ECIES

(Proyecto 3)

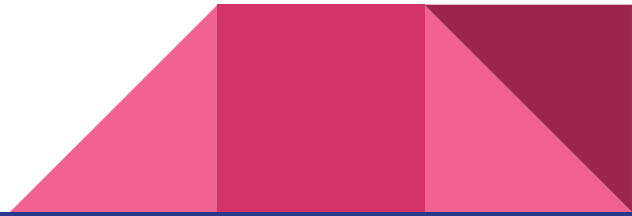
Canek García [kaan.ek@ciencias.unam.mx]

Parte 1

(Código)

Especificación general

Elaborar un programa que reciba el conjunto K = {(E, **P**, m, **Q**, **n**) : Q=mP} y un mensaje en claro; este programa devolverá el cifrado y descifrado de dicho mensaje. El programa deberá usar el criptosistema simplificado de ECIES.



Detalles de la especificación

1. pueden utilizar E, **P**, m, **Q**, **n** adecuados, para evitar usar números muy grandes.
2. Pueden utilizar algoritmos que ya se desarrollaron en las prácticas pasadas.
3. Pueden utilizar bibliotecas auxiliares para llevar a cabo operaciones complejas, pero el algoritmo principal del criptosistema de ECIES se debe apreciar.

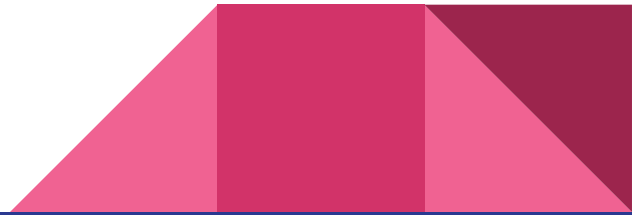
Parte 2

(Reporte)

Especificación del reporte

En clase vimos las técnicas de **XSS** (Cross Site Scripting) y **SQLinjection**. Utilizando el código visto en clase para **XSS** o la herramienta **sqlmap**, elaborar un breve reporte escrito con capturas de pantalla referente a estas herramientas.

Nota: Basta con documentar una técnica de las mencionadas, ustedes deciden cual eligen.



Detalles del reporte

- Para **XSS**, encontrar un sitio web (distinto a los vistos en clase) que presente esta vulnerabilidad, e inyectar una imagen de un servicio remoto, así como mostrar que se puede ejecutar código JavaScript ajeno a la página web original (pueden utilizar el mismo código JavaScript visto en clase). Incluir captura de pantalla del sitio web que muestre el antes y el después de la ejecución del código XSS.
- Con base en la documentación CSP (también visto en clase), proponer una posible solución para mitigar la falla que encontraron.

- Para **SQLinjection**, utilizar la herramienta **sqlmap**.
  Con base en la documentación de sqlmap y el análisis de los comandos vistos en clase, del sitio http://testphp.vulnweb.com/:

  1) Utilizar el parámetro cat en la url para detectar fallas y poder usar sqlmap.
  2) Obtener tablas de la base de datos: **information_schema.**
  3) Obtener el nombre de las columnas de la tabla: **KEYWORDS.**
  4) Obtener los datos de las columnas: **RESERVED** y **WORD**.

Notas

Notas adicionales

- El código fuente puede ser entregado en **Java 8+**, **C/C++** o **Python 3**. El reporte debe ser entregado en formato **PDF**.
- Desarrollar la práctica en equipos de **uno**, **dos** o **tres integrantes**.
- **Documentar** el código fuente e incluir el **nombre completo** de los integrantes en el método **main** del programa, de igual manera incluir los nombres en el reporte escrito.
- Entregar el código y el reporte el día **8 de diciembre de 2022**.
- Enviar el código fuente y reporte por medio de la plataforma **ClassRoom**. (al menos un integrante, pero de preferencia todos los miembros del equipo sin importar que se repita esta entrega).