Práctica 6
Clave Pública

Índice

Para entregar

- Carpeta "publica" con
  - El código de las funciones *clavesdh*(), $cifgamalnum()$, $decgamalnum()$, $cifgamal()$, *decgamal*(), *clavesRSA*(), $cifRSAnum()$, $decRSAnum()$, $decRSAnumch()$, $cifRSA()$, $decRSA()$ y $decRSAch()$ completado.
  - Problemas de la sección 5 resueltos.

1. Introducción

La Criptografía de *clave pública* se caracteriza por el empleo de dos claves: una para cifrar K_{E} o clave pública y otra para descifrar K_{D} o clave privada. La clave de cifrado no debe poder ser obtenida a partir de la clave de descifrado.

Se construye sobre las llamadas funciones de una dirección con trampa (*trapdoor one-way functions*). Se trata de funciones relativamente fáciles de calcular y muy difíciles de invertir, a menos que se disponga de información adicional (trapdoor).

Así, la función de cifrado es computacionalmente factible. La función de descifrado debe ser imposible de calcular (computacionalmente infactible).

La Criptografía de clave pública aparece en 1976 con el intercambio de claves de Diffie-Hellman. Está basada en algunos problemas matemáticos que en este momento se consideran intratables, es decir, de muy difícil solución, como son:

- La factorización de enteros.
- El problema del logaritmo discreto sobre un cuerpo finito.
- El cálculo de raíces cuadradas modulares.
- El problema del logaritmo elíptico sobre grupos definidos a partir de curvas elípticas.

2. Intercambio de claves de Diffie-Hellman

Se basa en el **problema de Diffie-Hellman**:

Dado un número primo p, un número g que sea generador de $\mathbb{Z}_p^*$ y los números g^a y g^b, encontrar g^{ab} (mód p).

Objetivo: A y B pretenden intercambiar una clave secreta a través de un canal abierto.

A y B acuerdan un número primo grande p y un generador g de $\mathbb{Z}_p^*$.
La información (p, g) es **pública**.

Protocolo:

- A elige un número aleatorio x_A , $0 < x_A < p - 1$ y envía

$$g^{x_A} \mod p.$$

- B elige un número aleatorio x_B , $0 < x_B < p - 1$ y envía

$$g^{x_B} \mod p.$$

- B recibe $g^{x_A} \mod p$ y calcula: $K = (g^{x_A})^{x_B} \equiv g^{x_A x_B} \mod p$.
- A recibe $g^{x_B} \mod p$ y calcula: $K = (g^{x_B})^{x_A} \equiv g^{x_B x_A} \mod p$.

Los valores x_A y x_B se mantienen **secretos**. La clave común es $g^{x_A x_B} \mod p$.

- Programar una función (*clavesdh*()) que admita como entradas un número primo p, un generador g de $\mathbb{Z}_p^*$ y los números x_A, x_B y cuya salida sea la información enviada por cada usuario y la clave intercambiada.

EJERCICIO. Probar la función con:

1. $p = 71$, $g = 21$ (públicos), $x_A = 46$, $x_B = 57$ (secretos).
   Solución: A envía $y_A = 9$. B envía $y_B = 61$. La clave intercambiada es $K = 16$.

2. $p = 107$, $g = 32$, (públicos), $x_A = 82$, $x_B = 25$ (secretos).
   Solución: A envía $y_A = 33$. B envía $y_B = 95$. La clave intercambiada es $K = 48$.

3. Criptosistema ElGamal

Está basado en el cálculo del logaritmo discreto.

A diferencia de otros criptosistemas de clave pública, para cifrar el emisor utiliza, además de la clave pública del receptor, una clave de sesión.

3.1. Generación de claves

Parámetros **públicos:** p, número primo grande y g, generador de $\mathbb{Z}_p^*$.

El receptor elige x, número aleatorio, $1 < x < p-1$ y calcula $y \equiv g^x \mod p$.
Clave **privada del receptor:** x. Clave **pública del receptor:** y.

El emisor elige b, número aleatorio, $1 < b < p-1$.
Clave de **sesión del emisor:** b.

3.2. Cifrado y descifrado de números

La función de cifrado se define a partir de la clave pública del receptor y y de una clave de sesión del emisor b.

$$\begin{array}{rccc} \mathrm{E}: & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p \times \mathbb{Z}_p \\ & M & \mapsto & (r, s) \end{array}$$

donde

$$r \equiv g^b \mod p, \quad s \equiv My^b \mod p.$$

La función de descifrado se define a partir de la clave privada del receptor x:

$$\begin{array}{rccc} \mathrm{D}: & \mathbb{Z}_p \times \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p \\ & (r, s) & \mapsto & s(r^x)^{-1} \mod p. \end{array}$$

Observación. Teniendo en cuenta que $r^{p-1} \equiv 1 \mod p$, podemos evitar la inversión en el cálculo anterior, ya que $r^{-x} \equiv r^{p-1-x} \mod p$. Así,

$$\mathrm{D}(r, s) \equiv sr^{p-1-x} \mod p.$$

- Programar una función ($cifgamalnum()$) que admita como entradas los parámetros p, g, la clave pública del receptor y el equivalente numérico M de un mensaje en claro y devuelva como salida el mensaje numérico cifrado $C = (r, s)$.

