

Lab_5 – Cifrado Asimétrico

Univ. Cristian Kevin Gallardo Coro

PREGUNTAS DE EVALUACIÓN

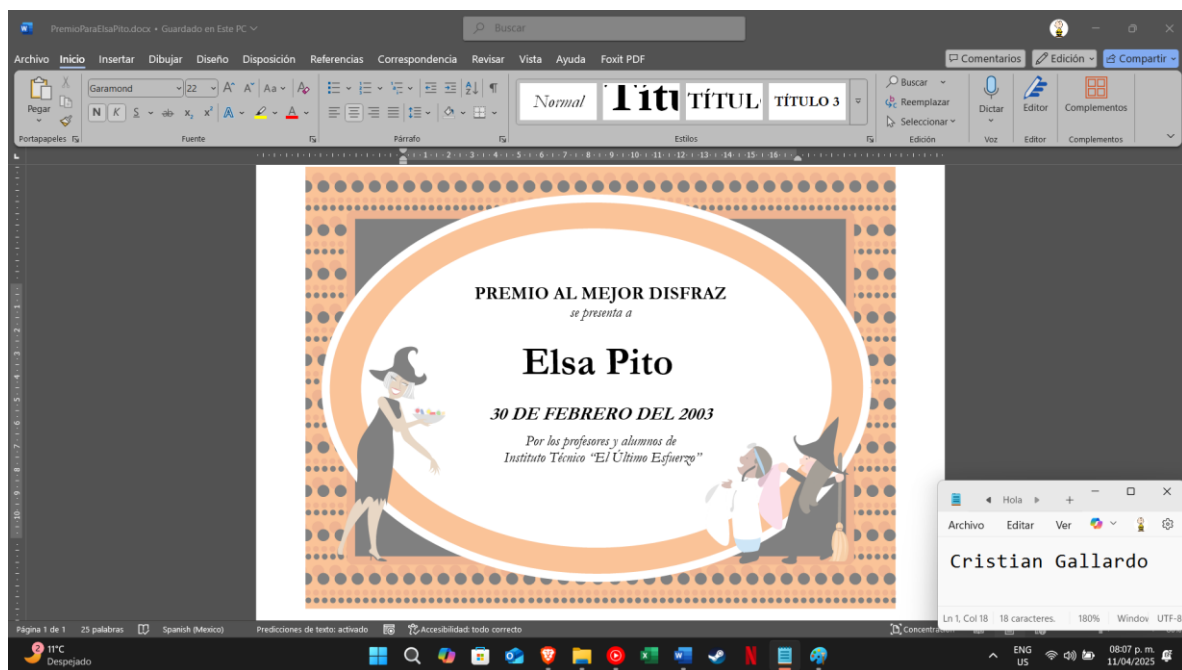
4. Con la ayuda del sitio web: <https://products.aspose.app/pdf/es/hash-generator/sha1>

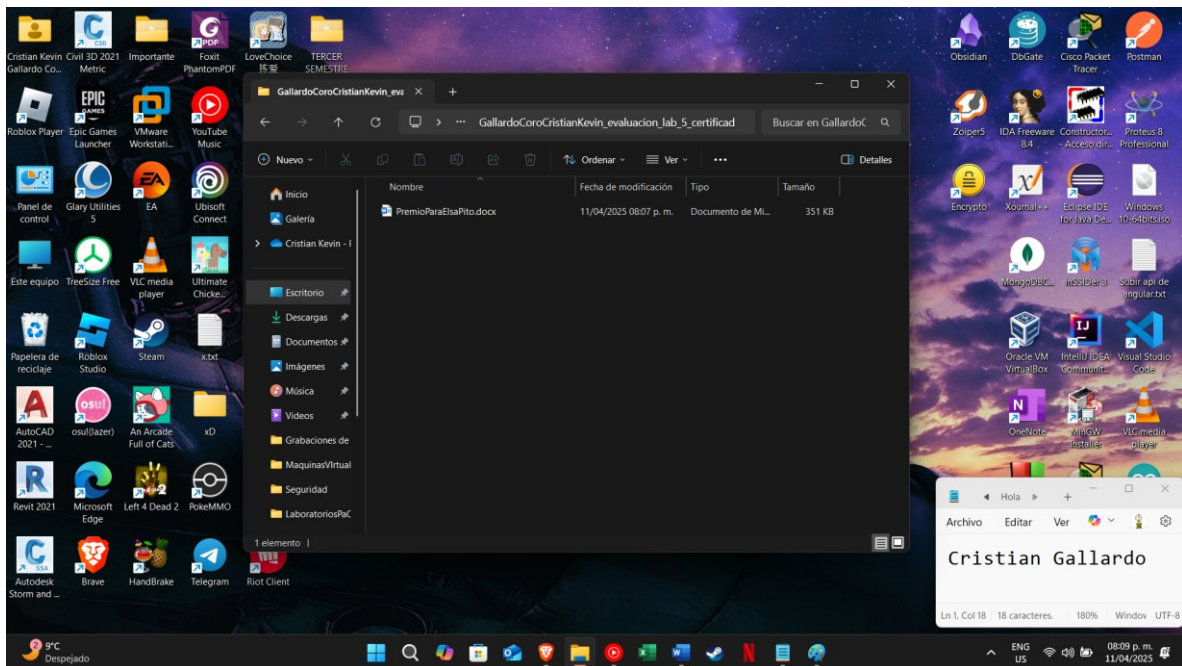
Realice la simulación siguiente:

