Universidad Nacional Autónoma de México
Facultad de Ciencias

Facultad de CIencias

Criptografía y Seguridad

Semestre: 2025-1

Equipo: Pingüicoders

Práctica 10:
Curvas elípticas y protocolo de Diffie-Hellman

Arrieta Mancera Luis Sebastián - 318174116
Cruz Cruz Alan Josue - 319327133
García Ponce José Camilo - 319210536
Matute Cantón Sara Lorena - 319331622

Introducción:

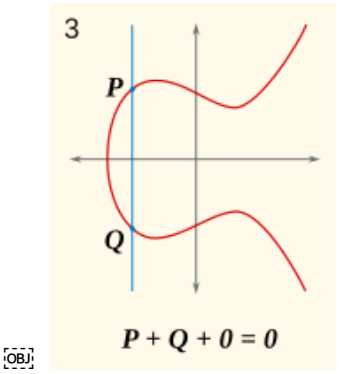
Durante el curso hemos revisado diversos sistemas criptográficos, principalmente aquellos que forman parte de los cimientos de criptografía, los cuales hoy en día no son usados en el ambiente laboral debido a que no son seguros. Por esto último es importante conocer la criptografía de curvas elípticas, una técnica relativamente moderna la cual cifra los mensajes de tal manera que es fácil de cifrar y muy complicada de descifrar. Para este método es importante que conozcamos cómo funciona al igual que las operaciones de curvas elípticas.

Nota:

Nuestro código se puede tardar mucho en encontrar el punto aleatorio o algunas veces se queda trabado, para resolver esto comentar la línea 172 de Entity.py.

Preguntas:

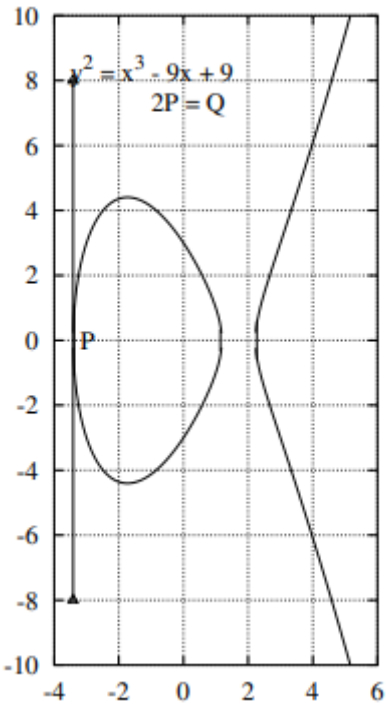
1. **Cuando sumamos un punto P con −P, que nos da como resultado el punto al infinito... ¿Qué quiere decir que un punto sea infinito?**
   Un punto es infinito cuando, al ver gráficamente la operación de suma, la recta que une a estos dos puntos es paralela al eje de las ordenadas tal que se extiende infinitamente por él sin volver a tocar a la curva elíptica. Como se muestra a continuación:



   fuente: https://es.wikipedia.org/wiki/Curva_el%C3%ADptica

   Veamos que la recta va a crecer infinitamente sin llegar a volver a tocar a la curva.

2. **Cuando sumamos un punto P consigo mismo, ¿qué característica tiene la recta que conecta a estos 2 puntos?**
   Para empezar esta recta se dibuja en el punto P y dependiendo de donde se encuentra la coordenada y de nuestro punto P. Si y es diferente a 0, entonces la recta que une a estos puntos va a cruzar a la curva exactamente dos veces, en el punto P y el punto -P, un ejemplo de como se ve esto se puede encontrar en el ejercicio anterior.
   En el caso contrario y y=0, entonces la recta cruzara a la curva exactamente una única vez en el punto P, como se muestra a continuación:



Fuente: Curvas Elípticas

En ambos casos esta recta va a a ser paralela al eje de las ordenadas y por lo tanto de igual manera es un punto al infinito.

3. **¿En qué otro cifrado se utiliza el protocolo Diffie-Hellman?**
   El protocolo Diffie-Helmman (DH) es utilizado en **SSL/TLS** como Diffie Hellman Efímero (DHE), esta es una implementación más segura porque proporciona un secreto directo perfecto, generalmente se combina con un algoritmo como **DSA** o **RSA** para autenticar una o ambas partes en la conexión. El cifrado **IPsec** es una función de software que codifica los datos para proteger su contenido frente a partes no autorizadas, las claves simétricas de este cifrado derivan de las claves del protocolo DH compartidas entre pares. El protocolo tambien puede utilizarse en **PGP/GPG** por ejemplo para generar claves PGP utilizando una subclave del cifrado Diffie Hellman.
4. **¿Cuántos bits de una llave de una curva necesitamos para poder igualar la seguridad en una llave de RSA?**
   Respuesta: Con ECC se obtiene una fuerza criptográfica equivalente con tamaños de clave significativamente menores, para conseguir la fuerza criptográfica equivalente a cifrar utilizando una clave simétrica de 112 bits en ECC se necesitaría una clave RSA de 2048 bits. A continuación se muestra la comparación:

