Criptografía al alcance de todos

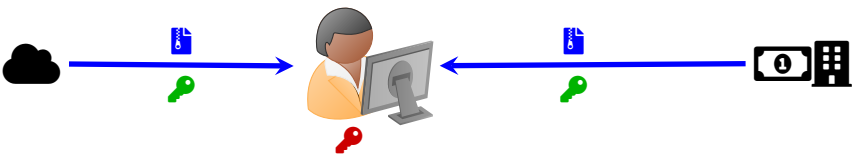
Reuniones virtuales

Una empresa docente, Universidad de los Andes

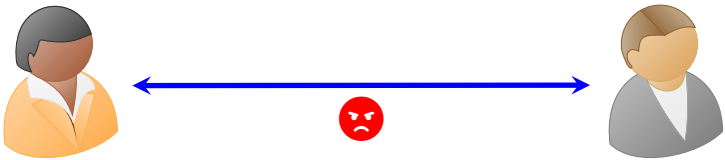
Enrique Acosta Jaramillo

Grupo LEMA www.grupolema.org
Mathematics Consortium Working Group

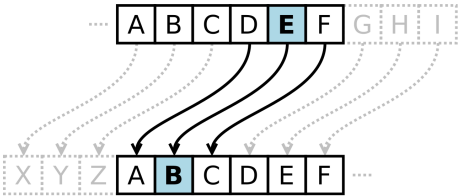
2 de julio de 2024



Diseño de mecanismos para comunicación segura frente a agentes adversarios.



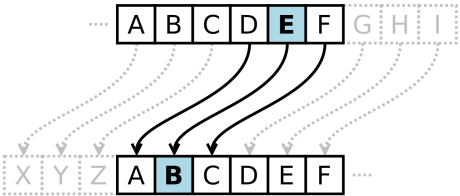
Uno de los primeros sistemas:
La cifra de César



No es tan difícil "quebrar" el sistema.
(Frecuencia de aparición de letras)

Imagen de wikipedia de dominio público: `https://commons.wikimedia.org/wiki/File:Caesar_cipher_left_shift_of_3.svg`

Uno de los primeros sistemas:
La cifra de César



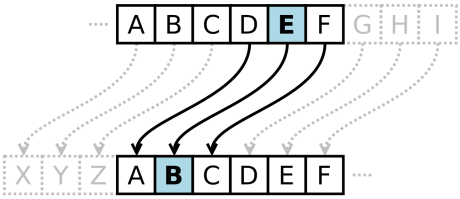
No es tan difícil "quebrar" el sistema.
(Frecuencia de aparición de letras)

Criptografía moderna

- objetos matemáticos complejos (curvas elípticas, campos finitos)
- números MUY grandes.

Imagen de wikipedia de dominio público: `https://commons.wikimedia.org/wiki/File:Caesar_cipher_left_shift_of_3.svg`

Uno de los primeros sistemas:
La cifra de César



No es tan difícil "quebrar" el sistema.
(Frecuencia de aparición de letras)

Criptografía moderna

- objetos matemáticos complejos (curvas elípticas, campos finitos)
- números MUY grandes.

Ideas de fondo:

- simples
- ingeniosas
- **¡se pueden entender con matemáticas escolares!**

Imagen de wikipedia de dominio público: `https://commons.wikimedia.org/wiki/File:Caesar_cipher_left_shift_of_3.svg`

Los mensajes como números

Cualquier mensaje se puede ver como un número

Los mensajes como números

Cualquier mensaje se puede ver como un número

símbolo	código
A	1001
a	1002
á	1003
B	1004
b	1005
C	1006
c	1007
⋮	⋮
#	1267
%	1268
(espacio)	1269
¿	1270
?	1271
⋮	⋮

$$1\,0\,0\,1\,1\,0\,0\,7\,1\,0\,0\,3\,1\,2\,6\,9\,1\,0\,4\,7$$

Los mensajes como números

Cualquier mensaje se puede ver como un número

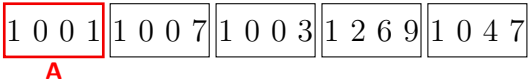
símbolo	código
A	1001
a	1002
á	1003
B	1004
b	1005
C	1006
c	1007
⋮	⋮
#	1267
%	1268
(espacio)	1269
¿	1270
?	1271
⋮	⋮

$$\boxed{1\ 0\ 0\ 1}\boxed{1\ 0\ 0\ 7}\boxed{1\ 0\ 0\ 3}\boxed{1\ 2\ 6\ 9}\boxed{1\ 0\ 4\ 7}$$

Los mensajes como números

Cualquier mensaje se puede ver como un número

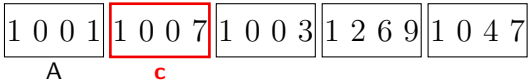
símbolo	código
A	**1001**
a	1002
á	1003
B	1004
b	1005
C	1006
c	1007
⋮	⋮
#	1267
%	1268
(espacio)	1269
¿	1270
?	1271
⋮	⋮



Los mensajes como números

Cualquier mensaje se puede ver como un número

símbolo	código
A	1001
a	1002
á	1003
B	1004
b	1005
C	1006
c	**1007**
⋮	⋮
#	1267
%	1268
(espacio)	1269
¿	1270
?	1271
⋮	⋮



Los mensajes como números

Cualquier mensaje se puede ver como un número

símbolo	código
A	1001
a	1002
á	**1003**
B	1004
b	1005
C	1006
c	1007
⋮	⋮
#	1267
%	1268
(espacio)	1269
¿	1270
?	1271
⋮	⋮

Los mensajes como números

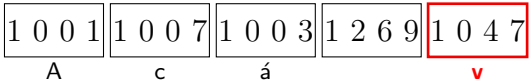
Cualquier mensaje se puede ver como un número

símbolo	código
A	1001
a	1002
á	1003
B	1004
b	1005
C	1006
c	1007
⋮	⋮
#	1267
%	1268
(espacio)	**1269**
¿	1270
?	1271
⋮	⋮

Los mensajes como números

Cualquier mensaje se puede ver como un número

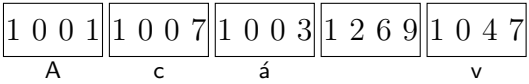
símbolo	código
A	1001
a	1002
á	1003
B	1004
b	1005
C	1006
c	1007
⋮	⋮
#	1267
%	1268
(espacio)	1269
¿	1270
?	1271
⋮	⋮



Los mensajes como números

Cualquier mensaje se puede ver como un número

símbolo	código
A	1001
a	1002
á	1003
B	1004
b	1005
C	1006
c	1007
⋮	⋮
#	1267
%	1268
(espacio)	1269
¿	1270
?	1271
⋮	⋮

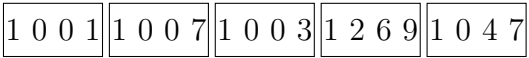


- Una novela entera es un número.

Los mensajes como números

Cualquier mensaje se puede ver como un número

símbolo	código
A	1001
a	1002
á	1003
B	1004
b	1005
C	1006
c	1007
⋮	⋮
#	1267
%	1268
(espacio)	1269
¿	1270
?	1271
⋮	⋮

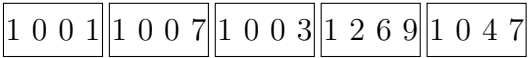


- Una novela entera es un número.
- La historia de sus vidas es un número.

Los mensajes como números

Cualquier mensaje se puede ver como un número

símbolo	código
A	1001
a	1002
á	1003
B	1004
b	1005
C	1006
c	1007
⋮	⋮
#	1267
%	1268
(espacio)	1269
¿	1270
?	1271
⋮	⋮

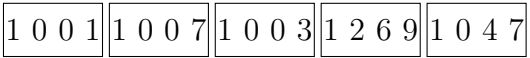


- Una novela entera es un número.
- La historia de sus vidas es un número.
- Su clave más compleja es un número.

