Criptografía y Seguridad
Tarea 01: Máximas de Kerckhoffs

Acosta Arzate Ruben
Bernal Márquez Erick
Deloya Andrade Ana Valeria
Gutiérrez Medina Sebastián Alejandro
Rivera Silva Marco Antonio

25 de agosto de 2023

1. ¿Quién fue Kerchoffs? ¿Cuáles son las máximas de Kerchoffs?

No hay mucha información al respecto acerca de quién fue Kerchoffs en internet. La mayoria de las páginas web, que realmente son pocas, se limitan a decir que fue un linguista de origén Neerlandés quien participó en la difusión de un idioma artificial llamado *volapük*.

También publicó ensayos para un revista francesa sobre la criptografía militar. A partir de estos se formaron 6 principios que hoy en día se siguen aplicando en la criptografía moderna, a estos principios también se les conoce como "máximas". Así como el principio de *Shannon* que también es conocido la máxima de *Shannon*

1. Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica.

   Es decir, que si en teoría el sistema de cifrado se puede romper, al menos en la práctica debería ser imposbile de romper. Por ejemplo tener un alfabeto de un mil millones digitos con el cifrado César, en teoría es rompible ya que basta con recorrer el alfabeto x cantidad de elementos, pero en la práctica esto llevaría una eternidad (Quizá con las computadoras modernas lo harían menos de un minuto, pero la idea se entiende)

2. La efectividad del sistema no debe depender de que su diseño permanezca en secreto.

   Es decir, si el mensaje es interceptado por alguien más entonces el mensaje seguirá siendo díficl de descifrar. Así lo intercpeten 10000 personas o una sola.

3. La clave debe ser fácilmente memorizable, de manera que no haya que recurrir a notas escritas.

   Creo que esta es fácil de interpretar

4. Los criptogramas deberán dar resultados alfanuméricos.

   Los mensajes ocultos deberán dar resultados que consistan en numeros y letras.

5. El sistema debe ser operable por una única persona.

   Un sistema aislado, nadie más lo puede usar. Y aunque cayera en manos equivocadas, por el segundo principio, el mensaje debe ser díficil de descifrar.

6. El sistema debe ser fácil de utilizar.

Debido a ser un pionero en la materia gracias a sus ensayos es que muchos lo consideran como el padre de la criptografía.

También manejan un principio aparte el cual fue expresado por Claude Shannon llamado **Maxima de Shannon** el cual dice:

"Diseñe el sistema suponiendo que el enemigo lo conoce totalmente"

2. Fuentes

- https://www.curistoria.com/2020/01/los-principios-de-kerckhoffs.html
- https://www.freetimelearning.com/online-quiz/programming-languages-quiz.php?Who-is-the-father-of-Computer-Security-or-Cyber-Security?&id=1450
- https://academia-lab.com/enciclopedia/principio-de-kerckhoff/