Ud. es una entidad educativa, que está generando certificados de un curso que brindó, ahora está preparando los mismos para hacer llegar de forma virtual a los participantes. Busque una alternativa para que los certificados que genere puedan ser controlados si es que sufren modificación.

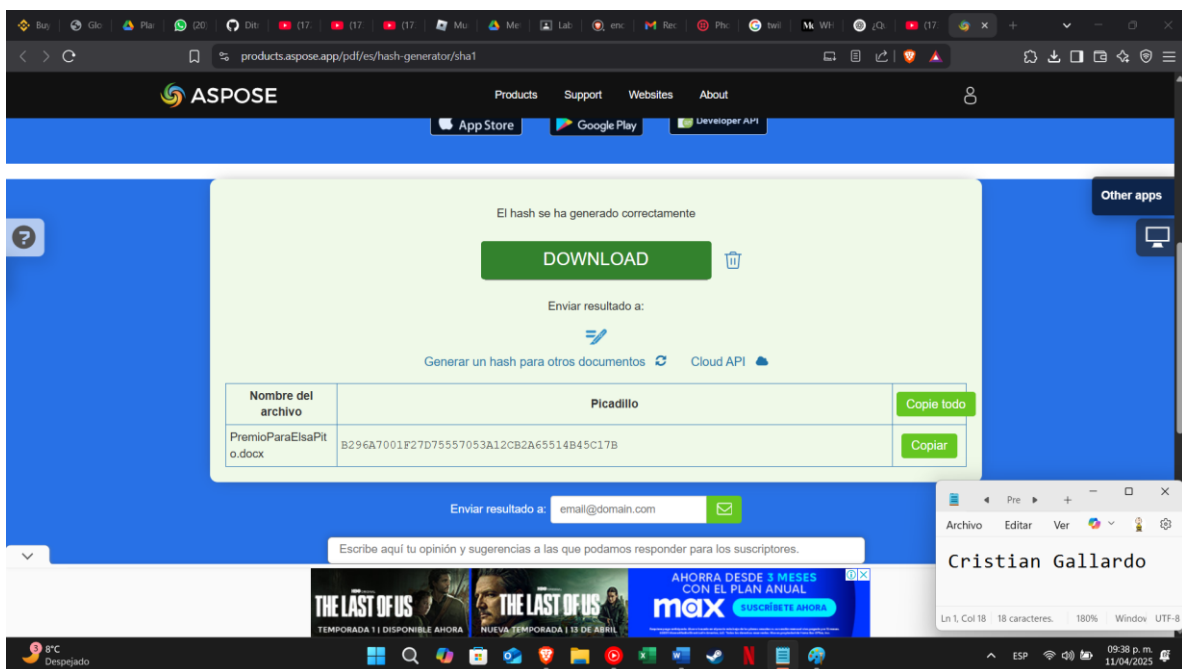
Explique su solución y cómo realizará el control.

Primeramente, una vez realizado el certificado correspondiente en el programa de su preferencia, en mi caso Word, se procede a guardar el certificado para luego ser enviado.