Los mensajes como números

Cualquier mensaje se puede ver como un número

símbolo	código
A	1001
a	1002
á	1003
B	1004
b	1005
C	1006
c	1007
⋮	⋮
#	1267
%	1268
(espacio)	1269
¿	1270
?	1271
⋮	⋮



- Una novela entera es un número.
- La historia de sus vidas es un número.
- Su clave más compleja es un número.

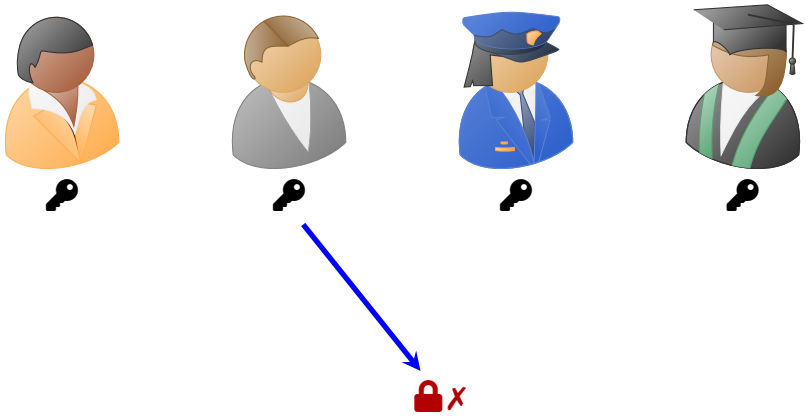
Criptografía: almacenamiento o envío de números de manera segura.

Primer ejemplo:

Esquema de Shamir

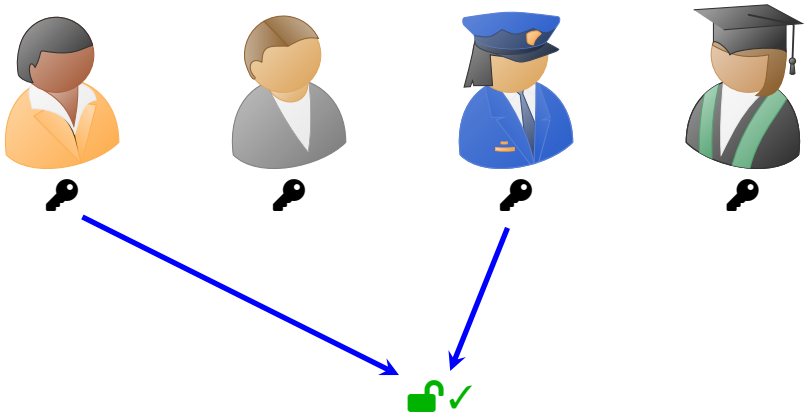
La idea de las llaves

- 1 llave no abre la caja fuerte.
- 2 o más llaves abren la caja fuerte.



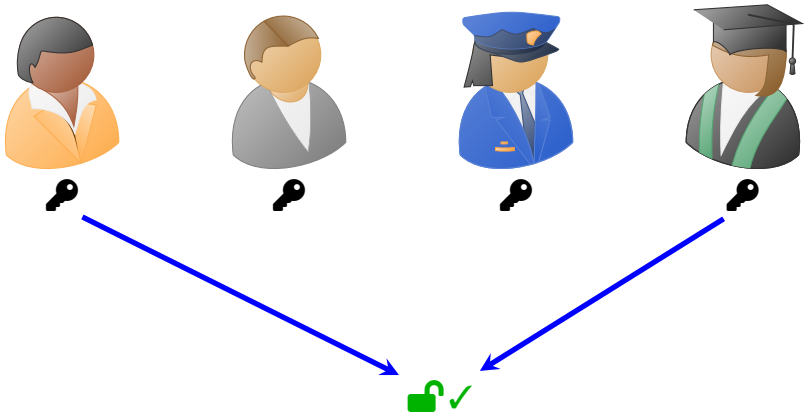
La idea de las llaves

- 1 llave no abre la caja fuerte.
- 2 o más llaves abren la caja fuerte.



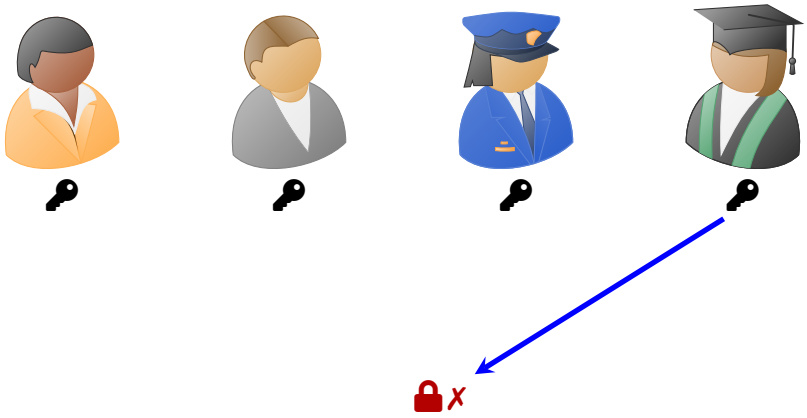
La idea de las llaves

- 1 llave no abre la caja fuerte.
- 2 o más llaves abren la caja fuerte.



La idea de las llaves

- 1 llave no abre la caja fuerte.
- 2 o más llaves abren la caja fuerte.



Actividad con Shamir

Entrega de llaves 

En persona:

- Se les entregó al entrar un papel con su llave.

Actividad con Shamir

Entrega de llaves 🔑

En persona:

- Se les entregó al entrar un papel con su llave.

Modalidad virtual:

- Vayan por su llave a `https://enriqueacosta.github.io/crypto/shamir-random.html`
- Avisen cuando ya la tengan.
- **¡no la compartan!**
- La página genera una llave única para cada uno (ya explico cómo).

Actividad con Shamir

Para qué sirve su llave 🔑:

- Hay una caja fuerte con una clave de 4 dígitos.

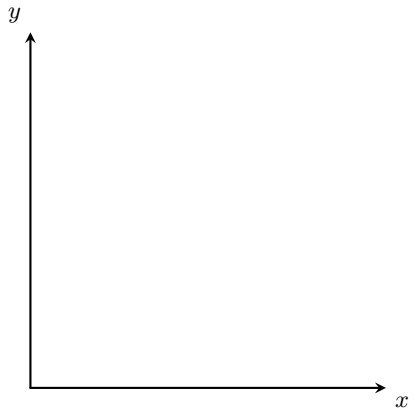
Actividad con Shamir

Para qué sirve su llave 🔑:

- Hay una caja fuerte con una clave de 4 dígitos.
- ¡Su llave sirve para descifrar la clave!

Shamir con rectas

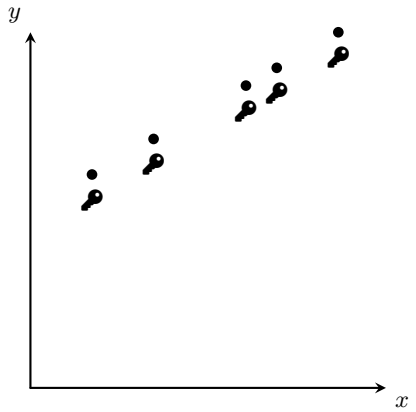
¡Usemos el sistema!



Shamir con rectas

¡Usemos el sistema!

- Sus llaves son puntos en el plano que están todos sobre una misma recta.

