Nuevas aventuras de Alicia en el país de la criptografía

Francisco Rodríguez-Henríquez
Cryptography Research Center of the Technology Innovation Institute

INCACrypto 2023
Universidad de las Fuerzas Armadas ESPE,
domingo primero de octubre de 2023

Breve contexto criptográfico y de seguridad informática

Tres leyes de la seguridad informática

Figure: Primera ley: Los sistemas absolutamente seguros no existen

Tres leyes de la seguridad informática

Figure: Segunda ley: Disminuir las vulnerabilidades de un sistema a la mitad implica duplicar los costos de seguridad

Tres leyes de la seguridad informática

Figure: Tercera ley: Típicamente la criptografía no es vulnerada sino más bien brincada

De la importancia del sigilo en la criptografía

- En criptografía y en seguridad informática los secretos arduamente obtenidos no suelen revelarse

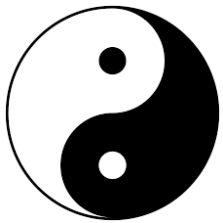
De la importancia del sigilo en la criptografía

- En criptografía y en seguridad informática los secretos arduamente obtenidos no suelen revelarse
- Innumerables ejemplos en que el crédito de vulnerar un criptosistema no se le otorga a los atacantes sino muchos años después [y a veces nunca]

De la importancia del sigilo en la criptografía

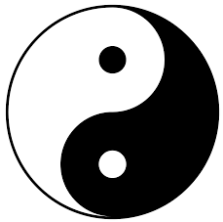
- En criptografía y en seguridad informática los secretos arduamente obtenidos no suelen revelarse
- Innumerables ejemplos en que el crédito de vulnerar un criptosistema no se le otorga a los atacantes sino muchos años después [y a veces nunca]
- Ejemplo paradigmático: Alan Turing y el éxito de su equipo para "romper" la máquina de cifrado Enigma durante la segunda guerra mundial

Glosario básico



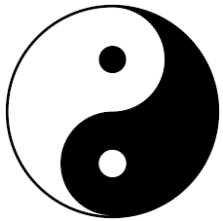
- Criptografía: Diseño de sistemas y esquemas para realizar comunicaciones confiables sobre canales inseguros.

Glosario básico



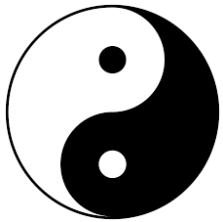
- Criptografía: Diseño de sistemas y esquemas para realizar comunicaciones confiables sobre canales inseguros.
- Criptoanálisis: Disciplina que estudia cómo romper esquemas criptográficos.

Glosario básico



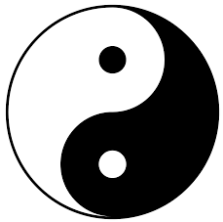
- Criptografía: Diseño de sistemas y esquemas para realizar comunicaciones confiables sobre canales inseguros.
- Criptoanálisis: Disciplina que estudia cómo romper esquemas criptográficos.
- Texto en claro: mensaje que desea transmitirse de manera segura.

Glosario básico



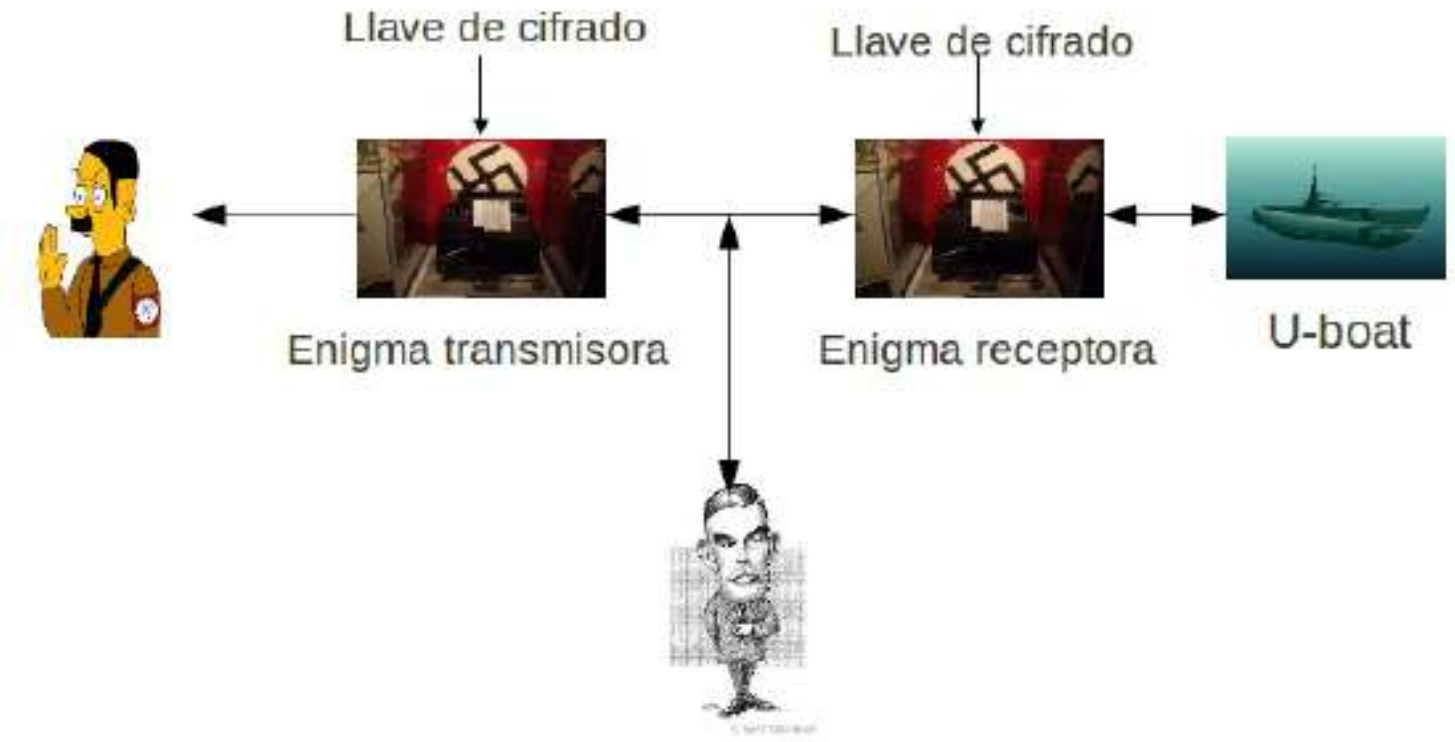
- Criptografía: Diseño de sistemas y esquemas para realizar comunicaciones confiables sobre canales inseguros.
- Criptoanálisis: Disciplina que estudia cómo romper esquemas criptográficos.
- Texto en claro: mensaje que desea transmitirse de manera segura.
- cifra: mensaje que resulta después de haber cifrado el texto en claro.

Glosario básico



- Criptografía: Diseño de sistemas y esquemas para realizar comunicaciones confiables sobre canales inseguros.
- Criptoanálisis: Disciplina que estudia cómo romper esquemas criptográficos.
- Texto en claro: mensaje que desea transmitirse de manera segura.
- cifra: mensaje que resulta después de haber cifrado el texto en claro.
- llave o clave secreta: información secreta que permite cifrar/descifrar documentos.

Modelo de seguridad de Enigma



Modelo de seguridad de Enigma

Posibles objetivos de Alan Turing:

1. Leer el mensaje original

Modelo de seguridad de Enigma

Posibles objetivos de Alan Turing:

1. Leer el mensaje original
2. Obtener la llave secreta de Alicia.

Modelo de seguridad de Enigma

Posibles objetivos de Alan Turing:

1. Leer el mensaje original
2. Obtener la llave secreta de Alicia.
3. Modificar el contenido del mensaje original.

Modelo de seguridad de Enigma

Posibles objetivos de Alan Turing:

1. Leer el mensaje original
2. Obtener la llave secreta de Alicia.
3. Modificar el contenido del mensaje original.
4. Usurpar la identidad de Alicia