  Observación: para generar la clave de sesión del emisor, se puede utilizar la orden

  ```
  b <- sample(2:(p-2), 1)
  ```

  Si se incluye esta orden en la función de cifrado, el mismo mensaje en claro, en general, dará lugar a diferentes mensajes cifrados.

- Programar una función ($decgamalnum()$) que admita como entradas el parámetro p, la clave privada del receptor x y el mensaje numérico cifrado $C = (r, s)$ y devuelva el equivalente numérico del mensaje en claro.

EJERCICIO. Sean $p = 2357$, primo, y $g = 2$, generador del grupo $\mathbb{Z}_p^*$. La clave pública del usuario B es $y = 902$. Cifrar el mensaje $M = 100$. Descifrar el mensaje cifrado obtenido, sabiendo que la clave privada del receptor es $x = 1571$.

3.3. Cifrado y descifrado de texto

Para cifrar un mensaje, primero debemos hallar su equivalente numérico. Para ello, partimos el mensaje en k-gramas y calculamos el equivalente numérico M de cada bloque.

Si el número de caracteres del alfabeto es N, se tiene que

$$M \in \mathbb{Z}_{N^k} = \{0, 1, \ldots, N^k - 1\}.$$

Como

$$\mathrm{E}: \ \mathbb{Z}_p \ \longrightarrow \ \mathbb{Z}_p \times \mathbb{Z}_p$$

para poder cifrar M, debe ser $M \in \mathbb{Z}_p = \{0, 1, \ldots, p - 1\}$. Es decir,

$$N^k \leq p.$$

Para transformar el criptograma $C = (r, s)$ en texto, tendremos en cuenta que $r, s \in \mathbb{Z}_p = \{0, 1, \ldots, p - 1\}$.

Si queremos transformar r y s en ℓ-gramas, como el número más grande que puede ser transformado en ℓ-grama es $N^\ell - 1$, debe ser $p \leq N^\ell$.

Es decir, si el mensaje en claro está partido en k-gramas y el mensaje cifrado en ℓ-gramas, se tiene que cumplir

$$N^k \leq p \leq N^\ell.$$

- Programar una función ($cifgamal()$) que admita como entradas los parámetros p, g, la clave pública del receptor y, un alfabeto, un mensaje en claro y dos enteros positivos k, ℓ tales que $N^k \leq p \leq N^\ell$. La salida es el mensaje cifrado. El mensaje en claro ha sido partido en k-gramas y el mensaje cifrado en ℓ-gramas.

  Observación: Como cada equivalente numérico de un bloque de mensaje en claro se cifra en dos números, el cifrado de cada bloque será un 2ℓ-grama. Si el número de k-gramas del mensaje en claro es m, el mensaje cifrado será un vector de 2ℓ-gramas de longitud m.

  Ejemplo:

```
> k=2
> l=3
> cifgamal(p,g, y, alfabeto, "TELEFONO", k, l)
[1] "ALCAWY" "BXFCIN" "CGXDAY" "AFWDHK"
```

  "TELEFONO" ha sido partido en cuatro bigramas ($k = 2$). Como $\ell = 3$, el mensaje cifrado es un vector de cuatro 6-gramas.

- Programar una función ($decgamal()$) que admita como entradas el parámetro p, la clave privada del receptor x, un alfabeto, un mensaje cifrado y un entero positivo k. La salida es el mensaje en claro. El mensaje cifrado está representado por un vector de 2ℓ-gramas y el mensaje en claro ha sido partido en k-gramas.

  Observación: Para dividir cada componente del mensaje cifrado en dos ℓ-gramas, puede usarse la función $substr()$.

  Ejemplo

```
> cifrado
[1] "BRMDAL" "DGEBAB" "AQUAIV" "CYQAWQ"
> l <- nchar(cifrado[1])/2
> substr(cifrado[1], 1, l)
[1] "BRM"
> substr(cifrado[1], l+1, 2*l)
[1] "DAL"
```

EJERCICIOS.