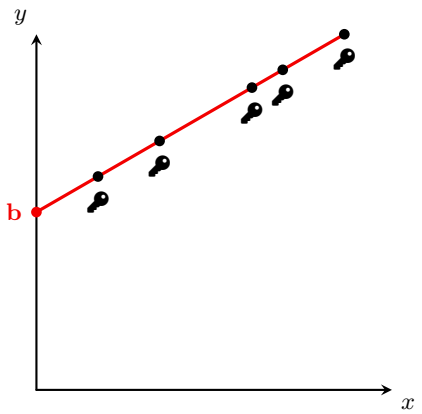


Shamir con rectas

¡Usemos el sistema!

- Sus llaves son puntos en el plano que están todos sobre una misma recta.
- El mensaje secreto es la intersección de la recta con el eje vertical

$$y = mx + \mathbf{b}$$



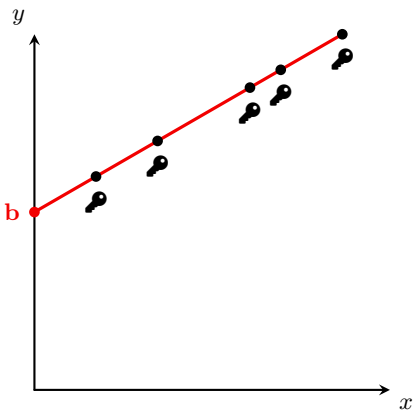
Shamir con rectas

¡Usemos el sistema!

- Sus llaves son puntos en el plano que están todos sobre una misma recta.
- El mensaje secreto es la intersección de la recta con el eje vertical

$$y = mx + \mathbf{b}$$

- Con su punto no pueden saber el mensaje secreto, **pero si lo comparten con alguien más, ¡lo pueden encontrar!**



Shamir con rectas

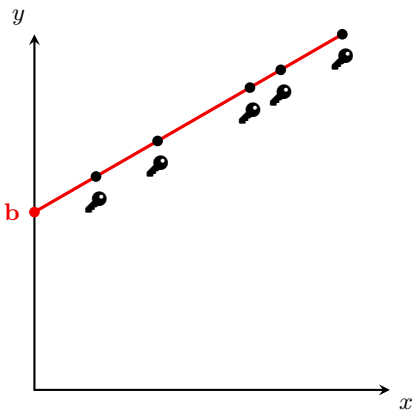
¡Usemos el sistema!

- Sus llaves son puntos en el plano que están todos sobre una misma recta.
- El mensaje secreto es la intersección de la recta con el eje vertical

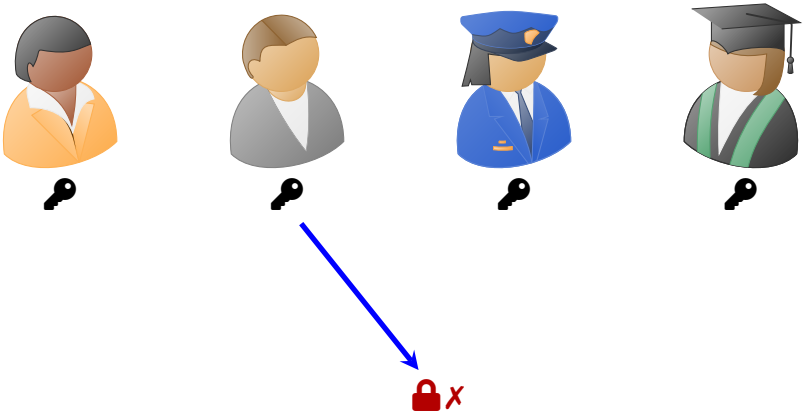
$$y = mx + \mathbf{b}$$

- Con su punto no pueden saber el mensaje secreto, **pero si lo comparten con alguien más, ¡lo pueden encontrar!**

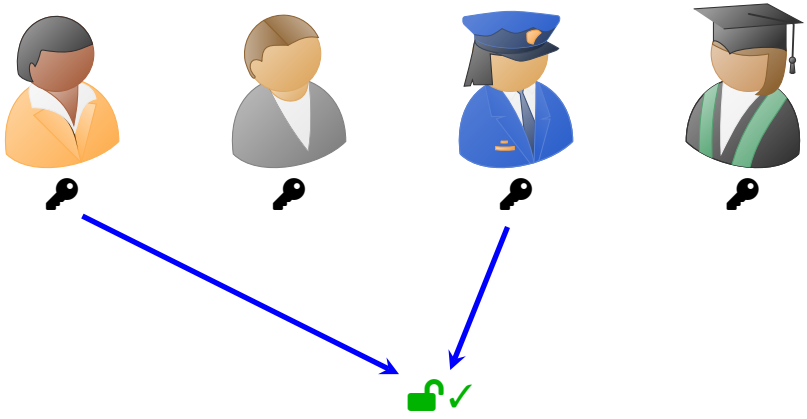
¡Encuentren el mensaje secreto!
Escribanlo en el chat



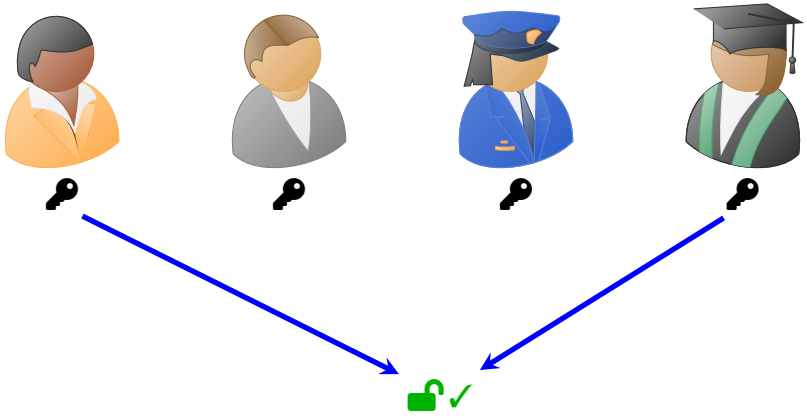
¡Tal cual!



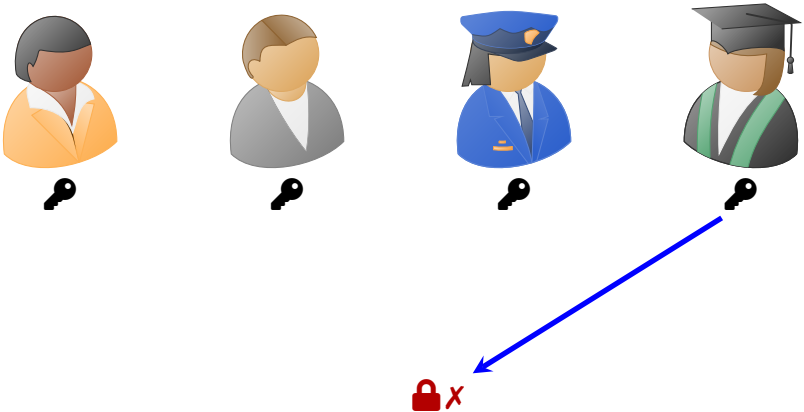
¡Tal cual!



¡Tal cual!

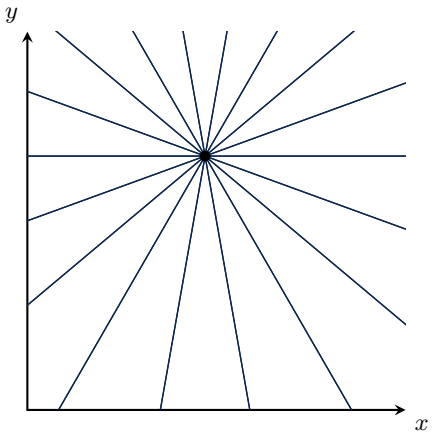


¡Tal cual!



¿Por qué funciona el sistema?

