CÓDIGOS Y CRIPTOGRAFÍA

Autenticación de firma
Cifrado ElGamal

INDEX

Autentificación de firma con RSA

- Vamos a ver como podemos garantizar la identidad del emisor, es decir, como se puede firmar un criptograma.

Autentificación de firma con RSA

- Vamos a ver como podemos garantizar la identidad del emisor, es decir, como se puede firmar un criptograma.
- Se puede llevar a cabo la firma con cualquier método de clave pública.

Autentificación de firma con RSA

- Vamos a ver como podemos garantizar la identidad del emisor, es decir, como se puede firmar un criptograma.
- Se puede llevar a cabo la firma con cualquier método de clave pública.
- Para ello tanto el receptor como el emisor deben generar sus propias claves públicas y privadas.

Autentificación de firma con RSA

- Vamos a ver como podemos garantizar la identidad del emisor, es decir, como se puede firmar un criptograma.
- Se puede llevar a cabo la firma con cualquier método de clave pública.
- Para ello tanto el receptor como el emisor deben generar sus propias claves públicas y privadas.
- La idea como veremos puede aplicarse con distintos métodos, pero aquí lo veremos con RSA.

Autentificación de firma con RSA

Generación de claves

- Tanto el emisor como el receptor generan sus propias claves públicas y privadas:

Autentificación de firma con RSA

Generación de claves

- Tanto el emisor como el receptor generan sus propias claves públicas y privadas:

Claves de A

CLAVE PÚBLICA: (n_A, e_A)

CLAVE PRIVADA: (n_A, d_A)

Claves de B

CLAVE PÚBLICA: (n_B, e_B)

CLAVE PRIVADA: (n_B, d_B)

Autentificación de firma con RSA

Cifrado del mensaje (A)

- A quiere enviar a B el mensaje mensaje, firmado con la firma firma.

Autentificación de firma con RSA

Cifrado del mensaje (A)

- A quiere enviar a B el mensaje mensaje, firmado con la firma firma.
- Prepara el envío en 2 pasos:

Autentificación de firma con RSA

Cifrado del mensaje (A)

- A quiere enviar a B el mensaje mensaje, firmado con la firma firma.
- Prepara el envío en 2 pasos:

1. Cifra el mensaje y la firma juntos del modo usual.

   Es decir, cifra mensaje firma con la clave pública de B, (n_B, e_B).

Autentificación de firma con RSA

Cifrado del mensaje (A)

- A quiere enviar a B el mensaje mensaje, firmado con la firma firma.
- Prepara el envío en 2 pasos:

1. Cifra el mensaje y la firma juntos del modo usual.

   Es decir, cifra mensaje firma con la clave pública de B, (n_B, e_B).

2. Hace un doble cifrado a su firma: primero con su clave privada, (n_A, d_A) y después con la clave pública de B, (n_B, e_B). Para ello:
   - Cifra firma con (n_A, d_A).
   - Completa los bloques para que tengan la misma longitud que dígitos(n_A).
   - Concatena y vuelve a cifrar con (n_B, e_B).

Autentificación de firma con RSA

Cifrado del mensaje (A)

- A quiere enviar a B el mensaje mensaje, firmado con la firma firma.
- Prepara el envío en 2 pasos:

1. Cifra el mensaje y la firma juntos del modo usual.

   Es decir, cifra mensaje firma con la clave pública de B, (n_B, e_B).

2. Hace un doble cifrado a su firma: primero con su clave privada, (n_A, d_A) y después con la clave pública de B, (n_B, e_B). Para ello:
   - Cifra firma con (n_A, d_A).
   - Completa los bloques para que tengan la misma longitud que dígitos(n_A).
   - Concatena y vuelve a cifrar con (n_B, e_B).

- Envía a B dos criptogramas distintos:

$$\text{cifr-mensajefirma-}e_B \quad y \quad \text{cifr-firma-}d_A\text{-}e_B$$

Autentificación de firma con RSA

Descifrado y autentificación de firma (B)

- B recibe dos criptogramas

$$\text{cifr-mensajefirma-}e_B \quad y \quad \text{cifr-firma-}d_A\text{-}e_B$$

y los descifra usando su clave privada, (n_B, d_B).

Autentificación de firma con RSA

Descifrado y autentificación de firma (B)

- B recibe dos criptogramas

$$\text{cifr-mensajefirma-}e_B \quad y \quad \text{cifr-firma-}d_A\text{-}e_B$$

  y los descifra usando su clave privada, (n_B, d_B).

