



Descripción del Proyecto

Título: *Simulador de Red Cifrada con Cifrado Vigenère Extendido y RSA*

Este proyecto integra conceptos fundamentales de **criptografía y seguridad en redes**, mediante la simulación de una red de nodos [ciudades colombianas] conectados entre sí. Cada nodo cuenta con claves RSA propias, permitiendo simular el envío de mensajes cifrados de forma segura.

El mensaje se cifra primero utilizando el **algoritmo de Vigenère extendido** con una clave simétrica aleatoria, la cual a su vez es cifrada con la clave pública RSA del receptor. Además, se implementa una **firma digital basada en hash SHA-256** para garantizar la integridad del mensaje.

La red se representa gráficamente sobre un **mapa interactivo** mediante Plotly, mostrando la ruta del mensaje, la distancia entre ciudades y un posible nodo espía [MITM]. Esta funcionalidad permite **visualizar de manera educativa** cómo viaja la información y qué riesgos podrían surgir si no se aplican técnicas adecuadas de cifrado.

Es una herramienta ideal para **formación en ciberseguridad, redes, criptografía y ética digital**, brindando un entorno visual, práctico e interactivo para comprender cómo proteger los datos en entornos distribuidos.

Aquí integramos estos códigos:

- ☒ Cifrado simétrico (Vigenère)
- ☒ Cifrado asimétrico (RSA)
- ☒ Firma digital básica
- ☒ Simulación de red con nodos (ciudades reales)
- ☒ Visualización con Plotly
- ☒ Simulación de ataque Man-In-The-Middle (MITM)
- ☒ Menú interactivo

¿Para qué sirve tu proyecto?

1. Enseñar conceptos de criptografía:

- Muestra el uso del **cifrado simétrico (Vigenère)** y **asimétrico (RSA)**.
- Explica cómo se **protege un mensaje** usando claves y firmas digitales.

2. Simular una red real:

- Representa una red de dispositivos o ciudades como nodos interconectados.
- Permite **visualizar la ruta de un mensaje cifrado** entre dos puntos.

3. Simular ataques de seguridad (MITM):

- Incluye un nodo espía [Man-In-The-Middle] para demostrar cómo **puede interceptarse y romperse la seguridad** si no se usan buenas prácticas.

4. Visualizar en mapas interactivos:

- Superpone la red en un **mapa geográfico real (Colombia)** usando Plotly.
- Muestra **distancias, rutas y nodos clave** de forma visual y didáctica.

5. Apoyo académico o formativo:

- Es una herramienta educativa para **explicar seguridad de la información, criptografía, redes y ciberseguridad**.

Impacto en la sociedad

El proyecto tiene un impacto directo en la **concientización sobre la ciberseguridad**, un tema cada vez más importante en nuestra sociedad digital. Aporta de las siguientes formas:

- **Educa** a estudiantes y usuarios sobre la importancia del cifrado de datos.
- **Simula entornos reales** de comunicación entre dispositivos, ayudando a comprender vulnerabilidades como ataques MITM (Man-In-The-Middle).
- **Desarrolla el pensamiento crítico y lógico** al combinar programación, criptografía y redes.

Problemáticas que ayuda a abordar

- **Falta de conciencia sobre la privacidad digital:** muchas personas no saben cómo se protegen sus datos.
- **Uso de comunicaciones inseguras:** este simulador demuestra qué puede pasar si no hay cifrado adecuado.
- **Educación técnica limitada en colegios o instituciones:** brinda una forma visual e interactiva de aprender conceptos avanzados.
- **Creciente cantidad de ciberataques:** desde WiFi públicos hasta redes corporativas mal protegidas.

Mercado potencial

Este proyecto puede escalar o adaptarse para diferentes sectores:

1. **Educación tecnológica:** como herramienta didáctica en colegios, universidades y bootcamps de programación o seguridad informática.
2. **Laboratorios de formación empresarial:** para capacitar a empleados en seguridad digital.
3. **Ferias de ciencia y tecnología:** como proyecto demostrativo o prototipo académico.
4. **Startups EdTech o Cybersecurity:** que buscan productos educativos interactivos o simuladores de amenazas reales.

Tendencias tecnológicas que se relacionan

- **Ciberseguridad educativa:** se promueve en todo el mundo como competencia básica.
- **Criptografía híbrida:** combinando métodos simétricos (Vigenère) y asimétricos (RSA), como lo hace tu proyecto.
- **Aprendizaje basado en simulación:** cada vez más adoptado por instituciones educativas.
- **Uso de redes descentralizadas y cifradas (blockchain, IoT):** donde la simulación de comunicación cifrada es esencial.
- **Gamificación y visualización interactiva:** especialmente si se conecta con visualización en Plotly o interfaces web.