

5) Rpta: Utiliza la clave pública de B para cifrar el mensaje

6) Rptas: - Se utilizan sobre todo para la autenticación de identidades.  
- Se basan en funciones matemáticas no invertibles computacionalmente, o carentes de inversa.

Averiguar las palabras en la base de datos de SHA 256

1. Implementación: C73cc36ca8f753dc12d62  
23109b6b4f4d99a135ecc4aaca  
ae3a6fc08be2ff046.

2. Administrador123: No se encuentra

3. hda.: 3b952738efc124f6b34181cb  
9e608432741ab05df195462dc  
98b26f50f9ef217



4. usuario: 9250e222c4c71fa58d4c54b50  
a880a312e9f9fed55d5c3aa0b0e860  
ded99165:

5. Estructuras Discretas: no se encuentra

Generar una clave SHA256 con las siguientes entradas

1. Clave Pública: fg6b746a3e39db3db1166f0c  
fecdo44423edd3e10961e2fdc8  
da5d36bd8c31c34

2. Encriptación Asimétrica: 37c389ea8ac971a  
3f761c1683349e09a2dd2525f391de  
5a9f32caac2

3. National Security Agency: 74c621c4d2d  
357267234a2e2a91f156bb9f108  
a910b6d2b5e6057ce26481c8e6

4. Estructuras Discretas: 6469c43eb01169  
4b9a4127d639a1081379b34dd13ab  
22d8ecf4b4abd1737d57d

5. basededatos: 1e3f5786d5065283a9dc7  
d6c65b819cde5949415b3  
333a627e1303dbb487cc26