- Obtiene mensajefirma y otro criptograma cifr-firma-d_A.

Autentificación de firma con RSA

Descifrado y autentificación de firma (B)

- B recibe dos criptogramas

$$\text{cifr-mensajefirma-}e_B \quad y \quad \text{cifr-firma-}d_A\text{-}e_B$$

  y los descifra usando su clave privada, (n_B, d_B).

- Obtiene mensajefirma y otro criptograma cifr-firma-d_A.
- Como firma le dice que puede ser de A, procede a descifrar el segundo criptograma con la clave pública de A, (n_A, e_A).

Autentificación de firma con RSA

Descifrado y autentificación de firma (B)

- B recibe dos criptogramas

$$\text{cifr-mensajefirma-}e_B \quad y \quad \text{cifr-firma-}d_A\text{-}e_B$$

  y los descifra usando su clave privada, (n_B, d_B).

- Obtiene mensajefirma y otro criptograma cifr-firma-d_A.
- Como firma le dice que puede ser de A, procede a descifrar el segundo criptograma con la clave pública de A, (n_A, e_A). Para ello:
  - Completa los bloques de cifr-firma-d_A para que todos tengan la misma longitud que $n_B - 1$.
  - Concatena, separa en bloques de la misma longitud que n_A y descifra con (n_A, e_A).
  - Obtiene firma.

Autentificación de firma con RSA

Descifrado y autentificación de firma (B)

- B recibe dos criptogramas

$$\text{cifr-mensajefirma-}e_B \quad y \quad \text{cifr-firma-}d_A\text{-}e_B$$

  y los descifra usando su clave privada, (n_B, d_B).

- Obtiene mensajefirma y otro criptograma cifr-firma-d_A.
- Como firma le dice que puede ser de A, procede a descifrar el segundo criptograma con la clave pública de A, (n_A, e_A). Para ello:
  - Completa los bloques de cifr-firma-d_A para que todos tengan la misma longitud que $n_B - 1$.
  - Concatena, separa en bloques de la misma longitud que n_A y descifra con (n_A, e_A).
  - Obtiene firma.
- Compara mensajefirma con firma.

Autentificación de firma con RSA: Ejemplo

Generación de claves

- A y B generan sus propias claves:

Autentificación de firma con RSA: Ejemplo

Generación de claves

- A y B generan sus propias claves:

Claves de A

$$p_A = 11,\ q_A = 13$$
$$n_A = 143,\ \varphi(n_A) = 120$$
$$e_A = 7,\ d_A = 103$$

Claves de B

$$p_B = 17,\ q_B = 59$$
$$n_B = 1003,\ \varphi(n_B) = 928$$
$$e_B = 3,\ d_B = 619$$

Autentificación de firma con RSA: Ejemplo

Cifrado y firma (A)

- A va a enviarle a B el mensaje prueba con la firma bya:

Autentificación de firma con RSA: Ejemplo

Cifrado y firma (A)

- A va a enviarle a B el mensaje prueba con la firma bya:

1. Cifra pruebabya con (n_B, e_B):

$$C_1 = [801 \quad 465 \quad 811 \quad 9 \quad 725 \quad 122].$$

Autentificación de firma con RSA: Ejemplo

Cifrado y firma (A)

- A va a enviarle a B el mensaje prueba con la firma bya:

1. Cifra pruebabya con (n_B, e_B):

$$C_1 = [801 \quad 465 \quad 811 \quad 9 \quad 725 \quad 122].$$

2. Hace un doble cifrado a bya:

Autentificación de firma con RSA: Ejemplo

Cifrado y firma (A)

- A va a enviarle a B el mensaje prueba con la firma bya:

1. Cifra pruebabya con (n_B, e_B):

$$C_1 = [801 \quad 465 \quad 811 \quad 9 \quad 725 \quad 122].$$

2. Hace un doble cifrado a bya:
   - Primero con (n_A, d_A):

$$[1 \quad 38 \quad 0]$$

Autentificación de firma con RSA: Ejemplo

Cifrado y firma (A)

- A va a enviarle a B el mensaje prueba con la firma bya:

