***Universidad del Norte***
***Departamento de Ingeniería de Sistemas y Computación***
***Criptografía***

# PARCIAL 2

El objetivo de este examen parcial es evaluar la capacidad de los estudiantes para implementar y analizar diferentes métodos criptográficos (simétricos, asimétricos, y protocolos de intercambio de llaves) y realizar ataques específicos sobre dichos esquemas.

Para ello, los estudiantes deben basarse en las implementaciones realizadas en el primer parcial, incorporando las mejoras sugeridas, y sobre estas implementar tres escenarios prácticos que cumplan con los siguientes requisitos:

## Escenario 1: Intercambio de Llaves Diffie-Hellman sobre un Grupo Cíclico $\mathbb{F}_p^*$

1. **Implementación del Protocolo:**
   - Implementar el protocolo de intercambio de llaves Diffie-Hellman sobre el grupo cíclico multiplicativo $\mathbb{F}_p^*$ para cada conjunto de parámetros contenidos en el archivo JSON adjunto.
   - Una vez que las partes acuerden el secreto compartido, utilizar una **KDF** (como una función hash criptográfica a elección) para generar una llave simétrica.
   - Usar dicha llave simétrica para cifrar los mensajes entre cliente y servidor utilizando el cifrador **Salsa20**.

2. **Ataque de Interceptación:**
   - El atacante debe capturar los mensajes intercambiados entre las partes usando una herramienta de monitoreo de red (como Wireshark).
     - **Nota:** Utilice al cliente o al servidor para capturar los mensajes con la herramienta de monitoreo de red.
   - Intentar resolver el problema del logaritmo discreto asociado al intercambio de llaves Diffie-Hellman utilizando el algoritmo de "pasos de bebé, pasos de gigante" dentro de un tiempo máximo de una hora.
   - Mostrar si el atacante logra obtener la llave simétrica y descifrar los mensajes cifrados con Salsa20.
     - **Nota:** Asuma que el atacante conoce la KDF utilizada.

## Escenario 2: Ataque de Hombre en el Medio en Diffie-Hellman sobre Curva Elíptica P256

1. **Implementación del Protocolo:**
   - Implementar el protocolo de intercambio de llaves Diffie-Hellman utilizando la curva elíptica **P256**. Las partes (cliente y servidor) deben acordar una llave simétrica generada mediante una **KDF** (por ejemplo, una función hash criptográfica).
   - Cifrar la comunicación posterior utilizando **AES-256** en modo **CBC**.

2. **Ataque de Hombre en el Medio (MitM):**
   - El atacante debe realizar un ataque de hombre en el medio, interceptando y modificando el intercambio de llaves, logrando establecer llaves distintas con cada parte (cliente y servidor).

## Escenario 3: Comparación entre Criptografía Simétrica y Asimétrica

1. **Implementación de Comunicaciones Asimétricas:**
   - Implementar dos comunicaciones asimétricas (los parámetros de inicialización quedan a su elección):
     - Utilizando el criptosistema **RSA OAEP**.
     - Utilizando el criptosistema **ElGamal**.

2. **Comparación de Eficiencia:**
   - Comparar la eficiencia de ambas comunicaciones asimétricas (en términos de la cantidad de información transmitida sobre la red) contra las comunicaciones simétricas realizadas en los escenarios anteriores (con **Salsa20** en el Escenario 1 y **AES-256** en el Escenario 2).
   - Evaluar el impacto en el rendimiento y en la cantidad de datos transmitidos.

## Análisis y Conclusiones

Al finalizar la implementación de los tres escenarios, los estudiantes deberán responder las siguientes preguntas y redactar conclusiones:

**Escenario 1:**

1. ¿Qué factores influyen en la dificultad de resolver el problema del logaritmo discreto utilizando el algoritmo de "pasos de bebé, pasos de gigante"? ¿Cuáles fueron los resultados del ataque y qué conclusiones puedes extraer?
2. ¿Cuáles son los beneficios y desventajas de utilizar Diffie-Hellman sobre un grupo cíclico $\mathbb{F}_p^*$ en comparación con otros métodos de intercambio de llaves (investigue otros métodos)?

**Escenario 2:**

1. ¿Qué vulnerabilidades inherentes a Diffie-Hellman sobre curvas elípticas se pueden explotar en un ataque de hombre en el medio?
2. ¿Qué contramedidas podrían implementarse para mitigar estos ataques en un entorno real?

**Escenario 3:**

1. ¿Cuáles son las principales diferencias en términos de eficiencia y seguridad entre RSA OAEP y ElGamal? Justifica cuál criptosistema asimétrico sería más adecuado en un contexto donde el tamaño de los mensajes y la rapidez de la comunicación son críticos.
2. En base a la comparación con las comunicaciones simétricas de los escenarios anteriores, ¿qué conclusiones puedes extraer sobre el uso de cifrado simétrico vs. asimétrico en aplicaciones de comunicación de red?

**Conclusiones:**

1. Resuma los principales aprendizajes en relación con la seguridad y la eficiencia de los distintos esquemas criptográficos implementados.
2. Discuta la relevancia de la correcta implementación de protocolos criptográficos y de los posibles ataques, como el hombre en el medio, para asegurar la privacidad y confidencialidad de la información.
3. Proporcione recomendaciones basadas en lo observado durante la implementación para garantizar un intercambio seguro de llaves y una comunicación cifrada robusta.

## Entrega y Evaluación:

Finalmente, los estudiantes deben presentar:

1. El código fuente de ambas implementaciones (cliente y servidor) para cada escenario y el código fuente de las acciones realizadas por el atacante.
2. Un documento en formato **PDF** donde se encuentren:
   - **a.** Capturas de pantalla de la ejecución de los códigos en los distintos escenarios.
   - **b.** Capturas de pantalla de la herramienta de monitorización de red que demuestren el análisis de tráfico los escenarios donde sea necesario.
   - **c.** Respuestas detalladas a las preguntas del análisis de seguridad, justificadas con evidencia (e.g. capturas de pantalla, fragmentos de código, etc.).

**Para tener en cuenta:**

- Este parcial es para desarrollar en grupos de **3** integrantes.
- La solución (análisis) debe ser original.
- Puede utilizar el lenguaje de su elección para desarrollarlo, se recomienda el uso de Python o Rust.
- Puede utilizar librerías de terceros para implementar el cifrado y descifrado con los algoritmos criptográficos solicitados (e.g. pycryptodome).
- Todos los códigos solicitados deben estar **documentados** y deben ser subidos a un repositorio de **GitHub**, cuyo enlace debe ser incluido en el documento de las respuestas.