1. Sean $p = 2357$, primo, y $g = 2$, generador del grupo $\mathbb{Z}_p^*$. La clave pública de un usuario es $y = 902$. Utilizando el alfabeto $LETTERS$, cifrar el mensaje "CRIPTOGRAFIA". Partir el mensaje en claro en bigramas y el mensaje cifrado en trigramas. Descifrar el mensaje sabiendo que la clave privada del receptor es $x = 1571$.

2. Sea p el primo $p = 65537$ y sea $g = 5$. Nuestra clave secreta es $x = 13908$. Recibimos el mensaje "ADBWNADPPI" "AAKRQACFWY" "AAZDKABCLT" "ABYSSABVIN" "ABNVDABHOE" que ha sido cifrado partiendo el mensaje en bloques de 3 letras en el alfabeto $LETTERS$. Descifrar el mensaje. Solución: "BIENDESCIFRADOZ".

4. Criptosistema RSA

Está basado en **el problema RSA:**

Dado un entero positivo n del que se sabe que es producto de dos números primos p y q, hallar sus factores.

Se trata de un caso particular del problema de factorización de enteros.

4.1. Generación de claves

Para generar las claves cada usuario elige dos primos pseudoaleatorios $p,\ q$ muy grandes y calcula $n = pq$. Después selecciona aleatoriamente un entero e tal que $1 < e < \phi(n)$ y $\text{mcd}(e, \phi(n)) = 1$ (se recomienda que $e > \text{máx}(p, q)$). Por último, calcula $d = e^{-1} \mod \phi(n)$.

Los parámetros (n, e) son **públicos**. El valor de d y de los factores p y q se mantienen **secretos**.

- Programar una función ($clavesRSA()$) que admita como entradas dos primos p y q y cuya salida sea una clave púbica y la correspondiente privada.

  Los pasos que habrá que seguir son:

  - Calcular $n = pq$ y $\phi(n) = (p-1)(q-1) = n + 1 - (p+q)$.
  - Seleccionar un entero impar aleatorio e tal que $\text{máx}(p, q) < e < \phi(n)$ y $\text{mcd}(e, \phi(n)) = 1$ (equivalentemente, $\text{mcd}(e, p-1) = 1$ y $\text{mcd}(e, q-1) = 1$):
    - Seleccionar un entero aleatorio e tal que $\text{máx}(p, q) < e < \phi(n)$.
    - Si e es par, hacer $e = e + 1$.
    - Mientras $\text{mcd}(e, p-1) \neq 1$ o $\text{mcd}(e, q-1) \neq 1$, hacer $e = e + 2$.
  - Calcular $d = e^{-1} \mod \phi(n)$.
  - Clave pública: (n, e). Clave privada: (p, q, d).

EJERCICIO. Generar una clave pública y la correspondiente clave privada con $p = 281$, $q = 167$.

4.2. Cifrado y descifrado de números

La función de cifrado se define a partir de la clave pública (n, e):

$$\begin{array}{rccc} \mathrm{E}: & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & M & \mapsto & M^e \mod n \end{array}$$

La función de descifrado se define a partir de la clave privada (p, q, d):

$$\begin{array}{rccc} \mathrm{D}: & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & C & \mapsto & C^d \mod n \end{array}$$

- Programar una función ($cifRSAnum()$) que admita como entradas la clave pública RSA (n, e) y el equivalente numérico M de un mensaje en claro y devuelva como salida el equivalente numérico del mensaje cifrado.
- Programar una función ($decRSAnum()$) que admita como entradas la clave privada RSA (p, q, d) y el equivalente numérico C de un mensaje cifrado y devuelva el equivalente numérico del mensaje en claro.

EJERCICIO. La clave pública de un usuario A es $(n = 46927, e = 39423)$ y la privada $(p = 281, q = 167, d = 26767)$. Cifrar el mensaje $M = 196$ utilizando la clave pública de A. Descifrar el mensaje cifrado utilizando la clave privada de A.

Descifrado utilizando el Teorema chino del resto

Para facilitar los cálculos, en el descifrado se puede utilizar el Teorema chino del resto.

Si la clave secreta es (p, q, d), el procedimiento para descifrar C consiste en

- Calcular

$$d_p \equiv d \mod p-1, \quad d_q \equiv d \mod q-1,$$

$$p_1 \equiv p^{-1} \mod q, \quad q_1 \equiv q^{-1} \mod p, \quad coef_1 = qq_1, \quad coef_2 = pp_1.$$

- Calcular

$$C_p \equiv C \mod p, \quad C_q \equiv C \mod q,$$

$$M_1 \equiv C_p^{d_p} \mod p, \quad M_2 \equiv C_q^{d_q} \mod q.$$

- Calcular

$$M \equiv coef_1 M_1 + coef_2 M_2 \mod pq.$$

Con ello conseguimos que el módulo al calcular las potencias sea sensiblemente menor y, en consecuencia, los cálculos más rápidos.