1. Cifra pruebabya con (n_B, e_B):

$$C_1 = [801 \quad 465 \quad 811 \quad 9 \quad 725 \quad 122].$$

2. Hace un doble cifrado a bya:
   - Primero con (n_A, d_A):

$$[1 \quad 38 \quad 0]$$

   - Completa los bloques para que tengan la longitud de n_A:

$$001 \quad 038 \quad 000$$

Autentificación de firma con RSA: Ejemplo

Cifrado y firma (A)

- A va a enviarle a B el mensaje prueba con la firma bya:

1. Cifra pruebabya con (n_B, e_B):

$$C_1 = [801 \quad 465 \quad 811 \quad 9 \quad 725 \quad 122].$$

2. Hace un doble cifrado a bya:
   - Primero con (n_A, d_A):

$$[1 \quad 38 \quad 0]$$

   - Completa los bloques para que tengan la longitud de n_A:

$$001 \quad 038 \quad 000$$

   - Concatena, 001038000, y cifra con (n_B, e_B):

$$C_2 = [1 \quad 710 \quad 0]$$

Autentificación de firma con RSA: Ejemplo

Cifrado y firma (A)

- A va a enviarle a B el mensaje prueba con la firma bya:

1. Cifra pruebabya con (n_B, e_B):

$$C_1 = [801 \quad 465 \quad 811 \quad 9 \quad 725 \quad 122].$$

2. Hace un doble cifrado a bya:
   - Primero con (n_A, d_A):

$$[1 \quad 38 \quad 0]$$

   - Completa los bloques para que tengan la longitud de n_A:

$$001 \quad 038 \quad 000$$

   - Concatena, 001038000, y cifra con (n_B, e_B):

$$C_2 = [1 \quad 710 \quad 0]$$

- Envía a B $C_1 = [801 \ 465 \ 811 \ 9 \ 725 \ 122]$ y $C_2 = [1 \ 710 \ 0]$.

Autentificación de firma con RSA: Ejemplo

Descifrado y autentificación (B)

- B recibe $C_1 = [801 \;\; 465 \;\; 811 \;\; 9 \;\; 725 \;\; 122]$ y $C_2 = [1 \;\; 710 \;\; 0]$.

Autentificación de firma con RSA: Ejemplo

Descifrado y autentificación (B)

- B recibe $C_1 = [801\ \ 465\ \ 811\ \ 9\ \ 725\ \ 122]$ y $C_2 = [1\ \ 710\ \ 0]$.
- Descifra ambos criptogramas usando su clave privada, (n_B, d_B).

Autentificación de firma con RSA: Ejemplo

Descifrado y autentificación (B)

- B recibe $C_1 = [801\ \ 465\ \ 811\ \ 9\ \ 725\ \ 122]$ y $C_2 = [1\ \ 710\ \ 0]$.
- Descifra ambos criptogramas usando su clave privada, (n_B, d_B).
- Del primer criptograma obtiene pruebabya.

Autentificación de firma con RSA: Ejemplo

Descifrado y autentificación (B)

- B recibe $C_1 = [801 \;\; 465 \;\; 811 \;\; 9 \;\; 725 \;\; 122]$ y $C_2 = [1 \;\; 710 \;\; 0]$.
- Descifra ambos criptogramas usando su clave privada, (n_B, d_B).
- Del primer criptograma obtiene pruebabya.
- Del segundo criptograma no obtiene un mensaje coherente, se queda con los bloques numéricos:

$$[1 \quad 38 \quad 0].$$

Autentificación de firma con RSA: Ejemplo

Descifrado y autentificación (B)

- B recibe $C_1 = [801 \;\; 465 \;\; 811 \;\; 9 \;\; 725 \;\; 122]$ y $C_2 = [1 \;\; 710 \;\; 0]$.
- Descifra ambos criptogramas usando su clave privada, (n_B, d_B).
- Del primer criptograma obtiene pruebabya.
- Del segundo criptograma no obtiene un mensaje coherente, se queda con los bloques numéricos:

$$[1 \quad 38 \quad 0].$$

- Completa los bloques para que tengan la misma longitud que $n_B - 1$:

$$001 \quad 038 \quad 000$$

Autentificación de firma con RSA: Ejemplo

Descifrado y autentificación (B)

- B recibe $C_1 = [801 \;\; 465 \;\; 811 \;\; 9 \;\; 725 \;\; 122]$ y $C_2 = [1 \;\; 710 \;\; 0]$.
- Descifra ambos criptogramas usando su clave privada, (n_B, d_B).
- Del primer criptograma obtiene pruebabya.
- Del segundo criptograma no obtiene un mensaje coherente, se queda con los bloques numéricos:

$$[1 \quad 38 \quad 0].$$

- Completa los bloques para que tengan la misma longitud que $n_B - 1$:

$$001 \quad 038 \quad 000$$

- Concatena y separa los bloques para que tengan la misma longitud que n_A (en este caso se quedan igual: $[1 \quad 38 \quad 0]$.) y descifra con (n_A, e_A), bya.

