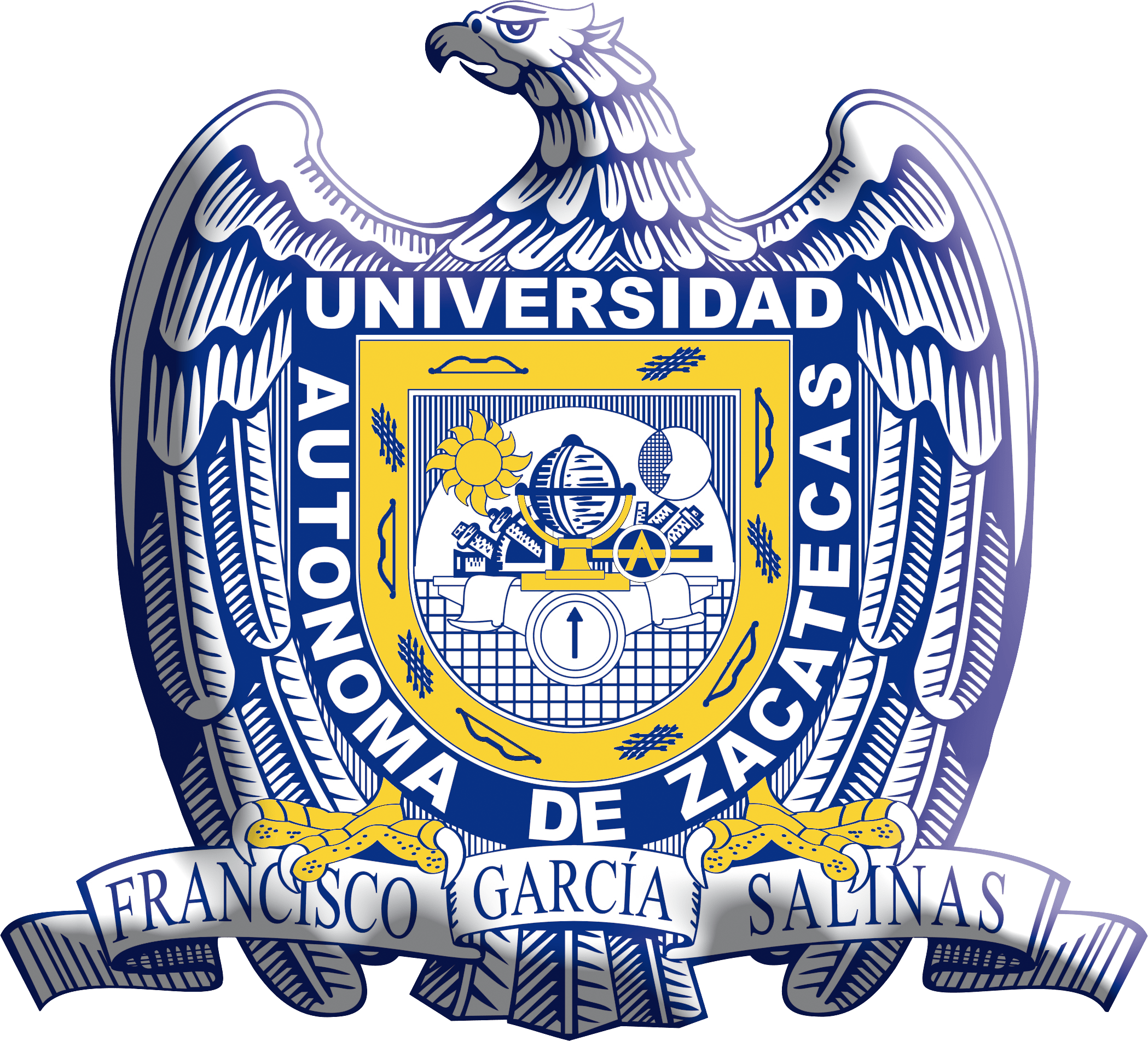
**UNIVERSIDAD AUTONOMA DE ZACATECAS**

**INGENIERÍA DE SOFTWARE**

****

**TAREA: “RESUMEN DE CONCEPTOS”**

**ALUMNO: JOSÉ LUIS REYES MAURICIO**

**MAESTRO: DR. ANTONIO DE JESÚS GARCÍA DOMÍNGUEZ**

**MATERIA: CRIPTOGRAFÍA**

**ZACATECAS, ZACATECAS**

**17/02/21**

**Kerckhoffs’s Principle/Shannon’s Maxim**

Shannons y Kerckhoffs tenían una idea parecida respecto a la seguridad en criptografía, Shannons dice que la seguridad de un cifrado depende del secreto de la llave no del secreto del algoritmo, y Kerckhoffs se deben diseñar sistemas bajo el supuesto de que el enemigo finalmente ganará plena familiaridad con ellos.

Básicamente ambos hablan de mantener en secreto la llave, no el algoritmo ya que siempre en un punto se conocerá este último.

**Scientific and Mathematical Theories**

Las matemáticas y la ciencia se encuentran muy relacionadas los procesos son ligeramente diferentes.

Las palabras pueden significar distintas cosas en diferentes situaciones como la palabra bug en inglés significa insecto y en el ámbito computacional se refiera a un error en un programa.

El término teoría es una palabra así. Esta palabra tiene un significado diferente en un contexto científico que en el lenguaje cotidiano.

En las matemáticas una teoría no es una suposición o un presentimiento, ni siquiera una suposición fundamentada.

**What Is a Mathematical Theory?**

Las teorías en matemáticas fluyen de axiomas. Un axioma es un hecho único que se supone cierto sin prueba.

A diferencia de la ciencia, las matemáticas tratan más con pruebas que con experimentos. Las teorías matemáticas individuales abordan un sistema particular. Comienzan con una base que son simplemente los datos que describen lo que se sabe o lo que se supone.

**The Scientific Process**

El proceso científico se trata principalmente de experimentación, nada se considera realmente cierto hasta que algún experimento demuestre que es cierto. Casi siempre se van a necesitan varios experimentos para confirmar que algo es cierto.

La parte clave es que la hipótesis es una suposición comprobable, una suposición que no se puede comprobar no tiene valor en la ciencia.

El pináculo del proceso científico es la teoría.

**A Scientific Theory**

Después de realizar un número de pruebas, se confirmarán uno o más hechos, varios hechos son recopilados, lo que requiere alguna explicación. La explicación de esos hechos se llama teoría.

Una teoría es una explicación de un conjunto de observaciones o eventos relacionados basados ​​en hipótesis probadas y verificadas varias veces

Una teoría es una explicación después de haber acumulado datos, es un modelo explicativo, explica los hechos que conocemos y nos da contexto para ampliar nuestra base de conocimientos.