Principio de Kerckhkoff

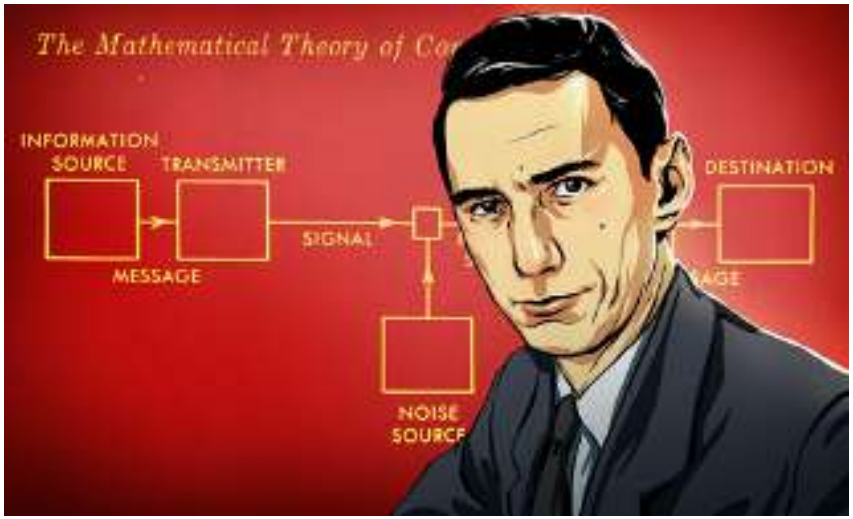
Fue presentado famosamente por el criptógrafo francés Auguste Kerckhoffs a finales del siglo XIX en París:
"*La sécurité repose sur le secret de la clé, et non sur le secret de l'algorithme.*"
Se parte de la premisa que el oponente **conoce** el algoritmo criptográfico utilizado. Por lo tanto, la seguridad del sistema debe descansar en:

Principio de Kerckhkoff

Fue presentado famosamente por el criptógrafo francés Auguste Kerckhoffs a finales del siglo XIX en París:
"*La sécurité repose sur le secret de la clé, et non sur le secret de l'algorithme.*"
Se parte de la premisa que el oponente **conoce** el algoritmo criptográfico utilizado. Por lo tanto, la seguridad del sistema debe descansar en:

- La calidad (fortaleza) del algoritmo
- El tamaño del espacio de la llave (tamaño en bits de la llave)

Parteaguas en el siglo XX: Claude Shannon, alquimista



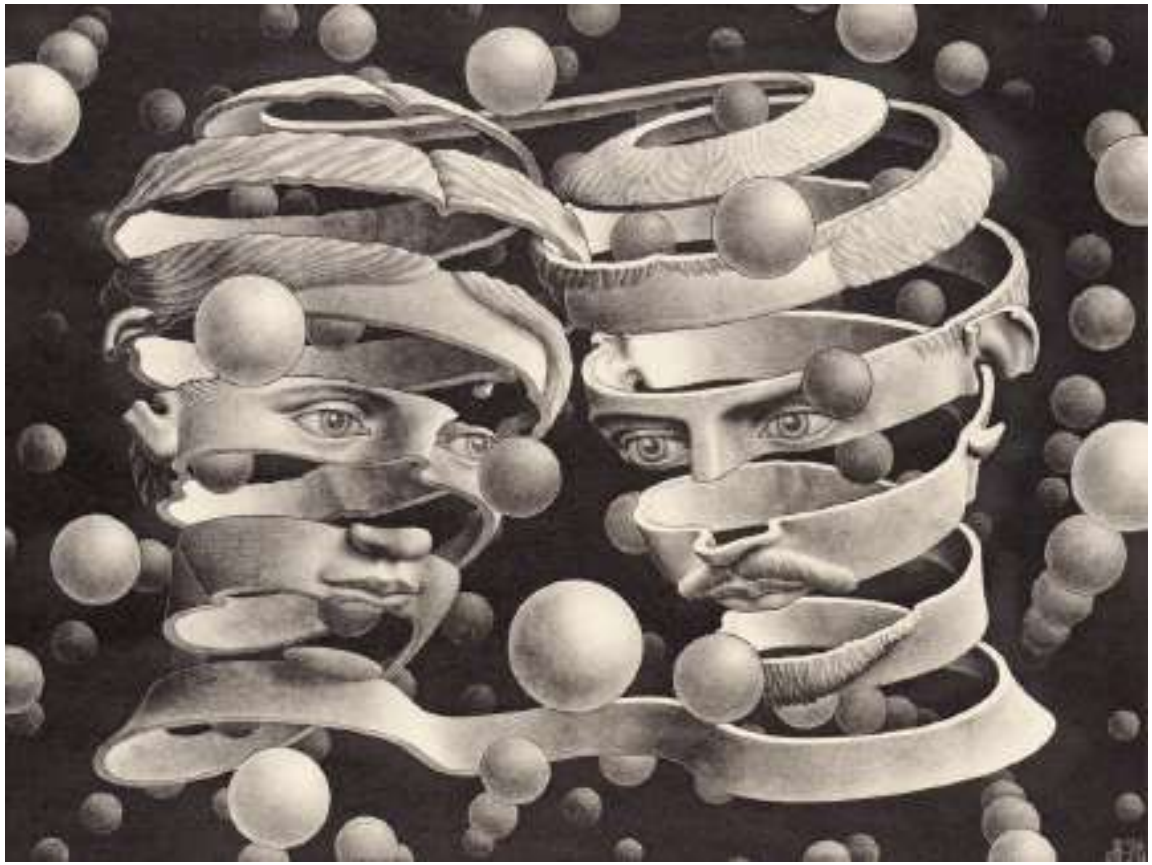
1. En 1948 Shannon publicó el artículo: "A Mathematical Theory of Communication", donde introdujo el concepto de la entropía de la información y con ello inventó el fascinante campo de la teoría de la información con su concepto de la entropía informática.
2. Al año siguiente publicó el artículo: "Communication Theory of Secrecy Systems", con lo cual la criptografía pasó de ser un oficio a ser una disciplina científica. En ese artículo, Shannon demostró la seguridad perfecta del cripto-esquema "One-time pad" inventado por Vernam y que había sido usado durante la primera guerra mundial.

Plegaria del Codificador teórico

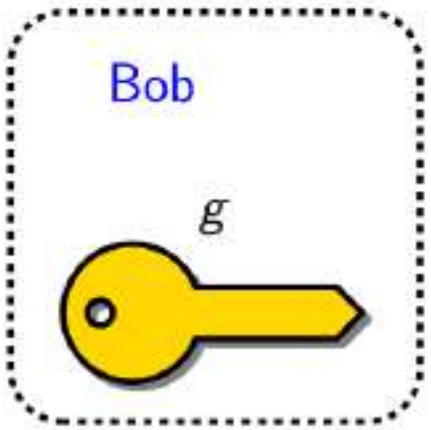
‘*Juro por Galois que seré leal a las nobles tradiciones de la teoría de códigos, que hablaré de ella en el secreto lenguaje sólo conocido por los contados iniciados, y que celosamente vigilaré la sagrada teoría de aquellos que quisieran profanarla para usarla en aplicaciones mundanas*”

J. L. Massey, circa 1975

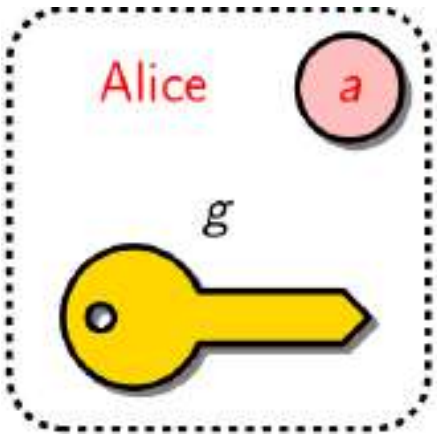
Problema de diseño: ¿Cómo establecer un secreto compartido?

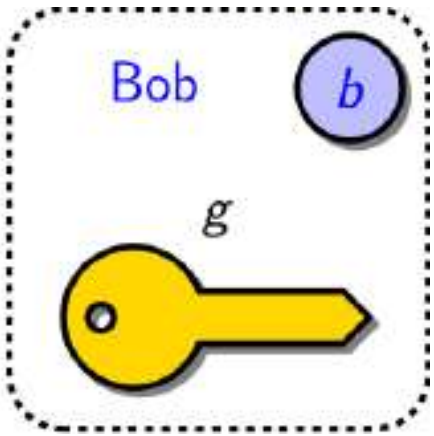


Problema de diseño: ¿Cómo establecer un secreto compartido?. Solución: Protocolo Diffie-Hellman 1976

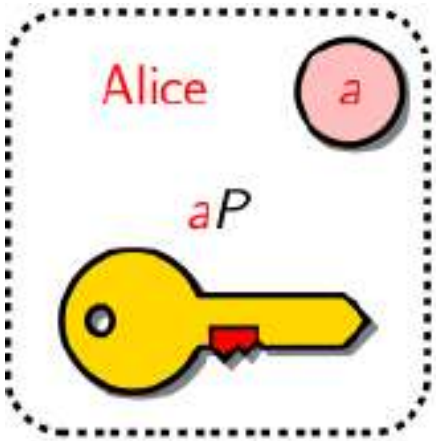


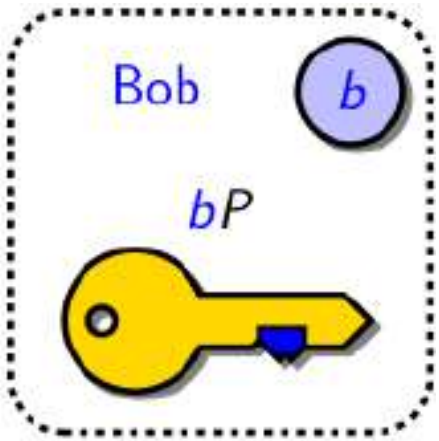
Problema de diseño: ¿Cómo establecer un secreto compartido?. Solución: Protocolo Diffie-Hellman 1976

