Tareas 5 y 6

Criptografía y seguridad 2020-2

Fecha límite de entrega: 30 de mayo

Indicaciones

- Resuelve los 9 ejercicios.
- Puede hacerse de forma individual o en pareja, en caso de hacerla en pareja basta que se entregue una solución.
- Sube tu tarea solo cuando estés completamente seguro de que es correcta, ya que solo se puede subir una vez.
- Escribe los cálculos que realizaste, o en caso de haber usado otra herramienta (como un programa) indícalo en tu respuesta.
- Organiza tus archivos en un archivo `.zip`, incluyendo los datos de los alumnos, y súbelo en `https://forms.gle/WgqKXxuwYPYwNhBb7`

Ejercicios

1. Acabas de intervenir la comunicación de un sistema que usa RSA.

   a) Si detectas que se envió el mensaje cifrado $c = 10$ al usuario que tiene clave pública $e = 5, N = 35$, ¿cuál es el mensaje claro?

   b) Si la clave pública de un usuario es $e = 31, N = 3599$, ¿cuál es la clave privada correspondiente?

2. Considera el esquema de ElGamal sobre $\mathbb{Z}_{71}^*$, con elemento generador $g = 7$.

   a) Si Bartolo tiene clave pública $Y_B = 3$ y Alicia escoge el entero $k = 2$, ¿cuál es el mensaje cifrado de $M = 30$?

   b) Si ahora Alicia escoge otro valor para k de manera que el cifrado de $M = 30$ es la pareja $(59, C_2)$, ¿cuál es el valor de C_2?

3. Cómo verificar si un entero positivo N es una potencia de un número. Sea $n = \lfloor \log N \rfloor + 1 =$ longitud en bits de N.

   a) Muestra que si $N = m^e$, para algunos enteros $m, e > 1$, entonces $e < n$.

   b) Dados N y e, donde $2 \leq e \leq n+1$, muestra cómo determinar si existe m tal que $N = m^e$. *Hint:* Usa búsqueda binaria en el rango $[2, N]$.

   c) Dado N, muestra cómo determinar si N es una potencia de un entero.

   La complejidad de los algoritmos debe ser polinomial en n. Justifica en ambos casos.

4. Intercambio de clave.

   a) Describe un ataque de hombre en el medio sobre el protocolo de Diffie-Hellman, donde un adversario comparte una clave k_a con Alice y una clave diferente k_b con Bob, y Alice y Bob no pueden detectar esta intervención.

   b) Se tiene el siguiente protocolo de intercambio de clave:

      I) Alicia escoge $k, r \leftarrow \{0,1\}^n$ al azar y envía $s := k \oplus r$ a Bartolo.
      II) Bartolo escoge $t \leftarrow \{0,1\}^n$ al azar y manda $u := s \oplus t$ a Alicia.
      III) Alicia calcula $w := u \oplus r$ y manda w a Bartolo.
      IV) Alicia devuelve k y Bartolo devuelve $w \oplus t$.

      Verifica que Alicia y Bartolo devuelven la misma clave, luego muestra que si Eva puede ver los mensajes intercambiados, entonces puede recuperar la clave.

5. El siguiente protocolo sirve para que Alice y Bob generen un bit aleatorio.

   I) Una entidad confiable T publica su llave pública pk.
   II) Alice escoge un bit aleatorio b_A, lo encripta usando pk, con lo que obtiene c_A y lo manda a Bob y a T.
   III) Luego de recibir c_A, Bob hace lo mismo que Alice y manda $c_B \neq c_A$.
   IV) T descifra c_A y c_B y anuncia el resultado. Alice y Bob hacen un XOR del resultado y este es el bit de salida.

   Preguntas.

   a) Supón que Bob actúa honestamente pero Alice no. ¿Por qué aun así el bit de salida es aleatorio?

b) Supón que en el protocolo se usa el cifrado de El Gamal. Muestra de qué forma Bob puede manipular el bit de salida para que resulte lo que él quiera. (Un bit b se codifica como el elemento g^b.)

