

Práctica 3 - Intercambio de llaves de Diffie-Hellman Criptografía y Seguridad 2023-2

Anayanzi Delia Martínez Hernández
anayanzi@ciencias.unam.mx

Ivan Daniel Galindo Perez
ivangalindo@ciencias.unam.mx

Luis Fernando Yang Fong Baeza
fernandofong@ciencias.unam.mx

Enero 2023

1 Introducción

En la criptografía de llave pública, es importante poder realizar un intercambio de llaves en un canal inseguro para poder realizar una comunicación segura (cifrada) entre dos o más sistemas, Diffie-Hellman es un algoritmo que garantiza tal cosa utilizando teoría de números.

2 Algoritmo

Sean p un primo y g una raíz primitiva de \mathbb{Z}_p y supongamos que se desea realizar un intercambio de llaves entre Alice y Bob.

1. Alice escoge un número secreto a y le manda a Bob el cálculo de $A \equiv g^a \pmod{p}$.
2. Bob ahora escoge un número secreto b y le envía a Alice $B \equiv g^b \pmod{p}$.
3. Alice calcula $s \equiv B^a \pmod{p}$
4. Bob calcula $s \equiv A^b \pmod{p}$
5. s es el mismo número para Alice como para Bob, puesto que como g es una raíz primitiva, entonces se cumple que:

$$A \equiv g^a \pmod{p}$$

$$A^b \equiv (g^a)^b \mod p$$

$$A^b \equiv (g^b)^a \mod p$$

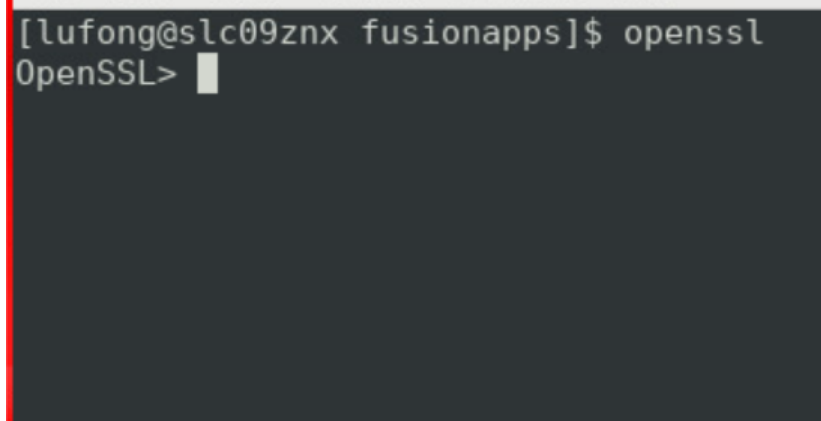
$$A^b \equiv B^a \mod p$$

Por lo tanto, se compartió el mismo número sin necesidad de intercambiar algo más que la raíz primitiva g y el primo p .

Afortunadamente, este algoritmo ya tiene una implementación completamente funcional y eficiente para utilizarse siempre en el mundo real y viene instalada por defecto en la mayoría de las paqueterías de Linux que es **OpenSSL**.

3 Desarrollo

Antes de empezar, hay que verificar que se tiene instalado OpenSSL, esto se hace con el comando `openssl` y debería de resultar un prompt como el que se muestra a continuación:



```
[lufong@slc09znx fusionapps]$ openssl
OpenSSL> █
```

Figure 1: Prompt de OpenSSL

En caso de no tener instalado openssl, se debera de utilizar el comando:

```
sudo apt-get install openssl -y
```

Esta práctica requerirá de interacción con los ayudantes para que sea 100% claro el funcionamiento del intercambio de llaves de manera práctica. Ahora, en los archivos de la práctica, se incluyen los siguientes dos archivos:

- `parametros.pem`
- `ayudantes.pub.key`

El archivo `parametros.pem` corresponde a g y p , con esto es más que suficiente para que se puedan crear llaves privadas, puesto que basta con escoger un número al azar, con el comando:

```
openssl genpkey -paramfile parametros.pem -out
<nombre_llave_privada>.pem
```

Esta es la llave privada, no debe de ser compartida jamás (puesto que si no cualquiera obtendría las llaves y no sirvió de nada).

Lo que hay que generar ahora, es la llave pública, con el comando:

```
openssl pkey -in <nombre_llave_privada>.pem -pubout -out
<nombre_llave_publica>.pub_key
```

Una vez creada tu llave privada, mandar la llave publica a cualquiera de los ayudantes (en cualquier momento), la respuesta debera de ser un archivo cifrado (con extensión `.bin`) el cual fue cifrado utilizando la última parte del algoritmo.