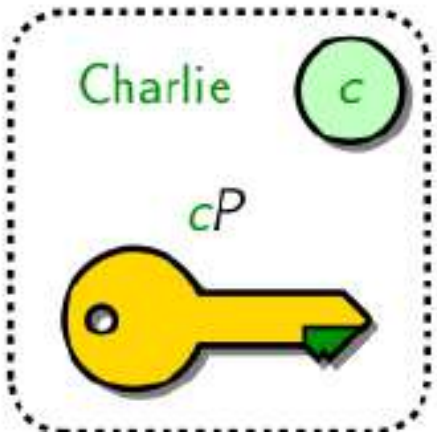




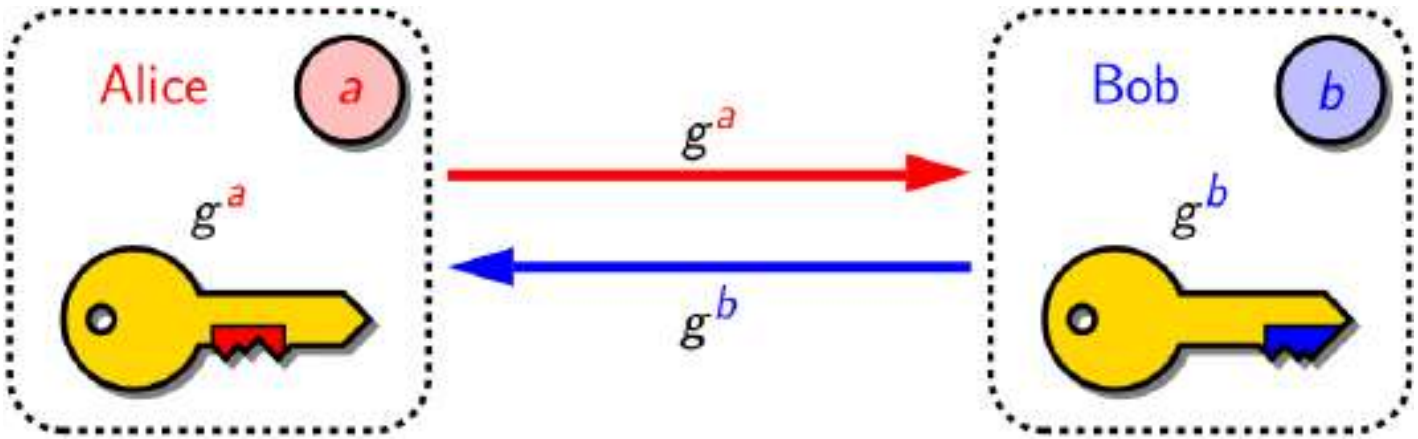
Problema de diseño: ¿Cómo establecer un secreto compartido?. Solución: Protocolo Diffie-Hellman 1976



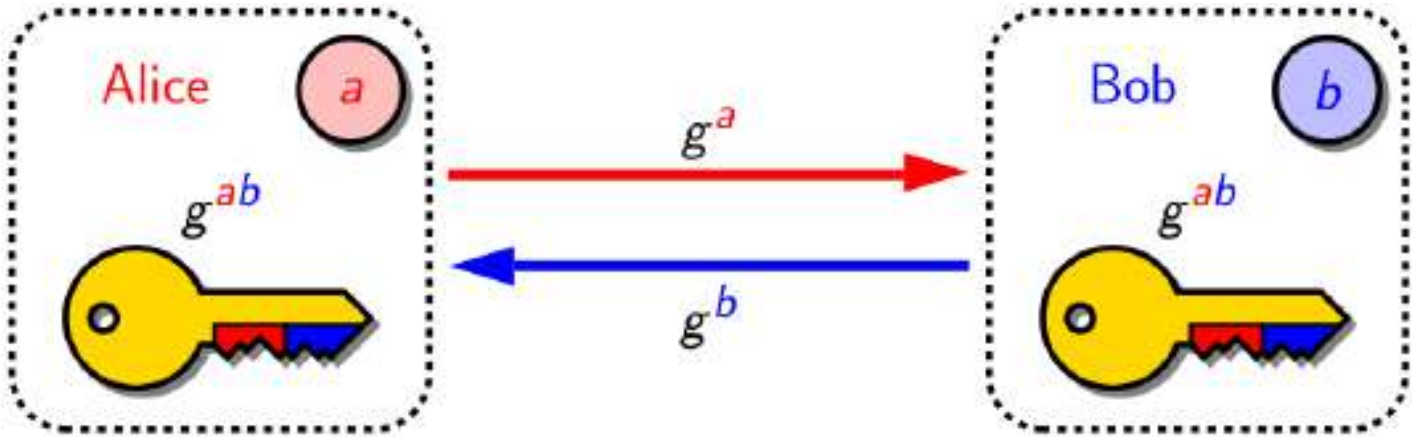




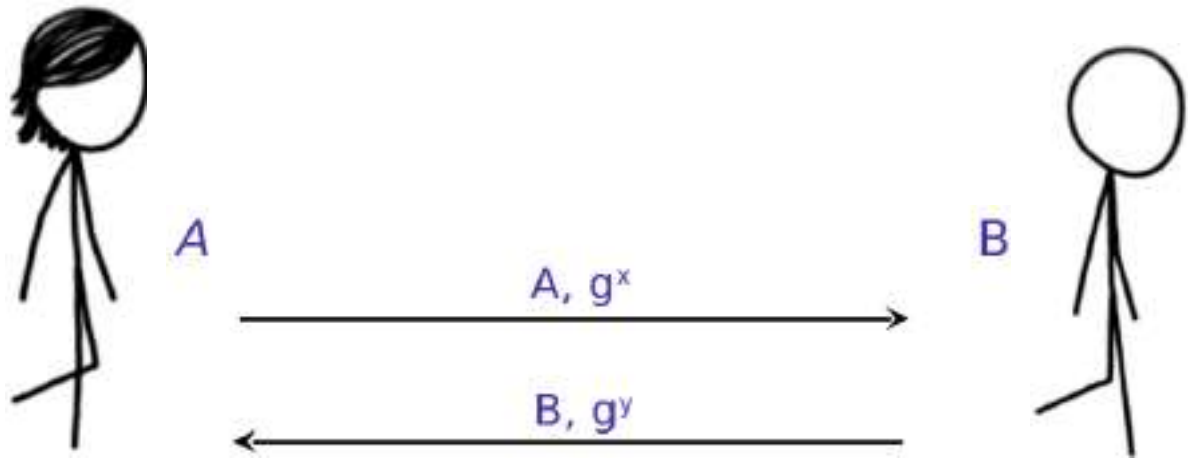
Problema de diseño: ¿Cómo establecer un secreto compartido?. Solución: Protocolo Diffie-Hellman 1976



Problema de diseño: ¿Cómo establecer un secreto compartido?. Solución: Protocolo Diffie-Hellman 1976



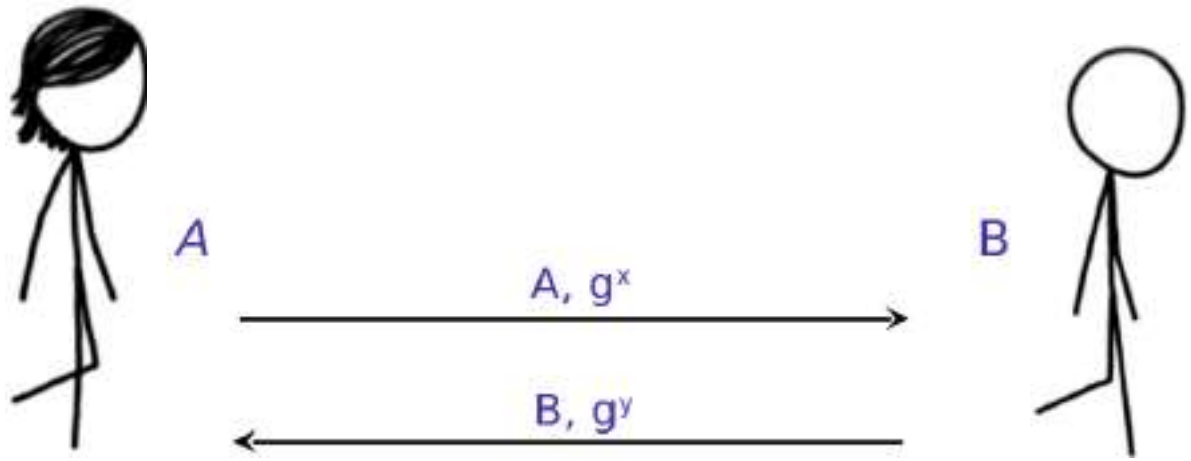
Problema de diseño: ¿Cómo establecer un secreto compartido?. Solución: Protocolo Diffie-Hellman 1976