6. ¿Para qué es el siguiente código? En particular, ¿cuál es el significado de la entrada y la salida (n y p respectivamente)? ¿Qué propósito tiene la línea 7?

```
1  def funcion(n=16):
2      r = open('/dev/urandom', 'rb')
3      p = 4
4      while not test_miller_rabin(p):
5          s1 = r.read(n)
6          s2 = int.from_bytes(s1, 'big')
7          p = s2 | (1<<(n*8-1))
8      return p
```

7. (2 puntos) Para el sistema de ElGamal se tienen los siguientes parámetros de una curva elíptica $E\colon y^2 = x^3 + ax + b$ sobre $\mathbb{F}_p$ con generador G:

$$\begin{aligned} p &= 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1 \\ &= \texttt{0xffffffff00000001000000000000000000000000ffffffffffffffffffffffff} \\ a &= -3 \\ b &= \texttt{0x5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b} \\ G &= (\texttt{0x6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296}, \\ &\quad\ \texttt{0x4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5}) \end{aligned}$$

Usando la clave pública

$$\begin{aligned} Q = (&\texttt{0xbbb041abbc4b2e9973726520c0a47b9db7d7a8d4e534f5c75d58acd68bf413a1}, \\ &\texttt{0xc567543991c0d7aac45ac9c325f10b62c77189e3f0a34d977a448bde60590e2d}) \end{aligned}$$

se encriptó un mensaje $M \in E(\mathbb{F}_p)$ y como resultado se obtuvieron los puntos

$$\begin{aligned} C_1 = (&\texttt{0x26efcebd0ee9e34a669187e18b3a9122b2f733945b649cc9f9f921e9f9dad812}, \\ &\texttt{0x90238bde9cc7bb330d150c67704dd25ae7055205744b6f31bf4070745872d0e6}) \text{ y} \\ C_2 = (&\texttt{0x46c4b5cc528f15953943e0a775d3a6d08057b1fa30878473aaa28399198c4f8c}, \\ &\texttt{0x3edff2f73f7a89cfddc967ad9af2f36a06b690761a5d25810efe223f906ce63}). \end{aligned}$$

Encuentra M y describe el procedimiento. *Hint:* La llave secreta es pequeña. Usa Sage.

8. Se tiene la siguiente clave pública RSA

```
-----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKzl5VggSXb/Jm2oqkPeRQwtpmGlLnJT
Nre4LKx3VUljtLzYWj4xoG+aHBouwJT7DyeibpasCH8Yderr4zIGTNUCAwEAAQ==
-----END PUBLIC KEY-----
```

y un mensaje que fue cifrado con ella

```
0x41b4e1609390ff8fb5f225b010d1cc79253dcab1744d5f865daabad0e28d2591
41722382114d9a73106b4d429676dae60a1528a0eb3b73eab0e9d2165c72492f
```

Se usó un generador de números aleatorios deficiente, y enseguida de obtener los primos para la clave anterior se obtuvieron los primos para la clave siguiente

```
-----BEGIN PUBLIC KEY-----
MFOwDQYJKoZIhvcNAQEBBQADTAAwSQJCAPsrpwx56OTlKtGAWn24bo5HUg3xYtnz
nTj1X/8Hq7pLYNIVE57Yxoyr3zTOOBJufgTNzdKSORc5Ti4zZUkCkQvpAgMBAAE=
-----END PUBLIC KEY-----
```

Descifra el mensaje y explica cómo lo encontraste. *Hint:* $|\{p_1, q_1, p_2, q_2\}| = 3$.

9. En el protocolo TLS, el primer paso para establecer una conexión es hacer un *handshake*. Explica las diferencias que hay en el proceso de handshake entre las versiones 1.2 y 1.3 de TLS.