Privacidad de Punto a Punto: Blindando Mensajes con CrypTXT y DecrypTXT

En la comunicación diaria de un equipo de IT, es común la necesidad de compartir credenciales temporales o datos sensibles. El error más frecuente es enviarlos en "texto plano" a través de aplicaciones de mensajería o sistemas de tickets que almacenan logs. Si esos sistemas se ven comprometidos, toda la información histórica queda expuesta.

¿Qué son CrypTXT y DecrypTXT?

Son un ecosistema de dos herramientas diseñadas por el mismo desarrollador para cifrar y descifrar texto de manera rápida utilizando el algoritmo **AES (Advanced Encryption Standard)** directamente en el navegador.

- **CrypTXT:** La herramienta de "salida". Permite escribir un mensaje, definir una contraseña (llave) y generar un bloque de texto cifrado ilegible.
- **DecrypTXT:** La herramienta de "entrada". Recibe el bloque de texto cifrado y, mediante la contraseña correcta, recupera el mensaje original.

https://github.com/ContactAlexey/decryptxt

https://github.com/ContactAlexey/cryptxt

https://github.com/Zalexanninev15/Encrypt-and-Decrypt?tab=readme-ov-file

https://zalexanninev15.github.io/Encrypt-and-Decrypt/

La ventaja del "Zero Knowledge"

Lo que hace destacar a estas herramientas es su simplicidad:

1. **Ejecución local:** Aunque se accede vía web, el cifrado ocurre en el lado del cliente (tu navegador). La contraseña nunca viaja al servidor.
2. **Portabilidad:** No requieren instalación. Son ideales para administradores de sistemas que saltan de un equipo a otro.

3. **Sin rastro:** El mensaje cifrado resultante parece una cadena de caracteres aleatorios que no levanta sospechas en filtros automáticos de contenido.

Ejercicio Práctico: "El Canal de Comunicación Seguro"

Objetivo: Simular un escenario de soporte técnico donde se deben enviar credenciales de administrador de forma segura, evitando que un intermediario (el log del chat) pueda leerlas.

Escenario:

El administrador de sistemas (Alumno A) debe enviarle al técnico de campo (Alumno B) la contraseña de una base de datos crítica. No pueden usar el teléfono y el chat corporativo está siendo auditado.

Paso 1: Cifrado (Alumno A)

1. Entra en Encrypt-and-Decrypt.
2. En el campo **"Text to encrypt"**, escribe: DB_ADMIN / Pass: Admin_2025_#Secure.
3. En el campo **"Key"**, introduce una palabra secreta acordada previamente (ej. CiberSeguridad2025).
4. Haz clic en **"Encrypt"**.
5. Copia el código resultante (el bloque de texto cifrado).

Paso 2: Transmisión (Intercambio)

1. El Alumno A envía el código cifrado al Alumno B por cualquier medio (el chat de la clase, un documento compartido o correo).
2. *Pregunta de reflexión:* Si un atacante intercepta este mensaje ahora mismo, ¿qué información útil obtiene?

Paso 3: Descifrado (Alumno B)

1. El Alumno B copia el código cifrado recibido.
2. Entra en Encrypt-and-Decrypt.

3. Pega el código en **"Text to decrypt"**.
4. Introduce la **Key** acordada (CiberSeguridad2025).
5. Haz clic en **"Decrypt"** para revelar la contraseña.

Paso 4: Prueba de Error

1. Intenta descifrar el mismo mensaje pero cambiando un solo carácter de la **Key**.
2. Observa el resultado. (Esto demuestra que sin la llave exacta, el algoritmo AES hace que sea matemáticamente imposible recuperar el texto original en un tiempo razonable).

Entrega:

Para completar el ejercicio, el alumno debe entregar una captura de pantalla del texto descifrado correctamente y una breve explicación de por qué es más seguro usar este método que enviar la contraseña directamente por el chat.