- Tanto Alicia como Beto acuerdan trabajar en el grupo $\mathbb{Z}_p$, con p un número primo impar grande, y escogen un generador $g \in \mathbb{Z}_p$ (i.e., $Ord(g) = p - 1$).
- Alicia y Beto escogen $x \in \mathbb{Z}_p$ e $y \in \mathbb{Z}_p$, respectivamente
- Alicia y Beto calculan un secreto compartido mediante la exponenciación:

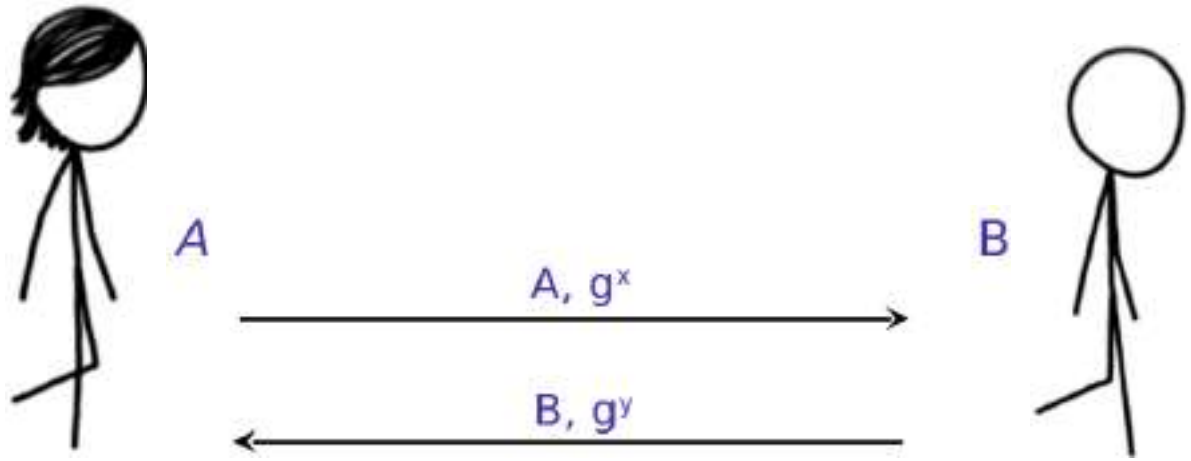
$$K = (g^x)^y = (g^y)^x$$

Problema de diseño: ¿Cómo establecer un secreto compartido?. Solución: Protocolo Diffie-Hellman 1976



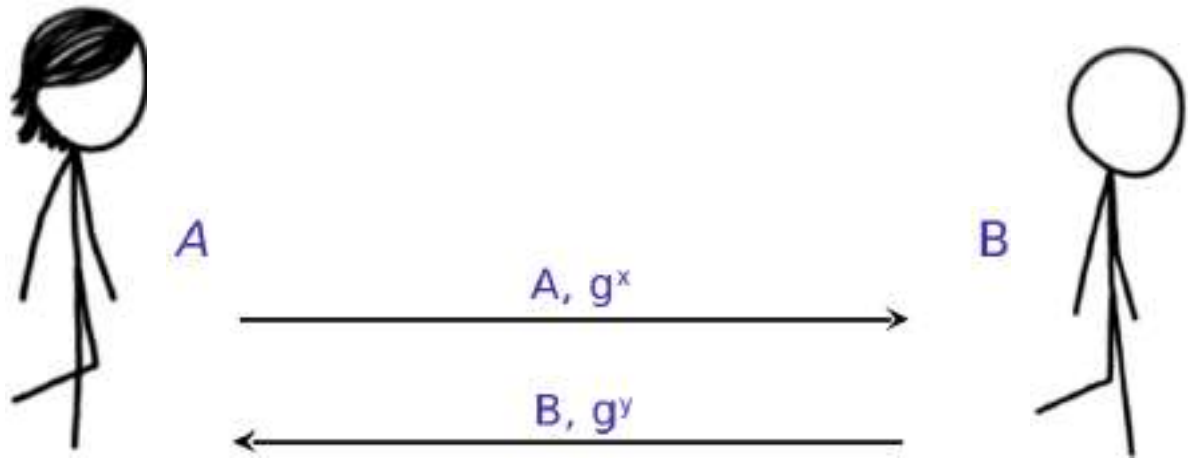
La seguridad del protocolo descansa en la intratabilidad del problema del logaritmo discreto: Dado un primo p y un generador $g, h \in [1, p-1]$, encuentre un entero x (si es que existe) tal que, $g^x \equiv h \bmod p$.

Problema de diseño: ¿Cómo establecer un secreto compartido?. Solución: Protocolo Diffie-Hellman 1976

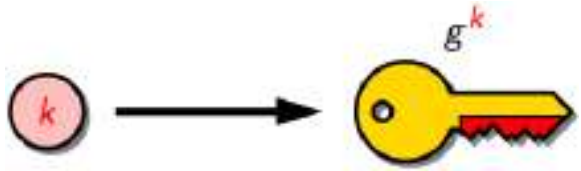


La seguridad del protocolo descansa en la intratabilidad del problema del logaritmo discreto: Dado un primo p y un generador $g, h \in [1, p-1]$, encuentre un entero x (si es que existe) tal que, $g^x \equiv h \bmod p$.

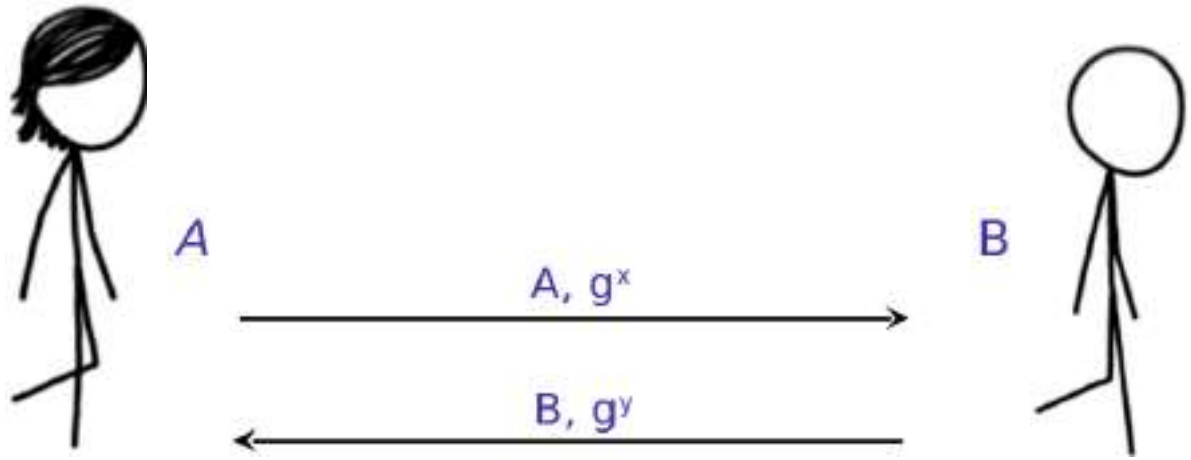
Problema de diseño: ¿Cómo establecer un secreto compartido?. Solución: Protocolo Diffie-Hellman 1976



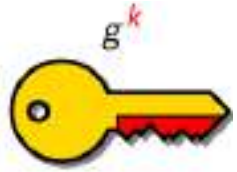
La seguridad del protocolo descansa en la intratabilidad del problema del logaritmo discreto: Dado un primo p y un generador $g, h \in [1, p-1]$, encuentre un entero x (si es que existe) tal que, $g^x \equiv h \bmod p$.