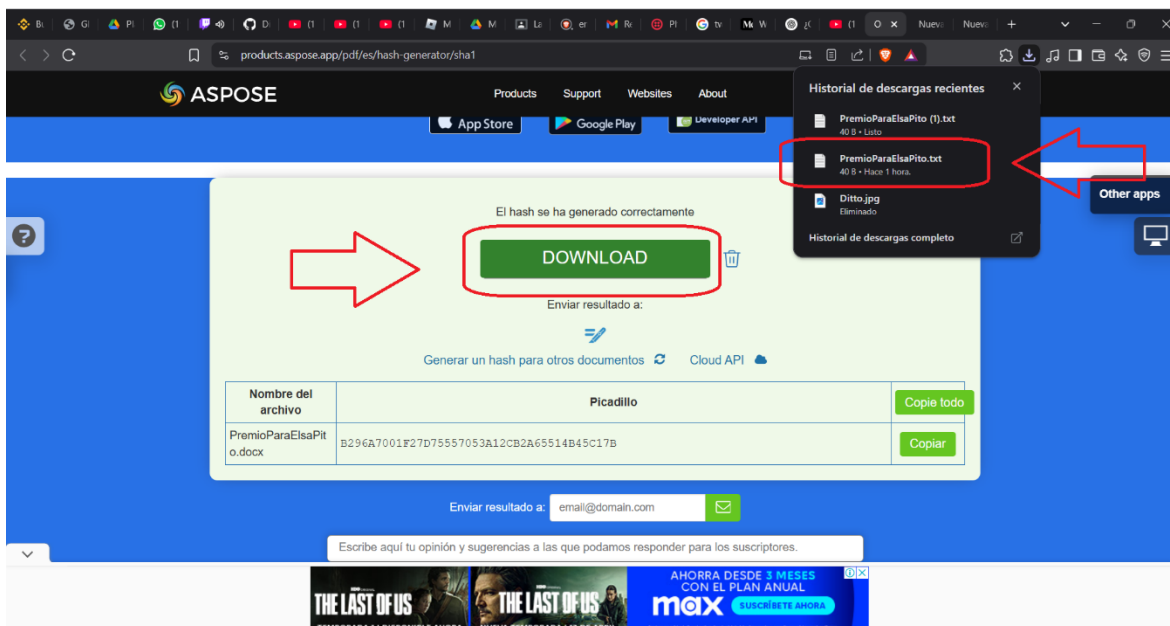




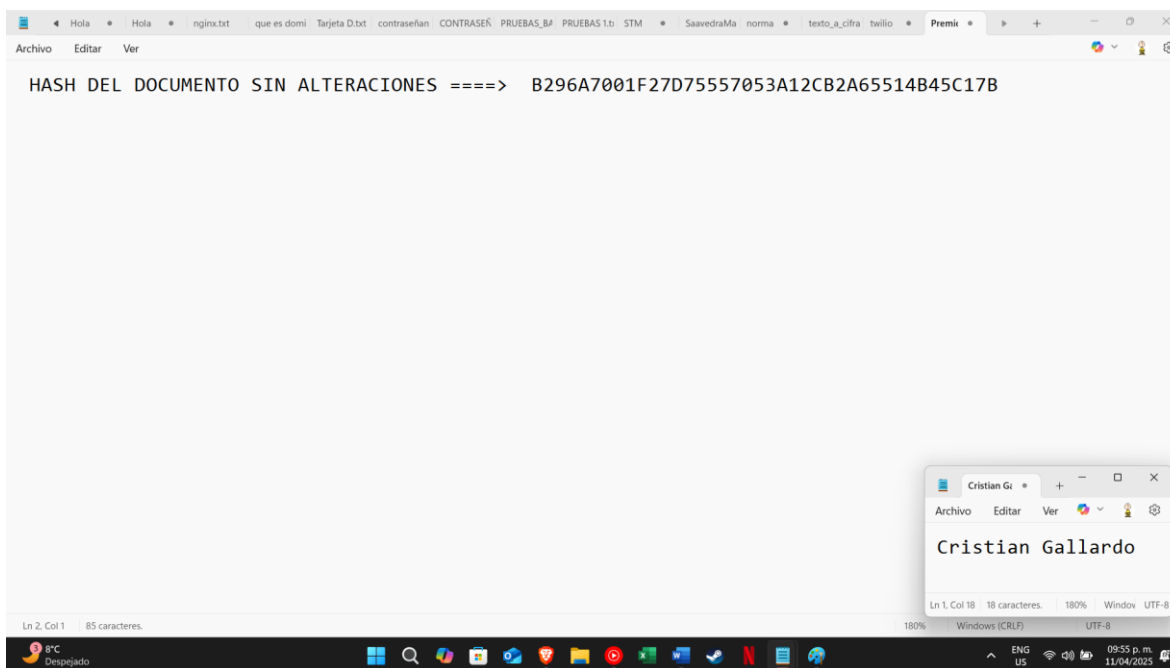
Una vez guardado el documento lo siguiente seria llevarlo a la página que se nos brindó para generar el hash correspondiente