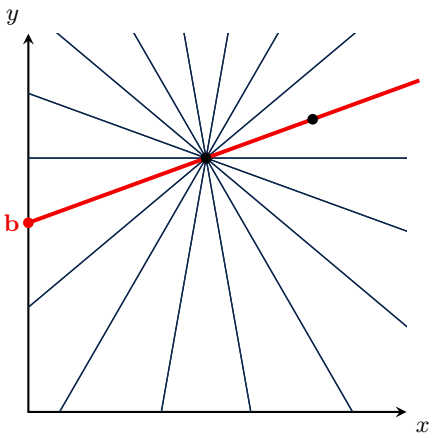
Un hecho geométrico muy simple:



¿Por qué funciona el sistema?

Un hecho geométrico muy simple:

Dos puntos determinan la recta, pero uno solo no.

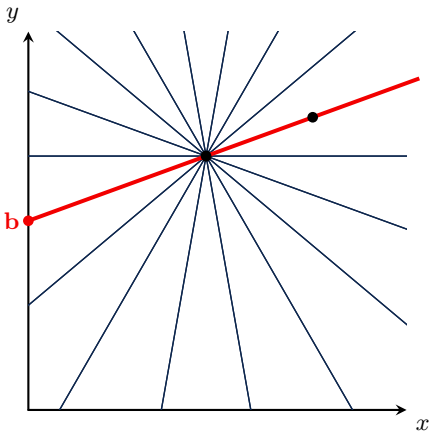


¿Por qué funciona el sistema?

Un hecho geométrico muy simple:

Dos puntos determinan la recta, pero uno solo no.

¡Una llave sola no sirve!



Testamento

Clave de cuenta bancaria

- dar un punto a cada miembro de su familia
- solo pueden desbloquear la clave si 2 o más miembros de la familia deciden desbloquearlo

Testamento

Clave de cuenta bancaria

- dar un punto a cada miembro de su familia
- solo pueden desbloquear la clave si 2 o más miembros de la familia deciden desbloquearlo

Guardar claves propias

- Guardar papelitos con llaves (puntos) en distintos lugares.
- Para recobrar la clave deben recordar dónde están 2 de los papelitos.
- ¡La clave no está en ninguno de los papelitos!

Posibles ideas de actividades con estudiantes

- que descifren el mensaje secreto pasando de la forma punto-pendiente $(y - y_0 = m(x - x_0))$ a la forma pendiente-intercepto $y = mx + \mathbf{b}$.

Posibles ideas de actividades con estudiantes

- que descifren el mensaje secreto pasando de la forma punto-pendiente $(y - y_0 = m(x - x_0))$ a la forma pendiente-intercepto $y = mx + \mathbf{b}$.
- que decodifiquen mensajes con un sistema que se les da (como hicieron uds.)

Posibles ideas de actividades con estudiantes

- que descifren el mensaje secreto pasando de la forma punto-pendiente ($y - y_0 = m(x - x_0)$) a la forma pendiente-intercepto $y = mx + \mathbf{b}$.
- que decodifiquen mensajes con un sistema que se les da (como hicieron uds.)
- que guarden un secreto con puntos y lo prueben con sus compañeros.

Mayor seguridad: Shamir que requiere 3 llaves

Mayor seguridad: Shamir que requiere 3 llaves

¿Cómo podemos hacer un sistema en el que se necesitan **tres** llaves para desbloquear el secreto?

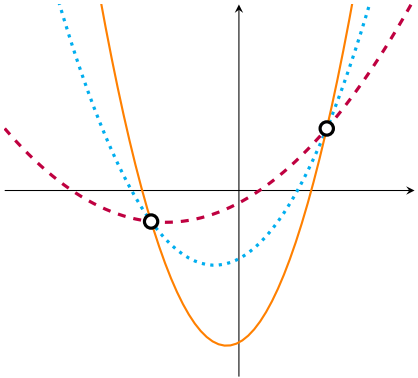
Mayor seguridad: Shamir que requiere 3 llaves

¿Cómo podemos hacer un sistema en el que se necesitan **tres** llaves para desbloquear el secreto?

¡Con cuadráticas!

- Tres puntos determinan una cuadrática de manera única.
- Pero dos o menos puntos no la determinan.

Dos llaves (puntos) no determinan una parabola.



Shamir con necesidad de tres llaves

Sistema de tres llaves

- Guardo el secreto en el término constante $\mathbf{c}$ de una cuadrática (puedo escoger los valores de a y b que quiera).

$$ax^2 + bx + \mathbf{c}$$

- Reparto como llaves puntos en la cuadrática.
- Puedo repartir todas las llaves que quiera.
- Los que quieran desbloquear el secreto $\mathbf{c}$ solo lo pueden encontrar si tienen acceso a tres o más llaves (puntos).

Shamir con necesidad de tres llaves

Sistema de tres llaves

- Guardo el secreto en el término constante $\mathbf{c}$ de una cuadrática (puedo escoger los valores de a y b que quiera).

$$ax^2 + bx + \mathbf{c}$$

- Reparto como llaves puntos en la cuadrática.
- Puedo repartir todas las llaves que quiera.
- Los que quieran desbloquear el secreto $\mathbf{c}$ solo lo pueden encontrar si tienen acceso a tres o más llaves (puntos).

¿Cómo se encuentra la cuadrática que pasa por tres puntos?

Shamir con necesidad de tres llaves

Sistema de tres llaves

- Guardo el secreto en el término constante $\mathbf{c}$ de una cuadrática (puedo escoger los valores de a y b que quiera).

$$ax^2 + bx + \mathbf{c}$$

- Reparto como llaves puntos en la cuadrática.
- Puedo repartir todas las llaves que quiera.
- Los que quieran desbloquear el secreto $\mathbf{c}$ solo lo pueden encontrar si tienen acceso a tres o más llaves (puntos).

¿Cómo se encuentra la cuadrática que pasa por tres puntos? sistemas de ecuaciones lineales

https://es.wikipedia.org/wiki/Esquema_de_Shamir

Sistema de compartición de secretos de Shamir [editar]

La idea esencial de la combinación de umbral de Shamir es que dos puntos son suficientes para definir una línea recta, tres puntos lo son para definir una parábola, cuatro para definir una curva cúbica y así sucesivamente. Es decir, son necesarios $n+1$ puntos para definir un polinomio de grado n.

Supongamos que queremos trabajar con un umbral de (k, n) para compartir un secreto S (cualquier número, sin pérdida de generalidad) siendo $k < n$. La elección de los valores de k y n determina la fortaleza del sistema.

Eligiendo al azar $(k-1)$ coeficientes $a_1, \cdots, a_{k-1}$, y siendo $a_0 = S$, se construye el polinomio $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{k-1} x^{k-1}$. Calculamos cualesquiera n puntos a partir del mismo, por ejemplo determinamos que $i = 1, \cdots, n$ de lo que se deriva $(i, f(i))$. A todo participante en el secreto se le da un punto (un par de valores, el de entrada y el de salida para el polinomio)

Dado cualquier subconjunto de k entre estos pares, podemos calcular los coeficientes del polinomio mediante interpolación y luego despejar a_0, que es el secreto.

https://es.wikipedia.org/wiki/Esquema_de_Shamir

Sistema de compartición de secretos de Shamir [editar]

La idea esencial de la combinación de umbral de Shamir es que dos puntos son suficientes para definir una línea recta, tres puntos lo son para definir una parábola, cuatro para definir una curva cúbica y así sucesivamente. Es decir, son necesarios $n+1$ puntos para definir un polinomio de grado n.

Supongamos que queremos trabajar con un umbral de (k, n) para compartir un secreto S (cualquier número, sin pérdida de generalidad) siendo $k < n$. La elección de los valores de k y n determina la fortaleza del sistema.