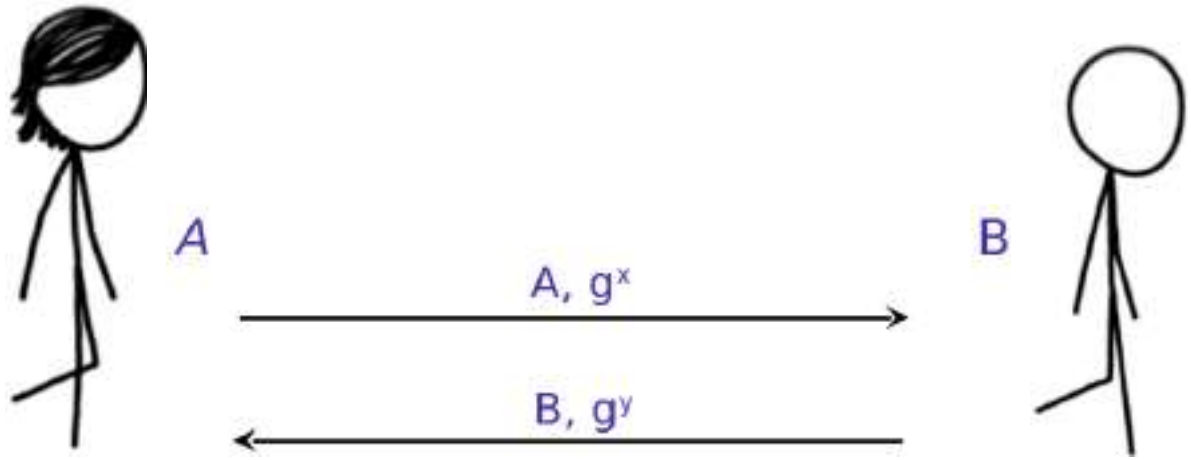
Problema de diseño: ¿Cómo establecer un secreto compartido?. Solución: Protocolo Diffie-Hellman 1976



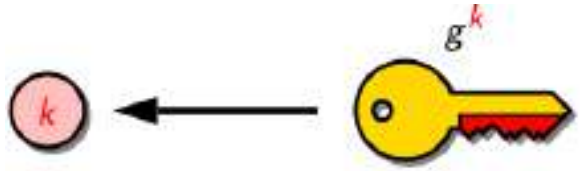
La seguridad del protocolo descansa en la intratabilidad del problema del logaritmo discreto: Dado un primo p y un generador $g, h \in [1, p-1]$, encuentre un entero x (si es que existe) tal que, $g^x \equiv h \bmod p$.



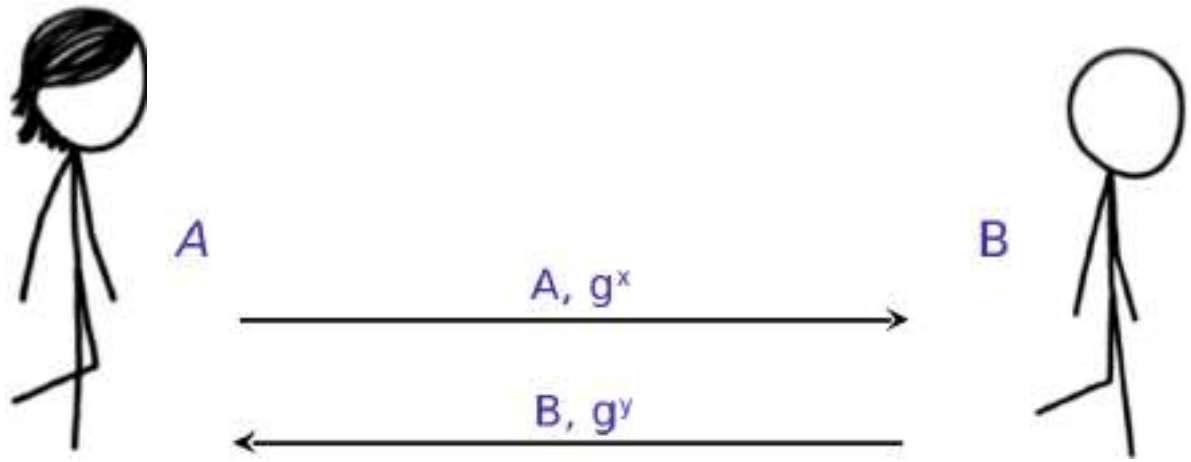
Problema de diseño: ¿Cómo establecer un secreto compartido?. Solución: Protocolo Diffie-Hellman 1976



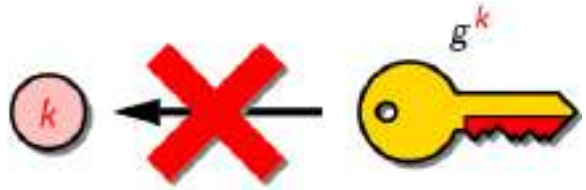
La seguridad del protocolo descansa en la intratabilidad del problema del logaritmo discreto: Dado un primo p y un generador $g, h \in [1, p-1]$, encuentre un entero x (si es que existe) tal que, $g^x \equiv h \bmod p$.



Problema de diseño: ¿Cómo establecer un secreto compartido?. Solución: Protocolo Diffie-Hellman 1976

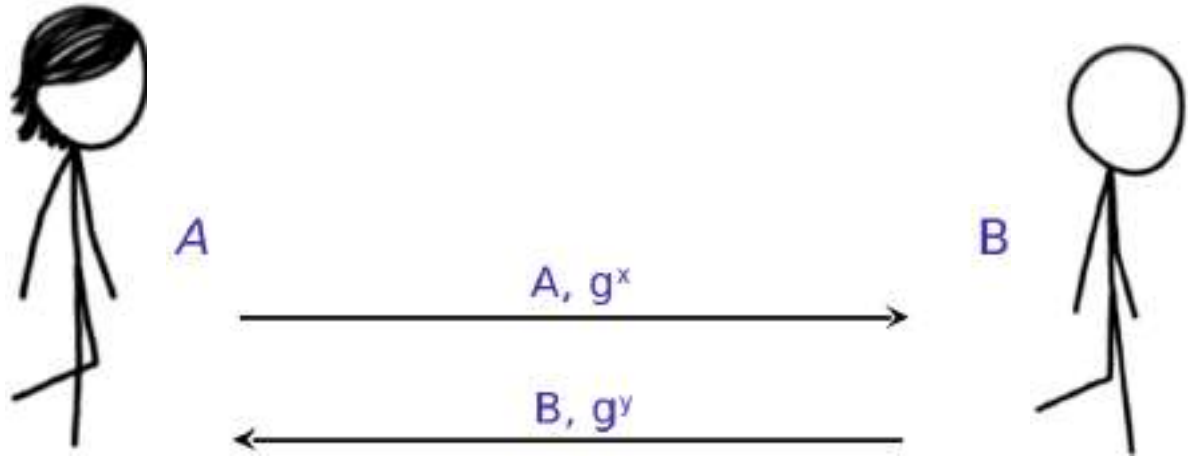


La seguridad del protocolo descansa en la intratabilidad del problema del logaritmo discreto: Dado un primo p y un generador $g, h \in [1, p-1]$, encuentre un entero x (si es que existe) tal que, $g^x \equiv h \bmod p$.



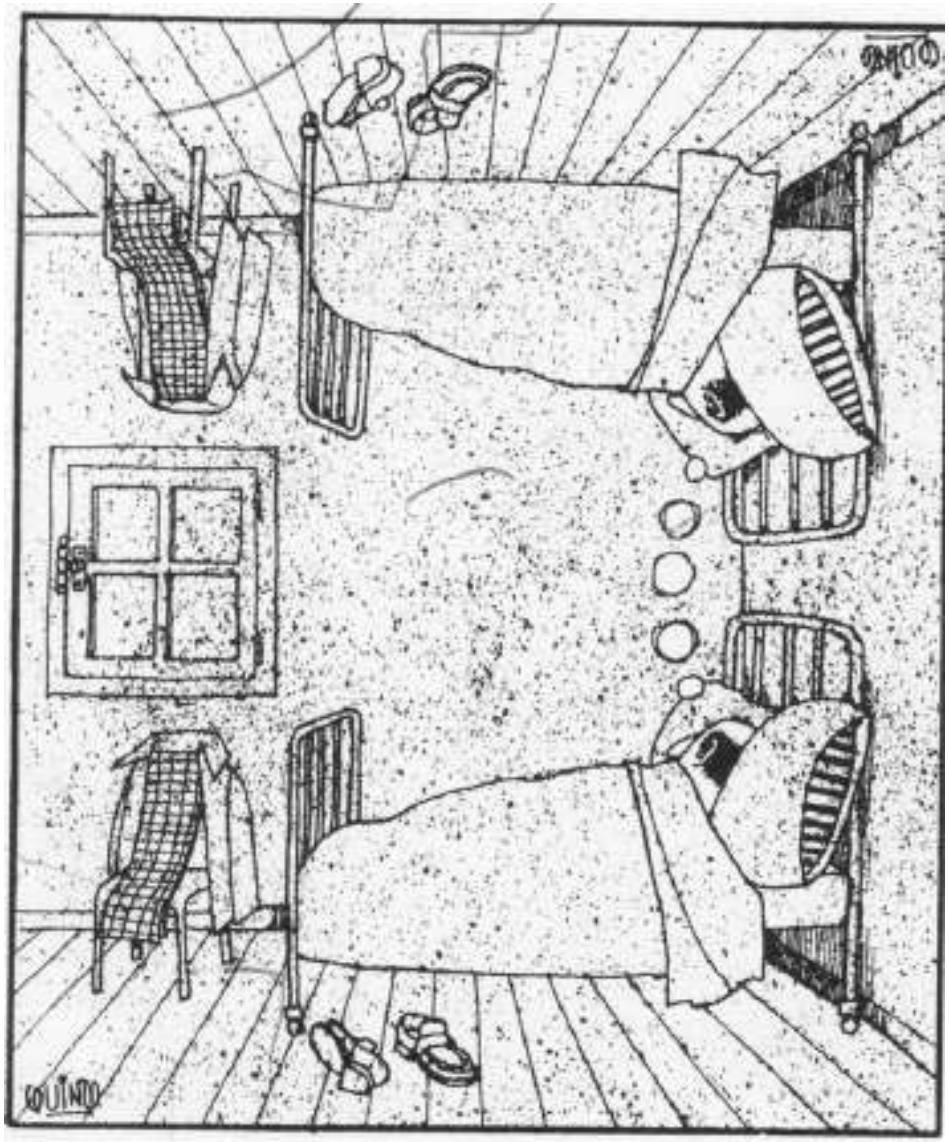
Problema de diseño: ¿Cómo establecer un secreto compartido?. Solución: Protocolo Diffie-Hellman 1976