INDEX

Cifrado ElGamal

- Cifrado de clave púplica basado en la exponenciación binaria y en el logaritmo discreto.

Cifrado ElGamal

- Cifrado de clave púplica basado en la exponenciación binaria y en el logaritmo discreto.
- Supongamos dos interlocutores: el receptor A y el emisor B.

Cifrado ElGamal

- Cifrado de clave púplica basado en la exponenciación binaria y en el logaritmo discreto.
- Supongamos dos interlocutores: el receptor A y el emisor B.
- Para comenzar, ambos interlocutores se ponen de acuerdo en la elección de un número primo q y de un número $0 \leq g \in \mathbb{Z}_q$ (no necesariamente generador).

Cifrado ElGamal

- Cifrado de clave púplica basado en la exponenciación binaria y en el logaritmo discreto.
- Supongamos dos interlocutores: el receptor A y el emisor B.
- Para comenzar, ambos interlocutores se ponen de acuerdo en la elección de un número primo q y de un número $0 \leq g \in \mathbb{Z}_q$ (no necesariamente generador).

Generación de claves (A)

Cifrado ElGamal

- Cifrado de clave púplica basado en la exponenciación binaria y en el logaritmo discreto.
- Supongamos dos interlocutores: el receptor A y el emisor B.
- Para comenzar, ambos interlocutores se ponen de acuerdo en la elección de un número primo q y de un número $0 \leq g \in \mathbb{Z}_q$ (no necesariamente generador).

Generación de claves (A)

- CLAVE PRIVADA: Un número a de modo que $2 \leq a \leq q-2$.

Cifrado ElGamal

- Cifrado de clave púplica basado en la exponenciación binaria y en el logaritmo discreto.
- Supongamos dos interlocutores: el receptor A y el emisor B.
- Para comenzar, ambos interlocutores se ponen de acuerdo en la elección de un número primo q y de un número $0 \leq g \in \mathbb{Z}_q$ (no necesariamente generador).

Generación de claves (A)

- CLAVE PRIVADA: Un número a de modo que $2 \leq a \leq q-2$.
- CLAVE PÚBLICA: El número $ga = g^a \bmod q$.

Cifrado ElGamal

Cifrado (B)

- B quiere enviar el mensaje mensaje a A.

Cifrado ElGamal

Cifrado (B)

- B quiere enviar el mensaje mensaje a A. Para ello:
- Elige un número k de modo que $2 \leq k \leq q-2$.

Cifrado ElGamal

Cifrado (B)

- B quiere enviar el mensaje mensaje a A. Para ello:
- Elige un número k de modo que $2 \leq k \leq q-2$.
- Calcula $gk = g^k \mod q$ y $gak = ga^k = g^{ak} \mod q$.

Cifrado ElGamal

Cifrado (B)

- B quiere enviar el mensaje mensaje a A. Para ello:
- Elige un número k de modo que $2 \leq k \leq q-2$.
- Calcula $gk = g^k \bmod q$ y $gak = ga^k = g^{ak} \bmod q$.
- Escribe M numéricamente utilizando dos dígitos por letra y separa en bloques de tamaño dígitos$(q) - 1$. Si es necesario añade varios 30's y/o un 0.

$$M = [M_1 \quad M_2 \quad M_3 \quad \ldots \quad]$$

Cifrado ElGamal

Cifrado (B)

- B quiere enviar el mensaje mensaje a A. Para ello:
- Elige un número k de modo que $2 \leq k \leq q-2$.
- Calcula $gk = g^k \bmod q$ y $gak = ga^k = g^{ak} \bmod q$.
- Escribe M numéricamente utilizando dos dígitos por letra y separa en bloques de tamaño dígitos$(q) - 1$. Si es necesario añade varios 30's y/o un 0.

$$M = [M_1 \quad M_2 \quad M_3 \quad \ldots \quad]$$

- Realiza dos envíos a A:
  1. Envía el número gk anterior.