Descargaremos el hash generado por la página el cual nos entregara un documento .txt el cual almacenaremos



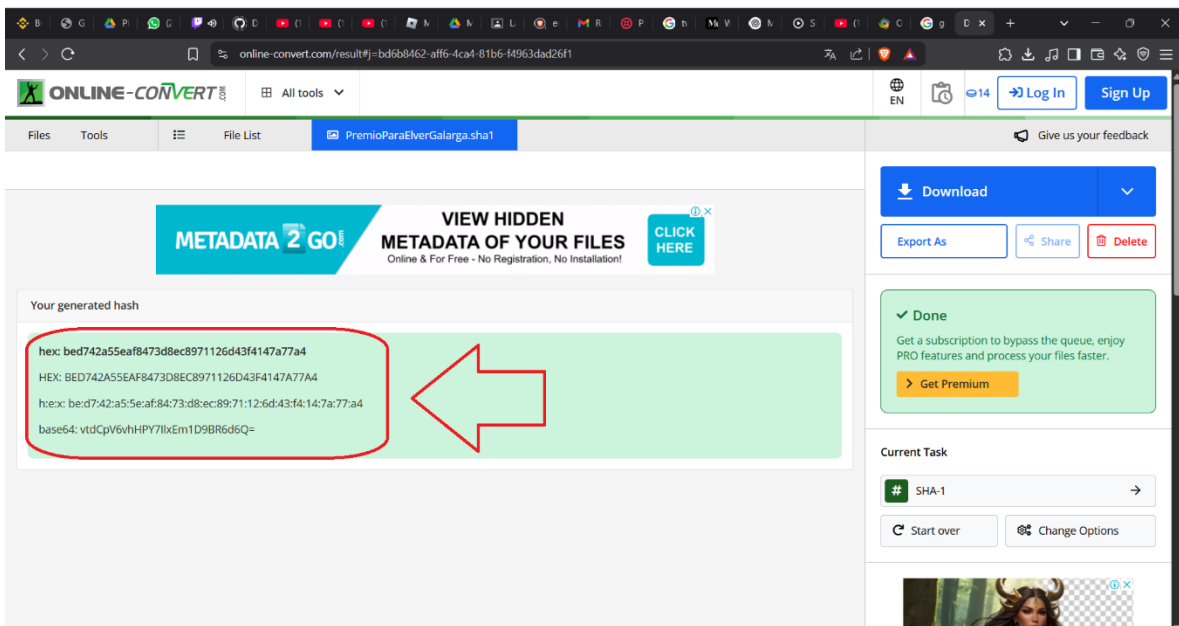
Teniendo la información del hash con cualquier alteración que se haya hecho en el documento automáticamente el valor que tenía el hash cambiará invalidando completamente la documentación presentada, a continuación, se hará una demostración del cambio



Realizaremos un cambio al nombre, simulando una alteración al certificado intentando falsificarlo



Al generar el hash con el documento modificado este cambiará, demostrándonos en efecto que el certificado no es válido



(Perdon auxi, por realizar algunas pruebas, se me acabaron los intentos disponibles en la otra pagina)

The screenshot shows a Windows desktop environment. In the background, a code editor window is open, displaying two lines of text:

```
HASH DEL DOCUMENTO SIN ALTERACIONES ====> B296A7001F27D75557053A12CB2A65514B45C17B
HASH DEL DOCUMENTO CON ALTERACIONES ====> BED742A55EAF8473D8EC8971126D43F4147A77A4
```

Below the code editor, a smaller window titled "Cristian Gallardo" is visible, showing the name "Cristian Gallardo" and some status information at the bottom: "Ln 1, Col 18 18 caracteres. 180% Window UTF-8". The Windows taskbar at the bottom shows the date and time as "10:35 p.m. 11/04/2025" and the language as "ENG US".

En resumen, de la realización y la solución, lo que primero debería de hacerse al crear el certificado es generar un hash de este, y una vez ya se tenga este hash almacenarla en una base de datos junto con el nombre del estudiante y el título del certificado y este se le ofrecerá al estudiante, para verificar la veracidad de esto el tendría que enviar el documento, para revisar si este cambió o no.