Problema de diseño: ¿Cómo establecer un secreto compartido?. Solución: Protocolo Diffie-Hellman 1976



- Diffie y Hellman publicaron su protocolo en el artículo seminal: Diffie, W.; Hellman, M. (1976). "New directions in cryptography". IEEE Transactions on Information Theory. 22 (6): 644–654."
- Los profesores Diffie y Hellman recibieron el premio Turing de computación en 2015
- "New directions in cryptography" es un artículo parteaguas en la disciplina. Desde su publicación en 1976 la comunidad criptográfica ha estado fascinada con el horizonte que abrió este trabajo. En esta presentación revisaremos cuatro versiones diferentes de este protocolo [¡!]

Primitivas y bloques básicos fundamentales en criptografía moderna



Primitivas y bloques básicos fundamentales en criptografía moderna

- Primitivas:
  - Cifrado/descifrado de documentos digitales [típicamente se resuelve utilizando criptografía de llave secreta]

Primitivas y bloques básicos fundamentales en criptografía moderna

- Primitivas:
  - Cifrado/descifrado de documentos digitales [típicamente se resuelve utilizando criptografía de llave secreta]
  - Establecimiento de un secreto compartido entre dos entidades [se resuelve invocando al protocolo Diffie-Hellman]

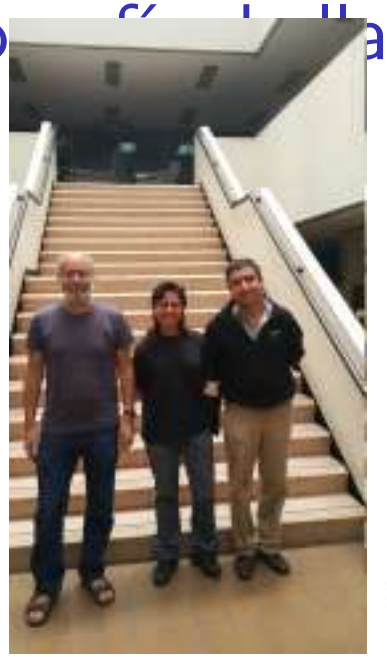
Primitivas y bloques básicos fundamentales en criptografía moderna

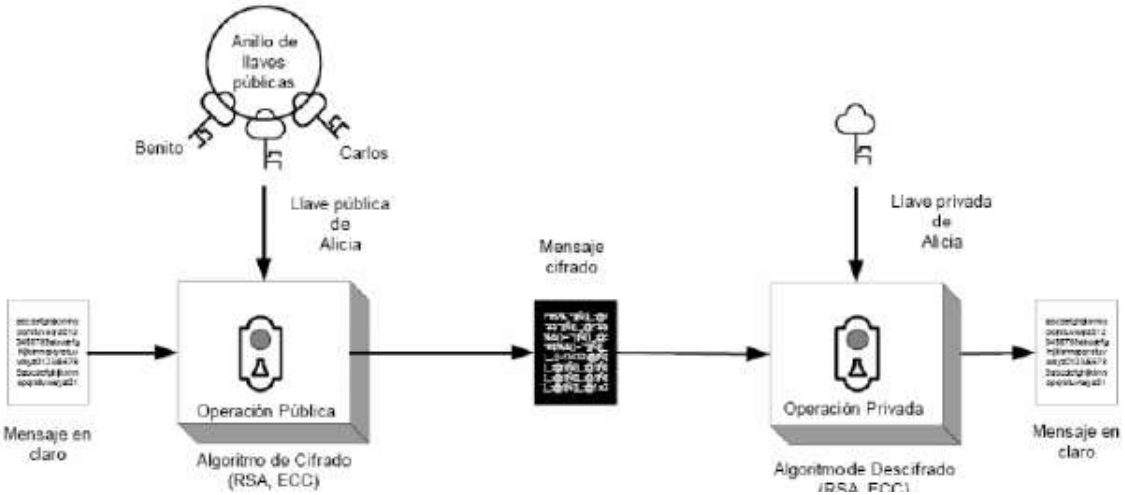
- Primitivas:
  - Cifrado/descifrado de documentos digitales [típicamente se resuelve utilizando criptografía de llave secreta]
  - Establecimiento de un secreto compartido entre dos entidades [se resuelve invocando al protocolo Diffie-Hellman]
  - Firma/verificación de documentos digitales [típicamente se resuelve utilizando criptografía de llave pública]

Primitivas y bloques básicos fundamentales en criptografía moderna

- Primitivas:
  - Cifrado/descifrado de documentos digitales [típicamente se resuelve utilizando criptografía de llave secreta]
  - Establecimiento de un secreto compartido entre dos entidades [se resuelve invocando al protocolo Diffie-Hellman]
  - Firma/verificación de documentos digitales [típicamente se resuelve utilizando criptografía de llave pública]
- Bloques básicos:
  - Cifradores por bloque y cifradores por flujo de datos
  - funciones picadillo
  - cripto-sistemas de llave pública
  - ...