El mensaje secreto

Eligiendo al azar $(k-1)$ coeficientes $a_1, \cdots, a_{k-1}$, y siendo $a_0 = S$, se construye el polinomio $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{k-1} x^{k-1}$. Calculamos cualesquiera n puntos a partir del mismo, por ejemplo determinamos que $i = 1, \cdots, n$ de lo que se deriva $(i, f(i))$. A todo participante en el secreto se le da un punto (un par de valores, el de entrada y el de salida para el polinomio)

Dado cualquier subconjunto de k entre estos pares, podemos calcular los coeficientes del polinomio mediante interpolación y luego despejar a_0, que es el secreto.

El número de llaves necesarias para desbloquear el secreto

Esquema de Shamir en el mundo

Guadrar la clave de billeteras digitales de criptomonedas.

Introduction

In the world of cryptocurrencies, security is of paramount importance. As digital assets gain popularity, the need to protect them from theft or loss becomes increasingly crucial. Hardware wallets have emerged as a popular solution for securely storing cryptocurrencies, offering a tangible and offline method of safeguarding private keys. To enhance the security of hardware wallets, a technique called Shamir Secret Sharing (SSS) has gained traction. SSS divides a secret into multiple shares, which are then distributed across different devices or individuals. In this blog, we will

`https://www.cypherock.com/blogs/`

`shamir-secret-sharing-in-hardware-wallets`

`https://d-central.tech/`

`how-shamirs-secret-sharing-revolutionizes-bitcoin-security`

¿Quién abrió la caja fuerte?

Un problema con estos sistemas es que no se sabe quién abrió la caja fuerte.

Sistema

- Las llaves van a ser ecuaciones de rectas en el plano.
- Clave compartida de dos rectas: coordenada y del punto de intersección. Cada pareja tiene una clave distinta.
- Diseño: hay que encontrar rectas en el plano que se interceptan en coordenadas y distintas.
- ¡Interesante reto – sobre todo para poder jugar con el sistema que uno crea!

Otro ejemplo:

Intercambio de llaves con Diffie–Hellman

Intercambio de llaves con Diffie–Hellman

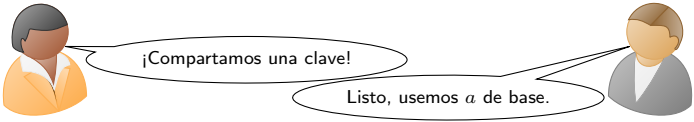
Acordar una “clave” para compartir sin que se transfiera la clave...

Intercambio de llaves con Diffie–Hellman

Acordar una “clave” para compartir sin que se transfiera la clave...

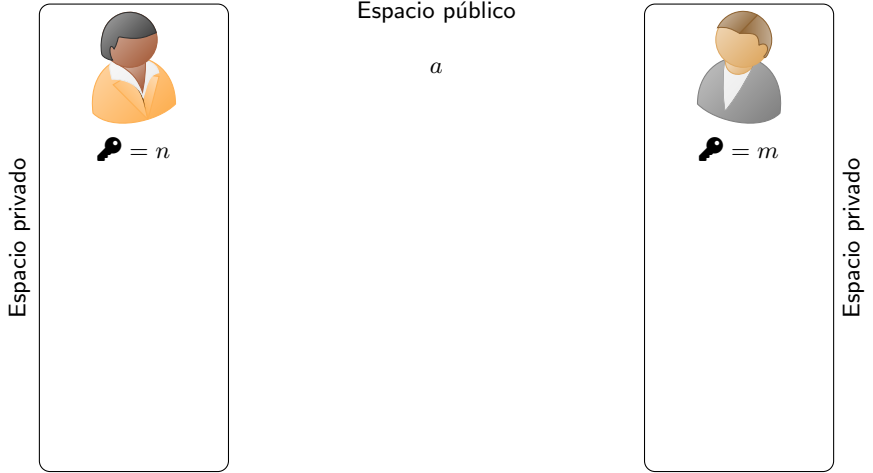
Intercambio de llaves con Diffie–Hellman

Acordar una “clave” para compartir sin que se transfiera la clave...



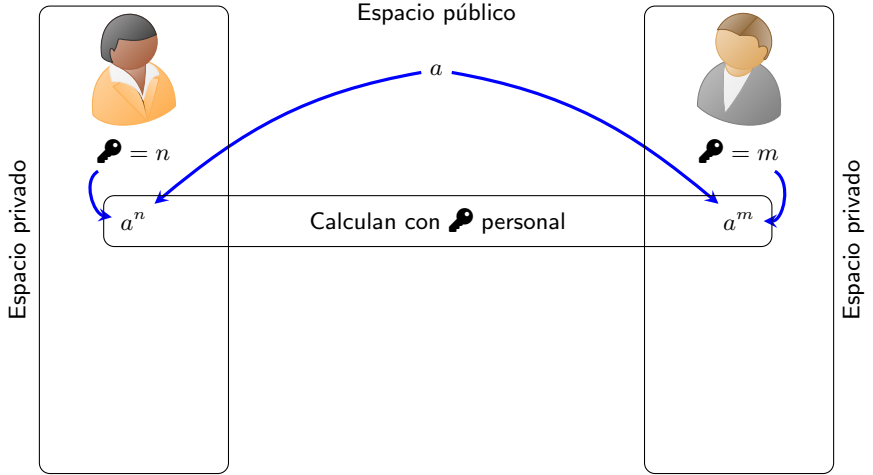
Intercambio de llaves con Diffie–Hellman

Acordar una “clave” para compartir sin que se transfiera la clave...



Intercambio de llaves con Diffie–Hellman

Acordar una “clave” para compartir sin que se transfiera la clave...



Intercambio de llaves con Diffie–Hellman

Acordar una “clave” para compartir sin que se transfiera la clave...

Espacio público

a

Espacio privado

$= n$

calcula:

a^n

Espacio privado

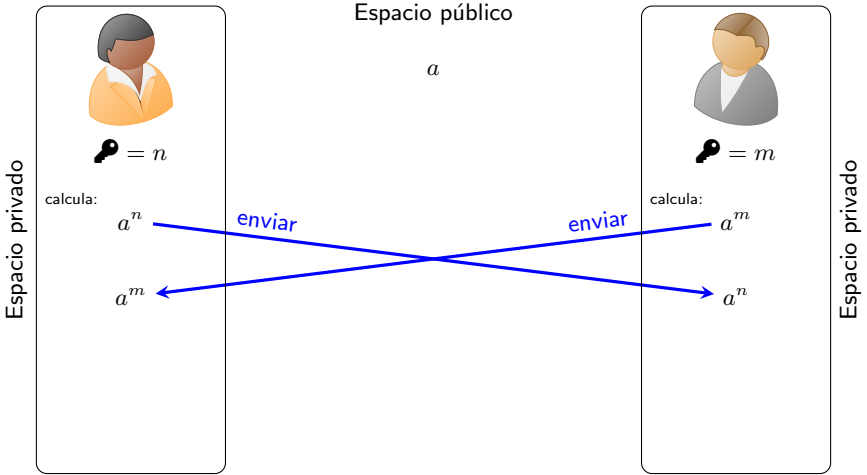
$= m$

calcula:

a^m

Intercambio de llaves con Diffie–Hellman

Acordar una “clave” para compartir sin que se transfiera la clave...



Intercambio de llaves con Diffie–Hellman

Acordar una “clave” para compartir sin que se transfiera la clave...