Además, los valores d_p, d_q, $coef_1$ y $coef_2$ sólo dependen de la clave privada y no del mensaje cifrado, por lo que pueden calcularse previamente.

- Programar una función ($decRSAnumch()$) que admita como entradas la clave privada RSA (p, q, d) y el equivalente numérico C de un mensaje cifrado y devuelva el equivalente numérico del mensaje en claro, habiéndolo descifrado utilizando el Teorema chino del resto.

EJERCICIO. La clave privada RSA de un usuario es $(p = 8191, q = 65537, d = 201934721)$. Descifrar $C = 487369684$ utilizando y sin utilizar el teorema chino del resto.
Solución: El mensaje en claro es $M = 1000$. Sin utilizar el teorema chino del resto puede que no lo obtengamos.

4.3. Cifrado y descifrado de texto

Para cifrar un mensaje, primero debemos hallar su equivalente numérico. Para ello, partimos el mensaje en claro en k-gramas y calculamos el equivalente numérico de cada bloque.

Una vez calculado el criptograma numérico, obtendremos el mensaje de texo cifrado convirtiendo cada número en un ℓ-grama.

Debe ser

$$N^k \leq n \leq N^\ell.$$

- Programar una función ($cifRSA()$) que admita como entradas la clave pública RSA (n, e), un alfabeto, un mensaje en claro y dos enteros positivos k, ℓ tales que $N^k \leq n \leq N^\ell$. La salida es el mensaje cifrado. El mensaje en claro ha sido partido en k-gramas y el mensaje cifrado en ℓ-gramas.

- Programar dos funciones ($decRSA()$ y $decRSAch()$) que admitan como entradas la clave privada RSA (p, q, d), un alfabeto, un mensaje cifrado y dos enteros positivos k, ℓ tales que $N^k \leq n \leq N^\ell$. La salida es el mensaje en claro. El mensaje cifrado ha sido partido en ℓ-gramas y el mensaje en claro en k-gramas.

  En $decRSAch()$ realizar el descifrado utilizando el teorema chino del resto y en $decRSA$ sin utilizarlo.

EJERCICIO. La clave pública de un usuario A es $(n = 46927, e = 39423)$ y la privada $(p = 281, q = 167, d = 26767)$. El alfabeto es $LETTERS$.

1. Cifrar el mensaje "HOLA" utilizando la clave pública de A y partiendo el mensaje en claro en bigramas y el mensaje cifrado en 4-gramas. Descifrar el mensaje cifrado utilizando la clave privada de A.

2. Cifrar el mensaje "MAÑANA NO HAY CLASES" utilizando la clave pública de A y partiendo el mensaje en claro en 3-gramas y el mensaje cifrado en 4-gramas. (Identificar "Ñ" y " " con "W"). Descifrar el mensaje cifrado utilizando la clave privada de A.

5. Problemas

Hay que escribir la solución de los problemas en el fichero "problemaspublica.R", escribiendo comentados todos los pasos necesarios para su resolución. A modo de ejemplo, el primer problema está resuelto.

1. Tratar de romper el cifrado RSA cuya clave pública es $(n, e) = (48959, 6529)$ factorizando n "por fuerza bruta" (dividiendo n por $3, 5, 7, \dots$). Descifrar a continuación el mensaje "CHUBBBVDCEMOBUFMBKYB". Se ha utilizado el alfabeto $LETTERS$, el texto en claro ha sido partido en 3-gramas y el texto cifrado en 4-gramas.

2. Tratar de romper el cifrado cuya clave pública es $(n, e) = (536813567, 3602561)$ factorizando n "por fuerza bruta" (dividiendo n por $3, 5, 7, \dots$). Descifrar a continuación el mensaje "axyfiudbkwngupbfpnazyahrchcf". Se ha utilizado el alfabeto $letters$, el texto en claro ha sido partido en 6-gramas y el texto cifrado en 7-gramas. Realizar el descifrado utilizando y sin utilizar el Teorema chino del resto.

3. Las claves públicas RSA de los usuarios A, B son:

$$(n, e_A) = (817, 19), \quad (n, e_B) = (817, 29).$$

   El cifrado del mensaje M es: $C_A = 191$, $C_B = 362$. Obtener M por un ataque de módulo común.

   Observación: Al calcular $C_A^u C_B^v$ hay que tener en cuenta que u o v es negativo. Si $x < 0$, $C^x \equiv (C^{-1})^{(-x)} \mod n$.

4. La clave pública RSA de un usuario es $(n, e) = (46927, 39423)$. El cifrado del mensaje M es $C = 20736$. Obtener M por un ataque cíclico.