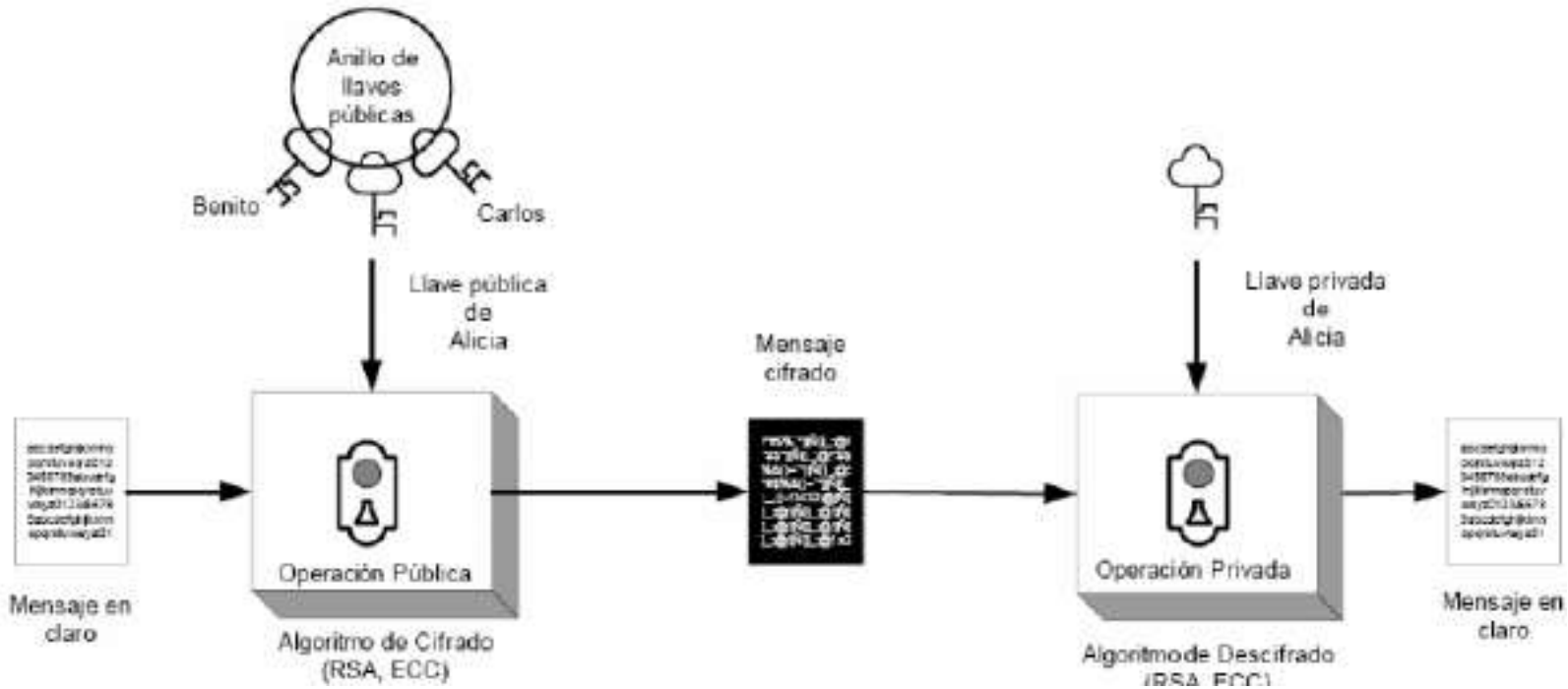
Cripto[illegible]ave pública





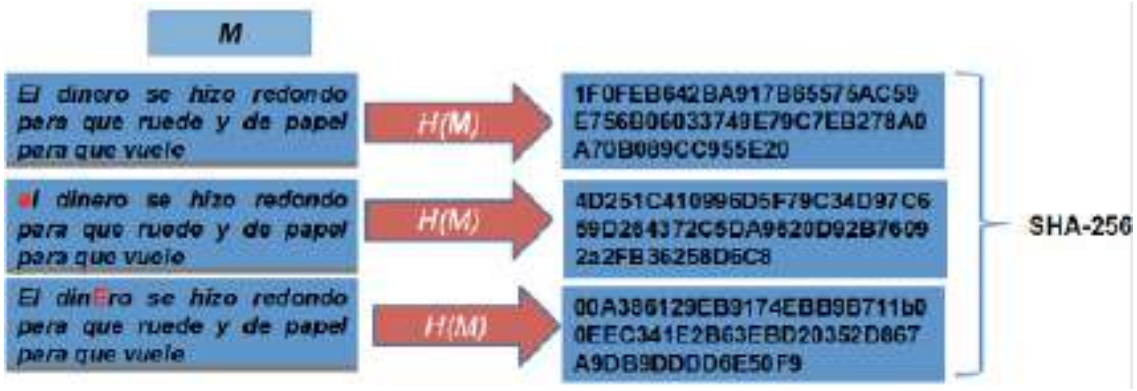
- Conceptualmente, fue inventada en 1976 por Diffie y Hellman.

Criptografía de llave pública

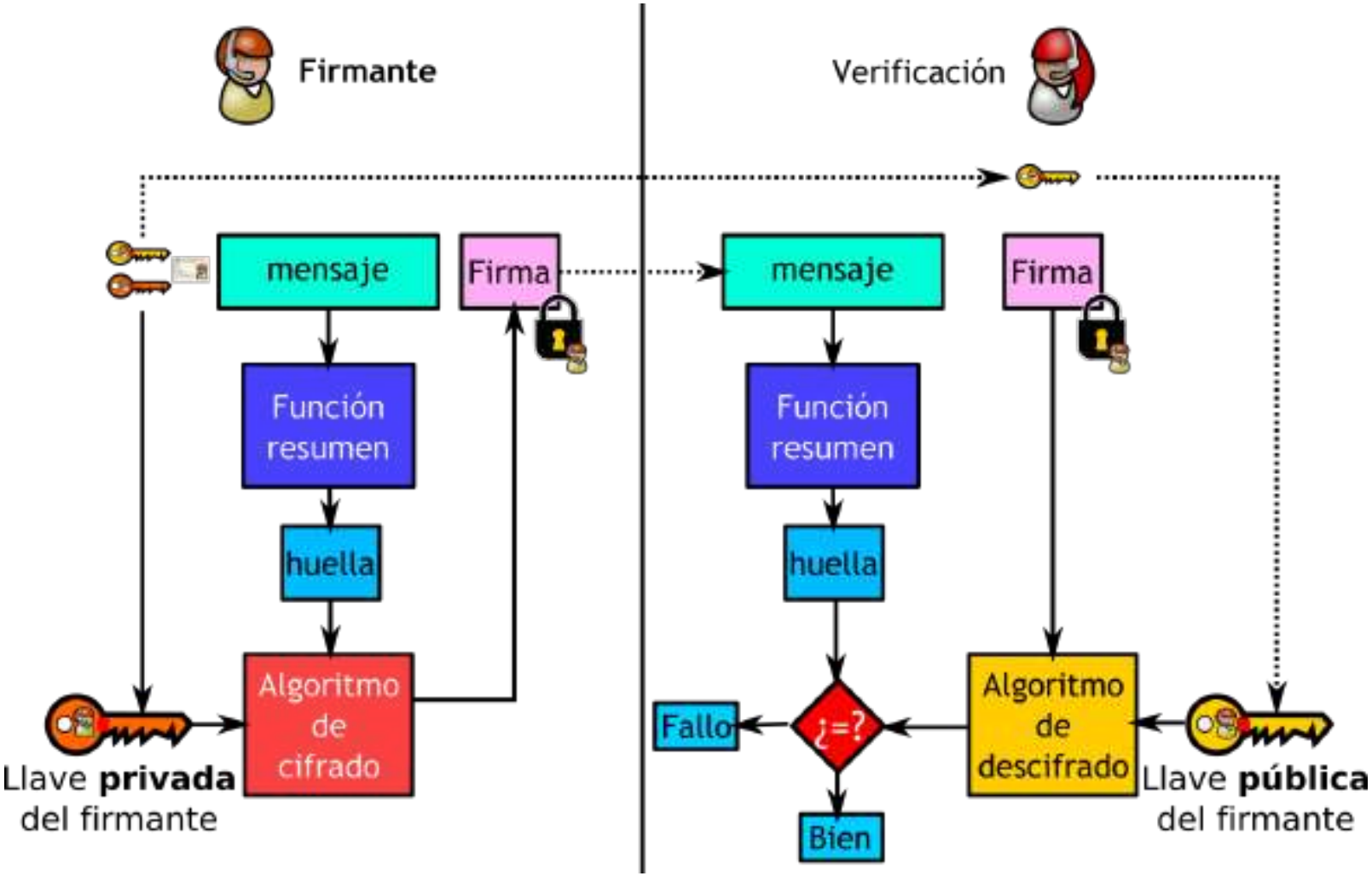


Funciones picadillo

Funciones picadillo



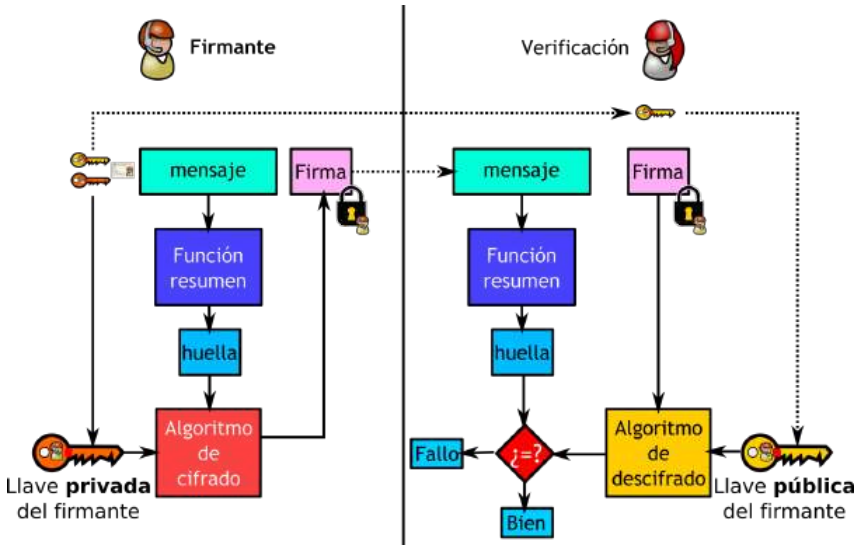
Firma digital



Firma digital

En resumen, a diferencia de la firma autógrafa tradicional donde sólo se verifica la autenticidad del signatario, para un esquema de firma digital el proceso de verificación regresa un valor verdadero si y sólo si se satisfacen las siguientes dos condiciones:

1. Autenticidad del signatario
2. Autenticidad del documento



Problemas matemáticos computacionalmente difíciles

- Problema de factorización entera: Dado un entero $N = p \cdot q$ encuentre sus factores primos p y q. Por ejemplo: ¿Cuál es la factorización de 2023?

