Pontificia Universidad Católica de Chile
Departamento de ciencias de la computacion
IIC3253 – Criptografía y Seguridad Computacional
Primer Semestre del 2025

Ayudantía 01

Aritmetica modular - OTP - Perfect secrecy

Ayudante: Manuel Cifuentes – mecifuentes@uc.cl

Repaso

Problema 1 (Aritmetica modular)

Calcula los siguientes módulos:

- $53 \mod 7$
- $255 \mod 16$
- $-14 \mod 6$

Determina si las siguientes igualdades son verdaderas o falsas:

- $6 \equiv 3 \mod 4$
- $8 \equiv 77 \mod 3$
- $14 \equiv 29 \mod 5$
- $-4 \equiv 45 \mod 6$
- $3879 \equiv 8391274129 \mod 10$

Problema 2 (Propiedades)

Explique las siguientes propiedades del módulo y utilícelas en algún problema anterior:

- $a \equiv b \mod n$ si y solo si n divide a $b - a$.
- Si $b = a \mod n$, entonces $a \equiv b \mod n$.
- Si $a \equiv b \mod n$ y $c \equiv d \mod n$, entonces $(a + c) \equiv (b + d) \mod n$.
- $a \equiv b \mod n$ si y solo si $a \mod n = b \mod n$.
- $(a + b) \mod n = [(a \mod n) + (b \mod n)] \mod n$.

Problema 3 (OTP)

Demuestre, utilizando propiedades del módulo, que la siguiente igualdad se cumple:

$$\mathbf{Dec_k}(\mathbf{Enc_k}(\mathbf{m})) = \mathbf{m}$$

Problema 4 (Implementacion OTP)

Complete el siguiente código para implementar el cifrado OTP, tanto para clave completa como para clave incompleta:

```
def encrypt(msg, key):
    msg = msg.upper()
    key = key.upper()
    final = ""
    if len(key) >= len(msg):
        pass
    else:
        pass
    return final


def decrypt(msg, key):
    msg = msg.upper()
    key = key.upper()
    final = ""
    if len(key) >= len(msg):
        pass
    else:
        pass
    return final
```

Con el código generado, realice lo siguiente:

- Encripte "ElAsesinoEsShmebulock" con la clave "noconfieseneltriangulo".
- Desencripte "PZSJXJSYGRTSUGAGOUMSSQ" con "claveseguraSisi".

Problema 5 (Perfect secrecy)

Desafío: Tienes que desencriptar este mensaje:

"OSCGLGXHTBLQQAZZCBQRMRRZDFQGAHGOASZKPPUQLBHBOUODREZ"

Sabes que fue encriptado con la técnica OTP. Como ayuda, sabes que este tipo de mensajes siempre comienza con la palabra "orden".

Para los siguientes dos casos, discute y demuestra:

- Sabes que el largo de la llave es igual al tamaño del mensaje. ¿Se puede desencriptar? Si la respuesta es sí, inténtalo?.
- Sabes que el largo de la llave es menor al tamaño del mensaje. ¿Se puede desencriptar? Si la respuesta es sí, pruébalo.