Espacio público

a

a^n

a^m

Espacio privado

$= n$

calcula:

a^n

recibe:

a^m

$= m$

calcula:

a^m

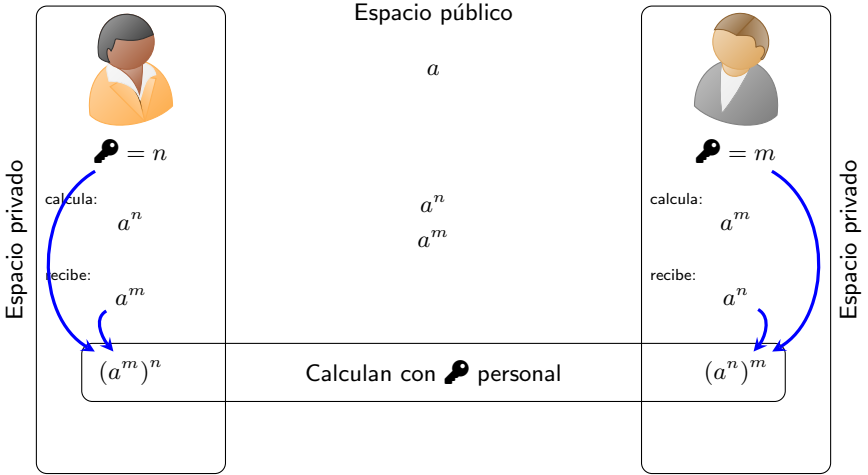
recibe:

a^n

Espacio privado

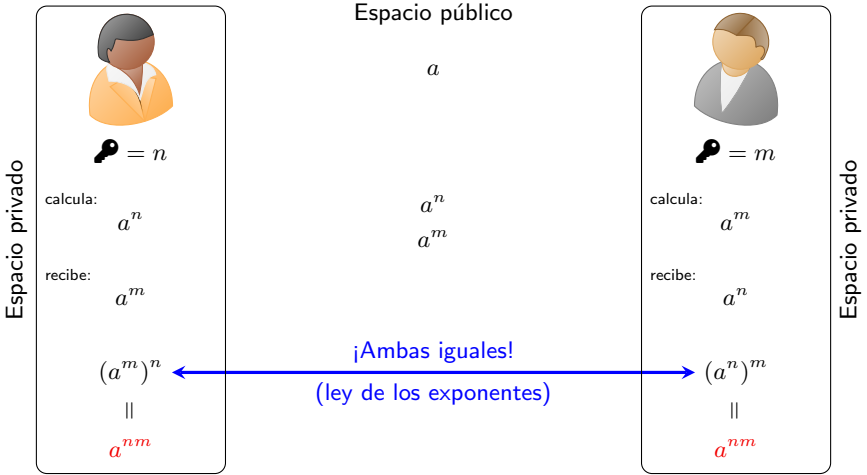
Intercambio de llaves con Diffie–Hellman

Acordar una “clave” para compartir sin que se transfiera la clave...



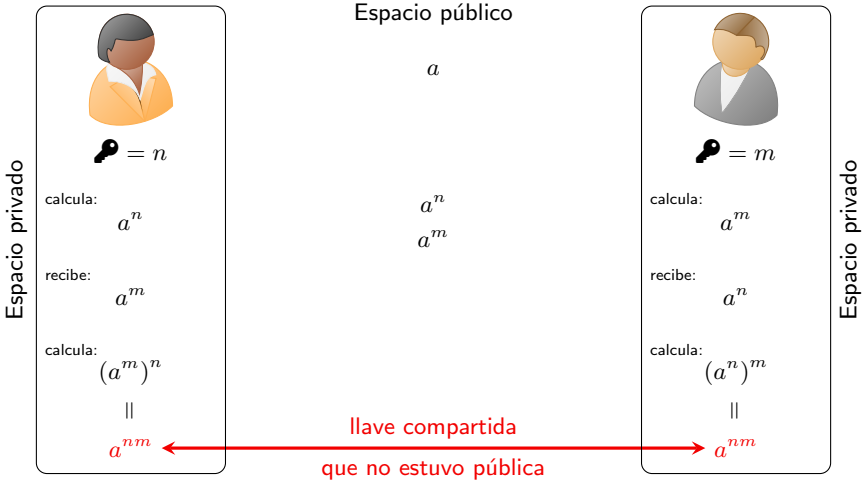
Intercambio de llaves con Diffie–Hellman

Acordar una “clave” para compartir sin que se transfiera la clave...



Intercambio de llaves con Diffie–Hellman

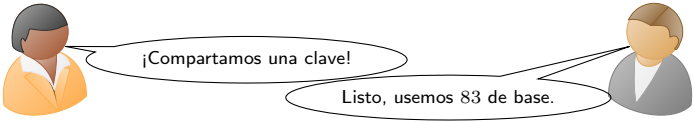
Acordar una "clave" para compartir sin que se transfiera la clave...



Ejemplo

Ejemplo

Ejemplo



Ejemplo

Espacio público

83

Espacio privado

$= n$

calcula:

a^n

$= m$

calcula:

a^m

Espacio privado

Ejemplo

Espacio público

83

27136050989627
326940373369

Espacio privado

$= n$

calcula:

a^n

recibe:

a^m

Espacio privado

$= m$

calcula:

a^m

recibe:

a^n

Ejemplo

Espacio público

83

27136050989627
326940373369

Espacio privado

$= n$

calcula:

a^n

recibe:

a^m

calcula:

$(a^m)^n$

$\|$

a^{nm}

¿Cuál es la llave compartida?

Espacio privado

$= m$

calcula:

a^m

recibe:

a^n

calcula:

$(a^n)^m$

$\|$

a^{nm}

Ejemplo

Espacio público

$a = 83$

$a^n = 27136050989627$

$a^m = 326940373369$

Espacio privado

$= n$

calcula:

a^n

recibe:

a^m

calcula:

$(a^m)^n$

$\|$

a^{nm}

¿Cuál es la llave compartida?

$= m$

calcula:

a^m

recibe:

a^n

calcula:

$(a^n)^m$

$\|$

a^{nm}

Espacio privado

Ejemplo

Espacio público

$a = 83$

$a^n = 27136050989627$

$a^m = 326940373369$

¡logarítmos!

$m = \log_{83}(326940373369) = 6$

$n = \log_{83}(27136050989627) = 7$

¿Cuál es la llave compartida?

Espacio privado

$= n$

calcula:

a^n

recibe:

a^m

calcula:

$(a^m)^n$

||

a^{nm}

Espacio privado

$= m$

calcula:

a^m

recibe:

a^n

calcula:

$(a^n)^m$

||

a^{nm}

Ejemplo

Espacio público

$a = 83$

$a^n = 27136050989627$

$a^m = 326940373369$

¡logarítmos!

$m = \log_{83}(326940373369) = 6$

$n = \log_{83}(27136050989627) = 7$

¿Cuál es la llave compartida?

Espacio privado

$= n$

calcula:

a^n

recibe:

a^m

calcula:

$(a^m)^n$

||

a^{nm}

Espacio privado

$= m$

calcula:

a^m

recibe:

a^n

calcula:

$(a^n)^m$

||

a^{nm}

Llave compartida a^{nm} :

399282135658682469334331901689876886678820965774126540592961885129481494196023689

Diffie–Hellman en el mundo real

https://en.wikipedia.org/wiki/Diffie\OT1\textendashHellman_key_exchange

Cryptographic explanation [edit]

The simplest and the original implementation,[2] later formalized as **Finite Field Diffie-Hellman** in *RFC 7919*,[9] of the protocol uses the multiplicative group of integers modulo *p*, where *p* is prime, and *g* is a primitive root modulo *p*. These two values are chosen in this way to ensure that the resulting shared secret can take on any value from 1 to *p*–1. Here is an example of the protocol, with non-secret values in blue, and secret values in **red**.