Comparación del tamaño de las claves:

Tamaño de clave simétrica (bits)	Tamaño RSA (bits)	Tamaño de clave de curva elíptica (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Tamaños de clave recomendados según el NIST

5. **En el ejemplo, en attack tenemos que la letra 't' es cifrada a 2 puntos diferentes de la curva, y sigue siendo recuperable. ¿Qué valor hace esto posible?**

   El valor que hace esto posible es el **valor aleatorio** que se usa para generar un punto aleatorio en la curva durante el cifrado. Los valores aleatorios generan diferentes puntos de la curva asociados al mensaje, sin embargo, la función de descifrado está diseñada para eliminar cualquier término dependiente del valor aleatorio, lo que asegura que el mensaje original pueda recuperarse.

6. **Cifra el mensaje: Perro salchicha, gordo bachicha usando la curva elíptica EC233(−2, 8) usando los 256 caracteres del código ASCCI. Pega la ejecución de la salida del main**

   Bob cifra el mensaje "Perro salchicha, gordo bachicha" como:
   Random r: 87
   P->((52, 53))= -> ;

   P->((77, 147))= -> P

   Random r: 26
   e->((227, 81))= -> Î

   e->((103, 15))= -> e

   Random r: 210
   r->((105, 186))= -> h

r->((122, 141))= -> r

Random r: 61
r->((194, 101))= -> ´

r->((122, 141))= -> r

Random r: 167
o->((214, 118))= -> Ç

o->((116, 51))= -> o

Random r: 123
 ->((25, 122))= -> "