Cifrado ElGamal

Cifrado (B)

- B quiere enviar el mensaje mensaje a A. Para ello:
- Elige un número k de modo que $2 \leq k \leq q-2$.
- Calcula $gk = g^k \bmod q$ y $gak = ga^k = g^{ak} \bmod q$.
- Escribe M numéricamente utilizando dos dígitos por letra y separa en bloques de tamaño dígitos$(q) - 1$. Si es necesario añade varios 30's y/o un 0.

$$M = [M_1 \quad M_2 \quad M_3 \quad \ldots \quad]$$

- Realiza dos envíos a A:
  1. Envía el número gk anterior.
  2. Opera cada bloque del mensaje mediante la fórmula

$$C_i = M_i \cdot gak \bmod q,$$

Cifrado ElGamal

Cifrado (B)

- B quiere enviar el mensaje mensaje a A. Para ello:
- Elige un número k de modo que $2 \leq k \leq q-2$.
- Calcula $gk = g^k \bmod q$ y $gak = ga^k = g^{ak} \bmod q$.
- Escribe M numéricamente utilizando dos dígitos por letra y separa en bloques de tamaño dígitos$(q) - 1$. Si es necesario añade varios 30's y/o un 0.

$$M = [M_1 \quad M_2 \quad M_3 \quad \dots \quad]$$

- Realiza dos envíos a A:
  1. Envía el número gk anterior.
  2. Opera cada bloque del mensaje mediante la fórmula

$$C_i = M_i \cdot gak \bmod q,$$

y envía

$$[C_1 \quad C_2 \quad C_3 \quad \dots \quad]$$

Cifrado ElGamal

Descifrado (A)

- A recibe un número gk, y un vector numérico $[C_1 \quad C_2 \quad C_3 \quad \dots \quad]$.

Cifrado ElGamal

Descifrado (A)

- A recibe un número gk, y un vector numérico $[C_1 \quad C_2 \quad C_3 \quad \dots \quad]$.
- Cacula $(gk^a)^{-1} \bmod q$.

Cifrado ElGamal

Descifrado (A)

- A recibe un número gk, y un vector numérico $[C_1 \quad C_2 \quad C_3 \quad \dots \quad]$.
- Cacula $(gk^a)^{-1} \bmod q$.
- Cada elemento del vector recibido lo opera multiplicándolo modularmente por el inverso anterior y obtiene

$$[M_1 \quad M_2 \quad M_3 \quad \dots \quad].$$

Cifrado ElGamal

Descifrado (A)

- A recibe un número gk, y un vector numérico $[C_1 \quad C_2 \quad C_3 \quad \dots \quad]$.
- Cacula $(gk^a)^{-1} \bmod q$.
- Cada elemento del vector recibido lo opera multiplicándolo modularmente por el inverso anterior y obtiene

$$[M_1 \quad M_2 \quad M_3 \quad \dots \quad].$$

- Completa los bloques para que todos sean de longitud dígitos$(q) - 1$.

Cifrado ElGamal

Descifrado (A)

- A recibe un número gk, y un vector numérico $[C_1 \quad C_2 \quad C_3 \quad \dots \quad]$.
- Cacula $(gk^a)^{-1} \bmod q$.
- Cada elemento del vector recibido lo opera multiplicándolo modularmente por el inverso anterior y obtiene

$$[M_1 \quad M_2 \quad M_3 \quad \dots \quad].$$

- Completa los bloques para que todos sean de longitud dígitos$(q) - 1$.
- Concatena todos los bloques, separa de dos en dos dígitos, y vuelve a convertir alfabéticamente recuperando el mensaje.

Cifrado ElGamal: Ejemplo

Elección de elementos comunes y claves

- A y B se ponen de acuerdo en $q = 13$ y $g = 2$.

Cifrado ElGamal: Ejemplo

Elección de elementos comunes y claves

- A y B se ponen de acuerdo en $q = 13$ y $g = 2$.
- A genera sus claves eligiendo $a = 5$ $(2 \leq a \leq q - 2)$:

Cifrado ElGamal: Ejemplo

Elección de elementos comunes y claves

- A y B se ponen de acuerdo en $q = 13$ y $g = 2$.
- A genera sus claves eligiendo $a = 5$ $(2 \leq a \leq q - 2)$:

  CLAVE PRIVADA: $a = 5$

Cifrado ElGamal: Ejemplo

Elección de elementos comunes y claves

- A y B se ponen de acuerdo en $q = 13$ y $g = 2$.
- A genera sus claves eligiendo $a = 5$ $(2 \leq a \leq q - 2)$:

  CLAVE PRIVADA: $a = 5$

  CLAVE PÚBLICA: $ga = 2^5 \bmod 13 = 6$

Cifrado ElGamal: Ejemplo

Elección de elementos comunes y claves

- A y B se ponen de acuerdo en $q = 13$ y $g = 2$.
- A genera sus claves eligiendo $a = 5$ $(2 \leq a \leq q - 2)$:

  CLAVE PRIVADA: $a = 5$

  CLAVE PÚBLICA: $ga = 2^5 \bmod 13 = 6$

Cifrado del mensaje (B)

- B quiere enviar el mensaje hola a A.

Cifrado ElGamal: Ejemplo

Elección de elementos comunes y claves

- A y B se ponen de acuerdo en $q = 13$ y $g = 2$.
- A genera sus claves eligiendo $a = 5$ $(2 \leq a \leq q - 2)$:

  CLAVE PRIVADA: $a = 5$

  CLAVE PÚBLICA: $ga = 2^5 \bmod 13 = 6$

Cifrado del mensaje (B)

- B quiere enviar el mensaje hola a A.
- Elige $k = 7$ $(2 \leq k \leq q - 2)$.

Cifrado ElGamal: Ejemplo

Elección de elementos comunes y claves

- A y B se ponen de acuerdo en $q = 13$ y $g = 2$.
- A genera sus claves eligiendo $a = 5$ $(2 \leq a \leq q - 2)$:

  CLAVE PRIVADA: $a = 5$

  CLAVE PÚBLICA: $ga = 2^5 \bmod 13 = 6$

Cifrado del mensaje (B)

- B quiere enviar el mensaje hola a A.
- Elige $k = 7$ $(2 \leq k \leq q - 2)$.
- Halla $gk = 2^7 \bmod 13 = 11$ y $gak = ga^k = 6^7 \bmod 13 = 7$

Cifrado ElGamal: Ejemplo

Elección de elementos comunes y claves

- A y B se ponen de acuerdo en $q = 13$ y $g = 2$.
- A genera sus claves eligiendo $a = 5$ $(2 \leq a \leq q - 2)$:

  CLAVE PRIVADA: $a = 5$

  CLAVE PÚBLICA: $ga = 2^5 \bmod 13 = 6$

Cifrado del mensaje (B)

- B quiere enviar el mensaje hola a A.
- Elige $k = 7$ $(2 \leq k \leq q - 2)$.
- Halla $gk = 2^7 \bmod 13 = 11$ y $gak = ga^k = 6^7 \bmod 13 = 7$
- Convierte el mensaje numéricamente (dos dígitos por letra):

h	o	l	a
07	15	11	00

Cifrado ElGamal: Ejemplo

Cifrado del mensaje (B)

- Concatena los dígitos y separa en bloques de longitud 1=dígitos$(q) - 1$:

$$0 \quad 7 \quad 1 \quad 5 \quad 1 \quad 1 \quad 0 \quad 0$$

Cifrado ElGamal: Ejemplo

Cifrado del mensaje (B)

- Concatena los dígitos y separa en bloques de longitud 1=dígitos$(q) - 1$:

$$0 \quad 7 \quad 1 \quad 5 \quad 1 \quad 1 \quad 0 \quad 0$$

- Multiplicada cada bloque por 7 módulo 13:

$$0 \cdot 7 \bmod 13 = 0, \quad 7 \cdot 7 \bmod 13 = 10, \quad 1 \cdot 7 \bmod 13 = 7$$

$$5 \cdot 7 \bmod 13 = 9, \quad 1 \cdot 7 \bmod 13 = 7, \quad 1 \cdot 7 \bmod 13 = 7$$

$$0 \cdot 7 \bmod 13 = 0, \quad 0 \cdot 7 \bmod 13 = 0$$

Cifrado ElGamal: Ejemplo

Cifrado del mensaje (B)