1. Alice and Bob publicly agree to use a modulus $p = 23$ and base $g = 5$ (which is a primitive root modulo 23).
2. Alice chooses a secret integer $a = 4$, then sends Bob $A = g^a \bmod p$
   - $A = 5^4 \bmod 23 = 4$ (in this example both A and a have the same value 4, but this is usually not the case)
3. Bob chooses a secret integer $b = 3$, then sends Alice $B = g^b \bmod p$
   - $B = 5^3 \bmod 23 = 10$
4. Alice computes $s = B^a \bmod p$
   - $s = 10^4 \bmod 23 = 18$
5. Bob computes $s = A^b \bmod p$
   - $s = 4^3 \bmod 23 = 18$
6. Alice and Bob now share a secret (the number 18).

Both Alice and Bob have arrived at the same values because under mod p,

$$A^b \bmod p = g^{ab} \bmod p = g^{ba} \bmod p = B^a \bmod p$$

More specifically,

$$(g^a \bmod p)^b \bmod p = (g^b \bmod p)^a \bmod p$$

Only *a* and *b* are kept secret. All the other values – *p*, *g*, g^a mod *p*, and g^b mod *p* – are sent in the clear. The strength of the scheme comes from the fact that g^{ab} mod *p* = g^{ba} mod *p* take

1976: Uno de los primeros sistemas criptográficos para el intercambio de llaves. **Todavía se usa.**

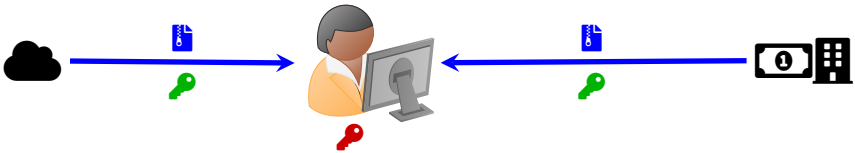
En un campo finito de tamaño MUY grande es **MUY** dificil calcular logarítmos.

Un sistema muy popular:

Public-key cryptography
Criptografía asimétrica

Public-key cryptography: criptografía asimétrica

- Sistema para que me puedan enviar secretos de manera segura.
- Lo que se usa en internet para la gran mayoría de transacciones seguras.



Public-key cryptography: criptografía asimétrica

- Sistema para que me puedan enviar secretos de manera segura.
- Lo que se usa en internet para la gran mayoría de transacciones seguras.

Partes

- Una llave pública:
  - la usan otras personas para encriptar información para enviarme.
- Una llave mia secreta (llave privada)
  - nunca la comparto
  - me sirve para desencriptar los mensajes que me mandan.

Mi llave secreta (llave privada)

No se las voy a dar!!!

Llave pública: para ustedes

¡Tres polinomios de grado 2!

- $f(x) = x^2 - 5x + 6$
- $g(x) = 2x^2 + 2x - 24$
- $h(x) = -5x^2 + 10x + 15$

Cómo enviarme un mensaje (número m)

Mejor con un ejemplo:

- Me van a enviar la clave de su tarjeta de crédito:

Cómo enviarme un mensaje (número $\mathbf{m}$)

Mejor con un ejemplo:

- Me van a enviar la clave de su tarjeta de crédito: **2222**

Cómo enviarme un mensaje (número $\mathbf{m}$)

Mejor con un ejemplo:

- Me van a enviar la clave de su tarjeta de crédito: **2222**
- Eligen A, B y C aleatorios:

$$A = -189 \qquad B = 438 \qquad C = 7$$

Cómo enviarme un mensaje (número $\mathbf{m}$)

Mejor con un ejemplo:

- Me van a enviar la clave de su tarjeta de crédito: **2222**
- Eligen A, B y C aleatorios:

$$A = -189 \qquad B = 438 \qquad C = 7$$

- Escriben el polinomio

$$Af(x) + Bg(x) + Ch(x) + \mathbf{m}$$

Cómo enviarme un mensaje (número $\mathbf{m}$)

Mejor con un ejemplo:

- Me van a enviar la clave de su tarjeta de crédito: **2222**
- Eligen A, B y C aleatorios:

$$A = -189 \qquad B = 438 \qquad C = 7$$

- Escriben el polinomio

$$Af(x) + Bg(x) + Ch(x) + \mathbf{m}$$

$$-189(x^2 - 5x + 6) + 438(2x^2 + 2x - 24) + 7(-5x^2 + 10x + 15) + \mathbf{2222}$$

Cómo enviarme un mensaje (número $\mathbf{m}$)

Mejor con un ejemplo:

- Me van a enviar la clave de su tarjeta de crédito: **2222**
- Eligen A, B y C aleatorios:

$$A = -189 \qquad B = 438 \qquad C = 7$$

- Escriben el polinomio (y lo reescriben en la forma $ax^2 + bx + c$)

$$Af(x) + Bg(x) + Ch(x) + \mathbf{m}$$

$$-189(x^2 - 5x + 6) + 438(2x^2 + 2x - 24) + 7(-5x^2 + 10x + 15) + \mathbf{2222}$$

$$652x^2 + 1891x - 9319$$

Cómo enviarme un mensaje (número $\mathbf{m}$)

Mejor con un ejemplo:

- Me van a enviar la clave de su tarjeta de crédito: **2222**
- Eligen A, B y C aleatorios:

$$A = -189 \qquad B = 438 \qquad C = 7$$

- Escriben el polinomio (y lo reescriben en la forma $ax^2 + bx + c$)

$$Af(x) + Bg(x) + Ch(x) + \mathbf{m}$$

$$-189(x^2 - 5x + 6) + 438(2x^2 + 2x - 24) + 7(-5x^2 + 10x + 15) + \mathbf{2222}$$

$$652x^2 + 1891x - 9319$$

- Me mandan $652x^2 + 1891x - 9319$.
- El **2222** ya no es visible y no se puede recuperar sin mi llave secreta (¡porque uds no están enviando los valores de A, B, C tampoco!).

¡¿¡¿¡¿Cómo funciona?!?!?!

Mi "llave" secreta

Yo sé algo que no sabe el público:

- $f(x)$, $g(x)$ y $h(x)$ tienen un cero en común.

¡¿¡¿¡¿Cómo funciona?!?!?!

Mi "llave" secreta

Yo sé algo que no sabe el público:

- $f(x)$, $g(x)$ y $h(x)$ tienen un cero en común.
  - $f(x) = (x-2)(x-3)$
  - $g(x) = 2(x-3)(x+4)$
  - $h(x) = -5(x+1)(x-3)$

¡¿¡¿¡¿Cómo funciona?!?!?!

Mi "llave" secreta

Yo sé algo que no sabe el público:

- $f(x)$, $g(x)$ y $h(x)$ tienen un cero en común.
  - $f(x) = (x-2)(x-3)$
  - $g(x) = 2(x-3)(x+4)$
  - $h(x) = -5(x+1)(x-3)$

$$f(3) = g(3) = h(3) = 0$$

Cómo desencripto el mensaje

Me llega el polinomio con el mensaje

$$652x^2 + 1891x - 9319$$

Cómo desencripto el mensaje

Me llega el polinomio con el mensaje

$$652x^2 + 1891x - 9319$$

No sé los valores de A, B y C (nadie los sabe aparte del que envió el mensaje).

Cómo desencripto el mensaje

Me llega el polinomio con el mensaje

$$652x^2 + 1891x - 9319$$

No sé los valores de A, B y C (nadie los sabe aparte del que envió el mensaje).

Pero sé que el polinomio es de la forma

$$Af(x) + Bg(x) + Ch(x) + \mathbf{m}$$

Cómo desencripto el mensaje

Me llega el polinomio con el mensaje

$$652x^2 + 1891x - 9319$$

No sé los valores de A, B y C (nadie los sabe aparte del que envió el mensaje).