 ->((24, 152))= ->

Random r: 81
s->((200, 46))= -> ¸

s->((123, 103))= -> s

Random r: 134
a->((169, 159))= ->

i->((106, 101))= -> i

Random r: 75
c->((138, 206))= -> |

c->((101, 108))= -> c

Random r: 140
h->((64, 83))= -> G

h->((105, 186))= -> h

Random r: 140
a->((64, 83))= -> G

a->((95, 59))= -> a

Random r: 134
,->((169, 159))= ->

h->((105, 186))= -> h

Random r: 141
i->((138, 27))= -> {

i->((106, 101))= -> i

Random r: 84
c->((142, 52))= -> }

c->((101, 108))= -> c

Random r: 198
h->((180, 103))= -> ¦

h->((105, 186))= -> h

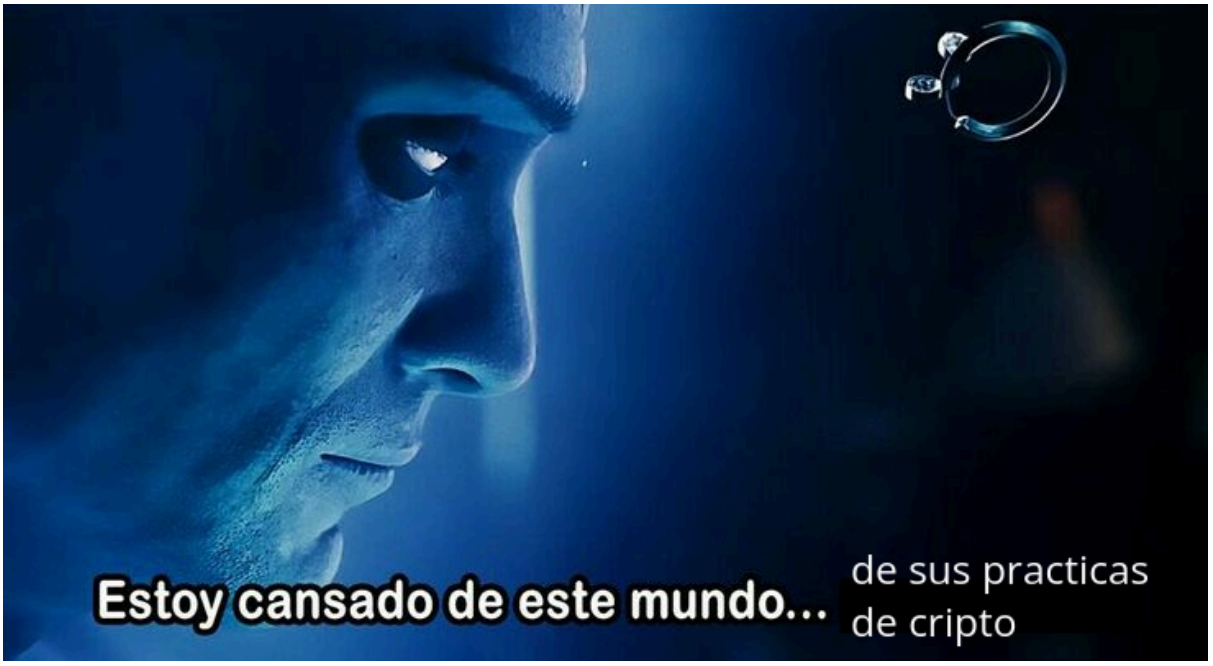
Random r: 79
a->((0, 63))= ->

a->((95, 59))= -> a

Mensaje cifrado: [(';', 'P'), ('Î', 'e'), ('h', 'r'), ('´', 'r'), ('Ç', 'o'), ('"', ' '), ('¸', 's'), ('\x9f', 'a'), ('"', 'l'), ('k', 'c'), ('\x11', 'h'), ('\x97', 'i'), ('|', 'c'), ('G', 'h'), ('G', 'a'), ('\x9f', ','), ('Ò', ' '), ('e', 'g'), ('b', 'o'), ('µ', 'r'), ('\x1c', 'd'), ('(', 'o'), ('Ì', ' '), ('\x1c', 'b'), (' ', 'a'), ('±', 'c'), ('\x86', 'h'), ('{', 'i'), ('}', 'c'), ('¦', 'h'), ('\x01', 'a')]

Conclusiones:

Con esta práctica comprendimos el funcionamiento del cifrado con curvas elípticas y sus ventajas sobre otros sistemas de cifrado como RSA. Aprendimos cómo se introducen propiedades matemáticas y aleatoriedad para ser un sistema criptográfico robusto y con claves de menor longitud, lo que optimiza el cifrado y el descifrado. En cuanto al curso, es cierto que la carga de trabajo es pesada, sin embargo, estaría bien que algunas prácticas se quedaran solamente en teoría y se quedaran las que tienen que ver más con cifrados, virus y hackeos. Esto haría que tanto las tareas como las prácticas sean más digeribles y comprendamos mejor los temas, ya que muchas veces se juntaban y no se terminaban de comprender al 100%. A continuación nuestra más humilde reacción:



Referencias:

- https://delta.cs.cinvestav.mx/~francisco/cripto/ellipticbg.pdf
- *Crypt4You*. (s. f.). https://criptored.es/crypt4you/temas/ECC/leccion1/leccion1.html#02
- Serengil, S. (2023, 29 septiembre). *Understanding Identity Element in Elliptic Curves - Sefik Ilkin Serengil*. Sefik Ilkin Serengil. https://sefiks.com/2023/09/29/understanding-identity-element-in-elliptic-curve/
- Thomas Pornin. (2013, August 26). Diffie-Hellman is used in SSL/TLS, as "ephemeral Diffie-Hellman" (the cipher suites with "DHE" in their name; see the standard). [Respuesta a la pregunta: Diffie-Hellman and its TLS/SSL usage] Stack Exchange. https://security.stackexchange.com/questions/41205/diffie-hellman-and-its-tls-ssl-usage
- AWS. (s.f.). ¿Qué es un certificado SSL/TLS? https://aws.amazon.com/es/what-is/ssl-certificate/
- f5. (s.f.). ¿Qué es el cifrado SSL/TLS? https://www.f5.com/es_es/glossary/ssl-tls-encryption
- Ciberseguridad. (s.f.). Qué es el intercambio de claves Diffie-Hellman y cómo funciona. https://ciberseguridad.com/guias/recursos/intercambio-claves-diffie-hellman/#:~:text=Diffie%2DHellman%20ef%C3%ADmero%3A%20se%20considera,que%20se%20ejecuta%20el%20protocolo.
- AWS. (s.f.). ¿Qué es IPsec?. https://aws.amazon.com/es/what-is/ipsec/

- Fortinet. (s.f.). Encriptación PGP. https://www.fortinet.com/lat/resources/cyberglossary/pgp-encryption
- Check Point. (s.f.) IPsec and IKE. https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SitetoSiteVPN_AdminGuide/Topics-VPNSG/IPsec-and-IKE.htm
- Sectigo. (2021, January 05). ¿Cuáles son las diferencias entre los algoritmos de cifrado RSA, DSA y ECC? https://www.sectigo.com/es/recursos/rsa-vs-dsa-vs-ecc-encryption