Puedes continuar con esta parte de la práctica aunque el ayudante no haya contestado. Ahora se necesita obtener el número compartido entre las dos llaves, que es la llave con que fue cifrado el archivo que te dará el ayudante, para poder calcular este secreto, utiliza el comando:

```
openssl pkeyutl -derive -inkey <nombre_llave_privada>.pem -peerkey
ayudantes.pub_key -out secreto
```

Esta parte no se puede continuar hasta que no haya respondido el ayudante.

Si ya fue obtenida la respuesta del ayudante, entonces se debe de descargar el archivo y con el comando que se muestra a continuación, reporta en un PDF o archivo de texto la bandera que te fue otorgada.

```
openssl enc -d -aes-128-cbc -nosalt -kfile secreto -in
<archivo_ayudante>.bin
```

Si se desean visualizar los archivos de manera más entendible, entonces se pueden utilizar los siguientes tres comandos.

Para visualizar los parámetros (otorgados por los ayudantes)

```
openssl pkeyparam -in params.pem -text
```

Que deberá de mostrar la siguiente pantalla:

```
[lufong@slc09znx ~/Diffie-Hellman]$ openssl pkeyparam -in params.pem -text
-----BEGIN DH PARAMETERS-----
MIGHAoGBAJOBQVktDes4e8+xvuK72S7W5Ko1rQJivd3ryxRPXlJveJw4CqBpB3HQ
4q0v5IeM1+5em6M1W+zR1t8bQzAFGhMdIo8tnQfF2CvTQapGtLK6FGL20kHU9h/M
MQUPsSkLAHdoFm1UVH3+3ZersPxIlt/EoiHo/Skcb9/Ukt+Q0ltzAgEC
-----END DH PARAMETERS-----
DH Parameters: (1024 bit)
  prime:
    00:93:81:41:59:2d:0d:eb:38:7b:cf:b1:be:e2:bb:
    d9:2e:d6:e4:aa:35:ad:02:62:bd:dd:eb:cb:14:4f:
    5e:52:6f:78:9c:38:0a:a0:69:07:71:d0:e2:a3:af:
    e4:87:8c:d7:ee:5e:9b:a3:35:5b:ec:d1:d6:df:1b:
    43:30:05:1a:13:1d:22:8f:2d:9d:07:c5:d8:2b:d3:
    41:aa:46:b4:b2:ba:14:69:76:3a:41:d4:f6:1f:cc:
    31:05:0f:b1:29:0b:00:77:68:16:6d:54:54:7d:fe:
    dd:91:2b:b0:fc:48:96:df:c4:a2:21:e8:fd:29:1c:
    6f:df:d4:92:df:90:3a:5b:73
  generator: 2 (0x2)
[lufong@slc09znx ~/Diffie-Hellman]$
```

Figure 2: Mostrando los parámetros para Diffie-Hellman

Para visualizar la llave privada (generada por el alumno)

```
openssl pkey -in <llave_privada>.pem -text -noout
```

Mostrando la siguiente salida:

```

[lufong@slc09znx ~/Diffie-Hellman]$ openssl pkey -in ayudantes.pem -text -noout
DH Private-Key: (1024 bit)
  private-key:
    68:24:f2:4e:22:5c:cc:fc:00:79:c1:6a:4b:f4:72:
    93:fa:6f:78:41:5c:c7:54:38:9c:a0:19:fd:0a:bb:
    8b:02:95:fa:98:a3:a7:2b:eb:e6:50:c5:b4:0d:46:
    64:1f:9c:70:7b:c8:3b:d5:e0:79:3b:00:ef:fc:ee:
    a3:b1:b7:c8:8b:36:94:42:d8:36:5d:34:5e:4f:7f:
    d0:65:54:c4:6b:c5:74:40:de:e2:04:61:d3:54:a0:
    d7:50:6e:9e:5b:fc:9b:29:11:ee:6a:d9:18:4a:90:
    47:47:84:d5:70:9f:7c:57:b6:fe:d7:ef:eb:c4:1b:
    cd:31:ce:38:62:a0:e0:4b
  public-key:
    26:13:93:0e:f6:19:12:25:a2:68:c3:be:a5:8d:bc:
    37:3e:66:e1:3d:db:c0:5b:9c:13:22:bf:09:15:4f:
    25:54:43:42:b9:51:97:d7:72:79:ae:e4:f6:01:5a:
    0b:02:96:4a:62:7d:06:d4:64:f4:4f:7e:a0:c7:09:
    08:8c:ec:b9:6d:db:24:1e:da:30:8c:da:e0:6e:65:
    4d:5b:00:72:79:7f:86:b1:7c:6a:4d:e2:91:7e:1c:
    54:e4:8c:39:57:86:29:8c:01:04:58:c2:59:1a:82:
    b9:97:0d:1f:51:a5:4d:f8:2d:e6:9e:f7:1e:3c:5d:
    21:39:e8:05:94:93:47:19
  prime:
    00:93:81:41:59:2d:0d:eb:38:7b:cf:b1:be:e2:bb:
    d9:2e:d6:e4:aa:35:ad:02:62:bd:dd:eb:cb:14:4f:
    5e:52:6f:78:9c:38:0a:a0:69:07:71:d0:e2:a3:af:
    e4:87:8c:d7:ee:5e:9b:a3:35:5b:ec:d1:d6:df:1b:
    43:30:05:1a:13:1d:22:8f:2d:9d:07:c5:d8:2b:d3:
    41:aa:46:b4:b2:ba:14:69:76:3a:41:d4:f6:1f:cc:
    31:05:0f:b1:29:0b:00:77:68:16:6d:54:54:7d:fe:
    dd:91:2b:b0:fc:48:96:df:c4:a2:21:e8:fd:29:1c:
    6f:df:d4:92:df:90:3a:5b:73
  generator: 2 (0x2)