Pero sé que el polinomio es de la forma

$$Af(x) + Bg(x) + Ch(x) + \mathbf{m}$$

Y puedo evaluar en $x = 3$:

$$Af(3) + Bg(3) + Ch(3) + \mathbf{m}$$

$$0 + 0 + 0 + \mathbf{m}$$

$$\mathbf{m}$$

¡Revisemos!

$$652x^2 + 1891x - 9319$$

$$652 \cdot 3^2 + 1891 \cdot 3 - 9319$$

$$5868 + 5673 - 9319$$

$$2222$$

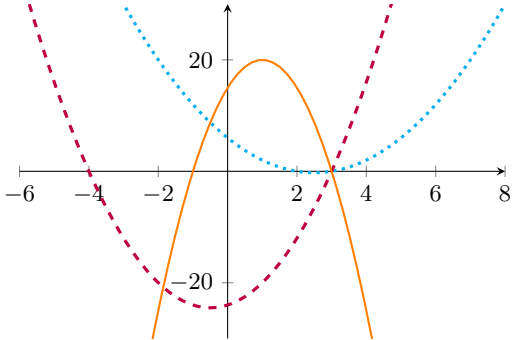
¡El mensaje original!

Quebrar este sistema para poder leer los mensajes encriptados:

Encontrar el cero común de tres polinomios cúbicos.

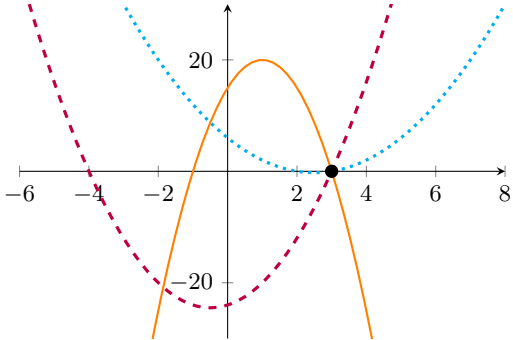
Quebrar este sistema para poder leer los mensajes encriptados:

Encontrar el cero común de tres polinomios cúbicos.



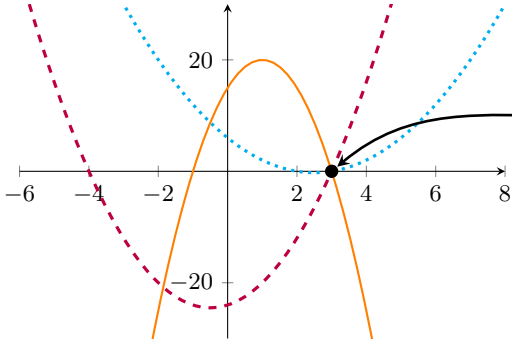
Quebrar este sistema para poder leer los mensajes encriptados:

Encontrar el cero común de tres polinomios cúbicos.



Quebrar este sistema para poder leer los mensajes encriptados:

Encontrar el cero común de tres polinomios cúbicos.



¡el cero en común!

privada

Este sistema en el mundo real: Polly Cracker

Polly Cracker

Cryptosystem 1.1 Abstract Polly Cracker.

1. *Key generation.* Alice selects randomly a point $\xi \in_{\mathrm{R}} \mathbb{F}^n$. Then she chooses an ideal $\mathfrak{a}$ in P so that ξ is a zero of $\mathfrak{a}$, that is, $f(\xi) = 0$ for all $f \in \mathfrak{a}$. Her public key is the ideal $\mathfrak{a}$ and her secret key the point ξ.

2. *Encryption.* In order to encrypt a message $m \in \mathbb{F}$ Bob chooses randomly a polynomial $h \in_{\mathrm{R}} \mathfrak{a}$ and computes the ciphertext by $c = h + m$.

3. *Decryption.* Alice evaluates c at ξ and gets $c(\xi) = h(\xi) + m = m$.

Security of the secret key arises from the difficulty of solving a system of algebraic equations. But, to get a real and practical cryptosystem we need much more ingredients, such as parameters, representation, and key-generation procedures. For instance, the ideal $\mathfrak{a}$ can be represented by a set of generators, as the kernel of a homomorphism or as an ideal of some variety. We shall discuss this in the second Chapter. Here we just focus on the abstract idea.

`https://d-nb.info/967582806/34`

No funciona bien sobre los reales, porque encontrar ceros comunes de polinomios no es tan complicado.

Se vuelve complicado cuando:

- uno usa varias variables (n-dimensiones)
- uno usa campos de números más complejos.

Estos sistemas en la realidad

RSA: de los más antiguos y más usados en internet

Operation [edit]

The RSA algorithm involves four steps: key generation, key distribution, encryption, and decryption.

A basic principle behind RSA is the observation that it is practical to find three very large positive integers e, d, and n, such that with modular exponentiation for all integers m (with $0 \leq m < n$):

$$(m^e)^d \equiv m \pmod{n}$$

and that knowing e and n, it can be extremely difficult to find d. Here the symbol ≡ denotes modular congruence: i.e. both $(m^e)^d$ and m have the same remainder when divided by n.

In addition, for some operations it is convenient that the order of the two exponentiations can be changed: the previous relation also implies

$$(m^d)^e \equiv m \pmod{n}.$$

RSA involves a *public key* and a *private key*. The public key can be known by everyone and is used for encrypting messages. The intention is that messages encrypted with the public key can only be decrypted in a reasonable amount of time by using the private key. The public key is represented by the integers n and e, and the private key by the integer d (although n is also used during the decryption process, so it might be considered to be a part of the private key too). m represents the message (previously prepared with a certain technique explained below).

`https://en.wikipedia.org/wiki/RSA_(cryptosystem)`

RSA con "raices n-ésimas" que no es fácil calcular.

Estos sistemas en la realidad

RSA: de los más antiguos y más usados en internet

Operation [edit]

The RSA algorithm involves four steps: key generation, key distribution, encryption, and decryption.

A basic principle behind RSA is the observation that it is practical to find three very large positive integers e, d, and n, such that with modular exponentiation for all integers m (with $0 \leq m < n$):

d es la raíz e-ésima ^(1/e)

$$(m^e)^d \equiv m \pmod{n}$$

... y es difícil de calcular

and that knowing e and n, it can be extremely difficult to find d. Here the symbol ≡ denotes modular congruence: i.e. both $(m^e)^d$ and m have the same remainder when divided by n.

`https://en.wikipedia.org/wiki/RSA_(cryptosystem)`

RSA con "raices n-ésimas" que no es fácil calcular.

Cierre

Cierre

Poder quebrar estos sistemas se reduce a saber:

- Calcular logaritmos
- Calcular raíces
- Encontrar ecuaciones de polinomios que pasan por unos puntos
- Encontrar ceros de polinomios
- Reescribir ecuaciones de distintas formas equivalentes
- ...

Cierre

Poder quebrar estos sistemas se reduce a saber:

- Calcular logaritmos
- Calcular raíces
- Encontrar ecuaciones de polinomios que pasan por unos puntos
- Encontrar ceros de polinomios
- Reescribir ecuaciones de distintas formas equivalentes
- ...

Funcionan porque con sistemas de números distintos, elegidos estratégicamente, ¡no es NADA fácil hacer lo que uno aprende a hacer en la escuela!

Cierre

Criptografía:

- Ideas simples, accesibles, relevantes.
- Mucho que se puede hacer con los estudiantes:
  - Usar sistemas
  - Diseñar sistemas
  - Jugar a quebrar sistemas
- Todo esto involucra ideas de álgebra que a menudo es difícil motivar.

Créditos

- Aaron Wootton, University of Portland
- Catherine Murphy, University of Portsmouth

Artículo 2024

Bringing Cryptology into the Secondary Education Classroom
Proceedings of the 7th International Conference on Historical Cryptology
https://doi.org/10.58009/aere-perennius0109

¡Gracias!

Contacto

Enrique Acosta Jaramillo

enriqueacostajaramillo@gmail.com

enriqueacostajaramillo@protonmail.com

www.grupolema.org