Practica Opcional: Cifrado ElGamal

José Manuel Cuevas Muñoz

Enero 2020

Para esta práctica vamos a utilizar varias funciones de la practica 6, entre estas: *genera(g,p)*, *letra2numeros(texto)*, *num_descifra(n, bloque_numero)*, *potencia(c, d, n)* y *prepar_num_cifrar(tama, bloque)*.

1.Función generar_clave_aleatoria(n)

Función que genera una clave publica y privada aleatoria para ElGamal a partir de un numero primo aleatorio entre los n primeros.

Entrada:
n: N primos de los que se cogerá aleatoriamente la clave

Salida:
cpubl: Clave publica formada por [g,n,q], siendo g un número generador, q el módulo primo y n la potencia de $g^a \ mod \ q$.
cpriv: Clave publica formada por [g,n,q], siendo g un número generador, q el módulo primo y a un número aleatorio entre 2 y q-2.

2.Función cifro_elgamal_num (g, n, q, blo)

Función que cifra un un bloque de números con ElGamal, generando para esto un número k aleatorio

Entrada:
g=Número generador en base q
n=Clave publica con la que cifrar
q=Número primo que representa el módulo
blo=Bloque de números a cifrar

Salida:
gk=g elevado a k módulo q
cifrado=Mensaje cifrado

Ejemplo
[gk,cifrado]=cifro_elgamal_num (98,107,109,[0,3,8,15,19])
k= 12 (K se escoge aleatoriamente)
gk =38
cifrado = 0 80 68 73 107

3.Función cifro_elgamal (g, n, q, texto)

Función que cifra un un texto con ElGamal. Para ello, primero hay que transformar el texto a números del tamaño del numero de cifras de q menos uno.

Entrada:
g=Número generador en base q
n=Clave publica con la que cifrar
q=Número primo que representa el módulo
texto=Texto a cifrar

Salida:
gk=g elevado a k módulo q
cifrado=Mensaje cifrado

Ejemplo
Ejemplo
[gk,cifrado]=cifro_elgamal (98,107,109, 'hola')

Ejemplo
k =31(K se escoge aleatoriamente)
gk =65
cifrado =10 37 78 0

4.Función descifro_elgamal_num (gk,a,q, cifrado_numero)

Función que descifra un texto encriptado en ElGamal y devuelve un bloque de números

Entrada:
gk=Valor de g elevado a k en módulo q que obtuviste en el cifrado ElGamal
a=Clave privada del cifrado
q=Número primo que representa el módulo
cifrado_numero=Bloque de números a descifrar

Salida:
descifro_num=Bloque de números que representa el texto descifrado

Ejemplo
descifro_elgamal_num(65,15,109,[10,37,78,0])
ans = 7 15 11 0

5.Función descifro_elgamal (gk,a,q, cifrado_numero)

Función que descifra un texto encriptado en ElGamal y pasa a caracteres estos números

Entrada:
gk=Valor de g elevado a k en módulo q que obtuviste en el cifrado ElGamal
a=Clave privada del cifrado
q=Número primo que representa el módulo
cifrado_numero=Bloque de números a descifrar

Salida:
descifrado=Mensaje descifrado

Ejemplo
descifro_elgamal(65,15,109,[10,37,78,0])
ans = 'hola'

6.Función firmo_elgamal_num (g,a,q, blo)

Función que firma un bloque de números con el cifrado ElGamal. Para ello genera un número k aleatorio.

Entrada:
g=Número generador en base q
a=Clave privada del cifrado
q=Número primo que representa el módulo
blo=Bloque de números a cifrar

Salida:
r= Número necesario para comprobar la firma
firmado=Mensaje firmado

Ejemplo
[r,firma]=firmo_elgamal_num(98,15,109,[7,15,11,0])
k =103
r =62
firma = 55 75 11 78

7.Función firmo_elgamal (g,a,q, texto)

Función que firma un bloque de números con el cifrado ElGamal. Para ello genera un número k aleatorio.

Entrada:
g=Número generador en base q
a=Clave privada del cifrado
q=Número primo que representa el módulo
texto=Texto a cifrar

Salida:
r= Número necesario para comprobar la firma
firmado=Mensaje firmado

Ejemplo
[r2,firma2]=firmo_elgamal(98,15,109,'adios')
k =103
r =62
firma = 78 99 98 75 31

8.Función verifico_firma_elgamal_num (r,g,n,q, firma, mensaje)

Función que recibe la firma y el mensaje en bloque numérico y verifica si una firma se corresponde al remitente.

Entrada:
r=Información extraída de la firma
g=Número generador en base q
n=Clave publica con la que cifrar
q=Número primo que representa el módulo
firma=Bloque numérico que representa la firma del documento
mensaje=Mensaje en bloque numérico que supuestamente se corresponde la firmado

Salida:
firma_v=Valor booleano que es true si se verifica la firma

Ejemplo
verifico_firma_elgamal_num(62,98,107,109,[55,75,11,78],[7,15,11,0])
rsgm =67 107 56 1
ans = logical 1

9.Función verifico_firma_elgamal (r,g,n,q, firma, mensaje)

Función que recibe la firma y el mensaje, transforma este mensaje a bloque numérico y verifica si una firma se corresponde al remitente.

Entrada:
r=Información extraída de la firma
g=Número generador en base q
n=Clave publica con la que cifrar
q=Número primo que representa el módulo
firma=Bloque numérico que representa la firma del documento
mensaje=Mensaje en forma de cadena que supuestamente se corresponde la firmado

Salida:
firma_v=Valor booleano que es true si se verifica la firma

Ejemplo
verifico_firma_elgamal(62,98,107,109,[78,99,98,75,31],'adios')
rsgm =1 86 26 107 39
ans = logical 1

10.Script Firma

Script en el que se generan claves aleatorias para A y B; B le envia un mensaje y su firma a A y A descifra el mensaje y comprueba la firma de B.

Generamos la clave publica y privada de A
cpubla =
18964 18391 44963
cpriva =
18964 41173 44963
Generamos la clave publica y privada de B
cpublb =
74332 15804 77471
cprivb =
74332 50800 77471
Introduce el mensaje que B quiere enviar a A:'hola que tal el dia'
Ciframos con la clave publica de A
ans =
5
k =
1607

gk =
24597
mensajecif =
11869 18260 19576 6972 36153 42793 23098 498
También firmamos con la clave privada de B
k =
30387
r =
29757
mensaje_firma =
25365 70480 53103 26010 35833 75663 24154 8480
A recibe un mensaje cifrado, una firma, r y gk
A desencripta el mensaje
mensajedescifrado =
'holaquetaleldia'
Comprobamos el mensaje con la firma
rsgm = 37923 28271 21280 64064 28775 26406 23759 14550
El mensaje viene de B con certeza