```

Figure 3: Mostrando la llave pública, privada, el primo p y generador g

Para visualizar la llave pública (la de los ayudantes o la del alumno)

```
openssl pkey -pubin -in <archivo>.pub_key -text -noout
```

Y mostraria la ultima pantalla:

```
[lufong@slc09znx ~/Diffie-Hellman]$ openssl pkey -pubin -in ayudantes.pub_key -text -noout
DH Public-Key: (1024 bit)
  public-key:
    26:13:93:0e:f6:19:12:25:a2:68:c3:be:a5:8d:bc:
    37:3e:66:e1:3d:db:c0:5b:9c:13:22:bf:09:15:4f:
    25:54:43:42:b9:51:97:d7:72:79:ae:e4:f6:01:5a:
    0b:02:96:4a:62:7d:06:d4:64:f4:4f:7e:a0:c7:09:
    08:8c:ec:b9:6d:db:24:1e:da:30:8c:da:e0:6e:65:
    4d:5b:00:72:79:7f:86:b1:7c:6a:4d:e2:91:7e:1c:
    54:e4:8c:39:57:86:29:8c:01:04:58:c2:59:1a:82:
    b9:97:0d:1f:51:a5:4d:f8:2d:e6:9e:f7:1e:3c:5d:
    21:39:e8:05:94:93:47:19
  prime:
    00:93:81:41:59:2d:0d:eb:38:7b:cf:b1:be:e2:bb:
    d9:2e:d6:e4:aa:35:ad:02:62:bd:dd:eb:cb:14:4f:
    5e:52:6f:78:9c:38:0a:a0:69:07:71:d0:e2:a3:af:
    e4:87:8c:d7:ee:5e:9b:a3:35:5b:ec:d1:d6:df:1b:
    43:30:05:1a:13:1d:22:8f:2d:9d:07:c5:d8:2b:d3:
    41:aa:46:b4:b2:ba:14:69:76:3a:41:d4:f6:1f:cc:
    31:05:0f:b1:29:0b:00:77:68:16:6d:54:54:7d:fe:
    dd:91:2b:b0:fc:48:96:df:c4:a2:21:e8:fd:29:1c:
    6f:df:d4:92:df:90:3a:5b:73
  generator: 2 (0x2)
```

Figure 4: Llave pública de los ayudantes

Cabe aclarar que las notaciones `.pem` y `.pub_key` son una mera convención, no necesariamente tienen que tener estas extensiones pero es más sencillo con estas extensiones para saber de qué clase de archivos se tratan.

4 Evaluación

Para obtener la calificación completa de esta práctica, basta con regresar la bandera correctamente, para obtener calificación parcial (en caso de que no se haya obtenido la bandera), mostrar mediante capturas de pantalla el procedimiento realizado y la calificación dependerá de hasta qué punto se haya llegado en la práctica.

5 Entregables

Se deberá de entregar el PDF o archivo de texto con la bandera descifrada o en su defecto el PDF con capturas de pantalla explicadas de hasta donde se logró avanzar, todo vía Classroom antes de las 23:59:59 de la fecha designada en la misma plataforma.