- Concatena los dígitos y separa en bloques de longitud $1 = \text{dígitos}(q) - 1$:

$$0 \quad 7 \quad 1 \quad 5 \quad 1 \quad 1 \quad 0 \quad 0$$

- Multiplicada cada bloque por 7 módulo 13:

$$0 \cdot 7 \bmod 13 = 0, \quad 7 \cdot 7 \bmod 13 = 10, \quad 1 \cdot 7 \bmod 13 = 7$$

$$5 \cdot 7 \bmod 13 = 9, \quad 1 \cdot 7 \bmod 13 = 7, \quad 1 \cdot 7 \bmod 13 = 7$$

$$0 \cdot 7 \bmod 13 = 0, \quad 0 \cdot 7 \bmod 13 = 0$$

- Envía a A:

$$gk = 11 \quad \text{y} \quad [0 \quad 10 \quad 7 \quad 9 \quad 7 \quad 7 \quad 0 \quad 0].$$

Cifrado ElGamal: Ejemplo

Descifrado del mensaje (A)

- A recibe

$$gk = 11 \quad \text{y} \quad [0 \quad 10 \quad 7 \quad 9 \quad 7 \quad 7 \quad 0 \quad 0].$$

Cifrado ElGamal: Ejemplo

Descifrado del mensaje (A)

- A recibe

$$gk = 11 \quad \text{y} \quad [0 \quad 10 \quad 7 \quad 9 \quad 7 \quad 7 \quad 0 \quad 0].$$

- Calcula $gk^a \bmod q = 11^5 \bmod 13 = 7$, y su inverso modular:

$$7^{-1} \bmod 13 = 2.$$

Cifrado ElGamal: Ejemplo

Descifrado del mensaje (A)

- A recibe

$$gk = 11 \quad \text{y} \quad [0 \quad 10 \quad 7 \quad 9 \quad 7 \quad 7 \quad 0 \quad 0].$$

- Calcula $gk^a \bmod q = 11^5 \bmod 13 = 7$, y su inverso modular:

$$7^{-1} \bmod 13 = 2.$$

- Multiplica cada bloque recibido por el valor obtenido:

$$0 \cdot 2 \bmod 13 = 0, \quad 10 \cdot 2 \bmod 13 = 7, \quad 7 \cdot 2 \bmod 13 = 1$$

$$9 \cdot 2 \bmod 13 = 5, \quad 7 \cdot 2 \bmod 13 = 1, \quad 7 \cdot 2 \bmod 13 = 1$$

$$0 \cdot 2 \bmod 13 = 0, \quad 0 \cdot 2 \bmod 13 = 0.$$

Cifrado ElGamal: Ejemplo

Descifrado del mensaje (A)

- A recibe

$$gk = 11 \quad \text{y} \quad [0 \quad 10 \quad 7 \quad 9 \quad 7 \quad 7 \quad 0 \quad 0].$$

- Calcula $gk^a \bmod q = 11^5 \bmod 13 = 7$, y su inverso modular:

$$7^{-1} \bmod 13 = 2.$$

- Multiplica cada bloque recibido por el valor obtenido:

$$0 \cdot 2 \bmod 13 = 0, \quad 10 \cdot 2 \bmod 13 = 7, \quad 7 \cdot 2 \bmod 13 = 1$$

$$9 \cdot 2 \bmod 13 = 5, \quad 7 \cdot 2 \bmod 13 = 1, \quad 7 \cdot 2 \bmod 13 = 1$$

$$0 \cdot 2 \bmod 13 = 0, \quad 0 \cdot 2 \bmod 13 = 0.$$

- No hace falta que complete los bloques (ya tienen longitud 1)

Cifrado ElGamal: Ejemplo

Descifrado del mensaje (A)

- A recibe

$$gk = 11 \quad \text{y} \quad [0 \quad 10 \quad 7 \quad 9 \quad 7 \quad 7 \quad 0 \quad 0].$$

- Calcula $gk^a \bmod q = 11^5 \bmod 13 = 7$, y su inverso modular:

$$7^{-1} \bmod 13 = 2.$$

- Multiplica cada bloque recibido por el valor obtenido:

$$0 \cdot 2 \bmod 13 = 0, \quad 10 \cdot 2 \bmod 13 = 7, \quad 7 \cdot 2 \bmod 13 = 1$$

$$9 \cdot 2 \bmod 13 = 5, \quad 7 \cdot 2 \bmod 13 = 1, \quad 7 \cdot 2 \bmod 13 = 1$$

$$0 \cdot 2 \bmod 13 = 0, \quad 0 \cdot 2 \bmod 13 = 0.$$

- No hace falta que complete los bloques (ya tienen longitud 1)
- Concatena los bloques, separa de dos en dos y recupera el mensaje:

07	15	11	00
h	*o*	*l*	*a*