Problemas matemáticos computacionalmente difíciles

- Problema de factorización entera: Dado un entero $N = p \cdot q$ encuentre sus factores primos p y q. Por ejemplo: ¿Cuál es la factorización de 2023?
  Respuesta: $2023 = 7 \cdot 17^2$

Problemas matemáticos computacionalmente difíciles

- Problema de factorización entera: Dado un entero $N = p \cdot q$ encuentre sus factores primos p y q. Por ejemplo: ¿Cuál es la factorización de 2023?
  Respuesta: $2023 = 7 \cdot 17^2$
- Problema del logaritmo discreto: Dado un número primo p y $g, h \in [1, p-1]$, encuentre un entero x (en caso de que exista) tal que: $g^x \equiv h \bmod p$.
  Por ejemplo: ¿Cuánto vale x tal que: $2^x \equiv 304 \bmod 419$?]

Problemas matemáticos computacionalmente difíciles

- Problema de factorización entera: Dado un entero $N = p \cdot q$ encuentre sus factores primos p y q. Por ejemplo: ¿Cuál es la factorización de 2023?
  Respuesta: $2023 = 7 \cdot 17^2$
- Problema del logaritmo discreto: Dado un número primo p y $g, h \in [1, p-1]$, encuentre un entero x (en caso de que exista) tal que: $g^x \equiv h \bmod p$.
  Por ejemplo: ¿Cuánto vale x tal que: $2^x \equiv 304 \bmod 419$?]
  Respuesta: $2^{343} \equiv 304 \bmod 419$.

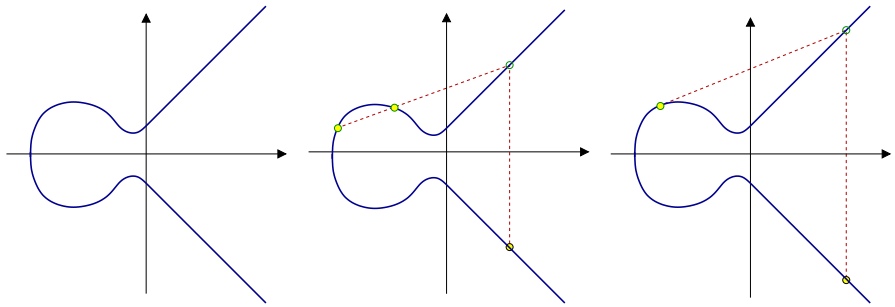
Problemas matemáticos computacionalmente difíciles

- Problema de factorización entera: Dado un entero $N = p \cdot q$ encuentre sus factores primos p y q. Por ejemplo: ¿Cuál es la factorización de 2023?
  Respuesta: $2023 = 7 \cdot 17^2$
- Problema del logaritmo discreto: Dado un número primo p y $g, h \in [1, p-1]$, encuentre un entero x (en caso de que exista) tal que: $g^x \equiv h \bmod p$.
  Por ejemplo: ¿Cuánto vale x tal que: $2^x \equiv 304 \bmod 419$?]
  Respuesta: $2^{343} \equiv 304 \bmod 419$.
- Problema del logaritmo discreto para curvas elípticas: Dada una curva elíptica definida sobre $E/\mathbb{F}_q$ y $P, Q \in E(\mathbb{F}_{q^k})$, encuentre un entero x (en caso de que exista) tal que: $xP = Q$

Criptografía basada en curvas elípticas

- El uso de curvas elípticas en criptografía fue propuesto independientemente por los profesores Victor Miller y Neal Koblitz en 1985.
- Tomó más de dos décadas para que este tipo de criptografía fuera aceptada ampliamente y desbancara a RSA en aplicaciones comerciales
- Actualmente la criptografía de curvas elípticas es utilizada masivamente en aplicaciones cotidianas

Criptografía basada en curvas elípticas

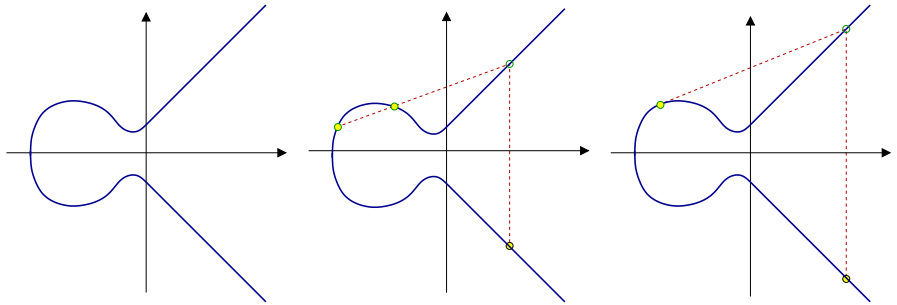


Una curva elíptica está definida por el conjunto de puntos afines $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, donde p es un primo impar grande, que satisface la ecuación corta de Weierstrass,

$$E : y^2 = x^3 + ax + b,$$

junto con un punto al infinito denotado por $\mathcal{O}$. El conjunto de puntos que satisfacen la anterior ecuación forman un grupo abeliano denotado por $E(\mathbb{F}_p)$ con orden $\#E(\mathbb{F}_p) = h \cdot r$, donde r es un primo grande y el cofactor h es un entero pequeño.

Criptografía basada en curvas elípticas

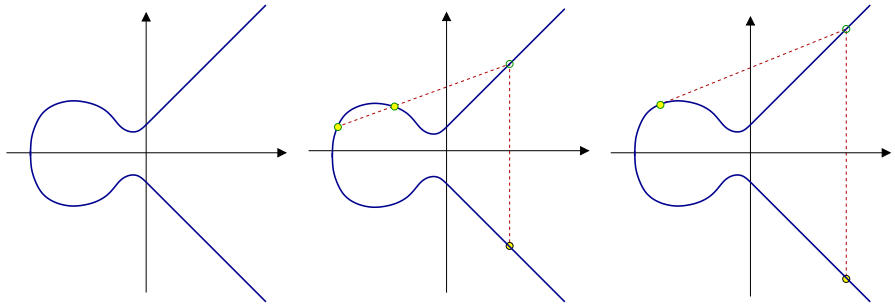


Una curva elíptica está definida por el conjunto de puntos afines $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, donde p es un primo impar grande, que satisface la ecuación corta de Weierstrass,

$$E : y^2 = x^3 + ax + b,$$

junto con un punto al infinito denotado por $\mathcal{O}$. El conjunto de puntos que satisfacen la anterior ecuación forman un grupo abeliano denotado por $E(\mathbb{F}_p)$ con orden $\#E(\mathbb{F}_p) = h \cdot r$, donde r es un primo grande y el cofactor h es un entero pequeño.

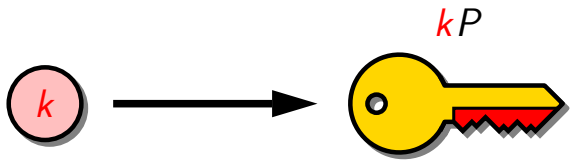
Criptografía basada en curvas elípticas



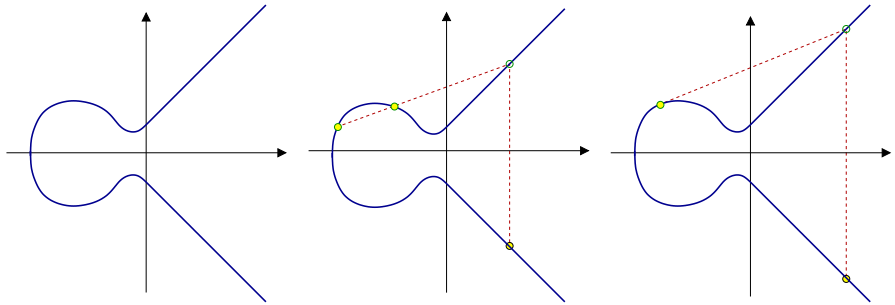
Una curva elíptica está definida por el conjunto de puntos afines $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, donde p es un primo impar grande, que satisface la ecuación corta de Weierstrass,

$$E : y^2 = x^3 + ax + b,$$

junto con un punto al infinito denotado por $\mathcal{O}$. El conjunto de puntos que satisfacen la anterior ecuación forman un grupo abeliano denotado por $E(\mathbb{F}_p)$ con orden $\#E(\mathbb{F}_p) = h \cdot r$, donde r es un primo grande y el cofactor h es un entero pequeño.



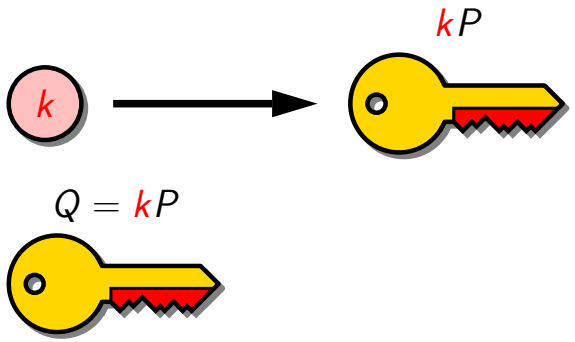
Criptografía basada en curvas elípticas



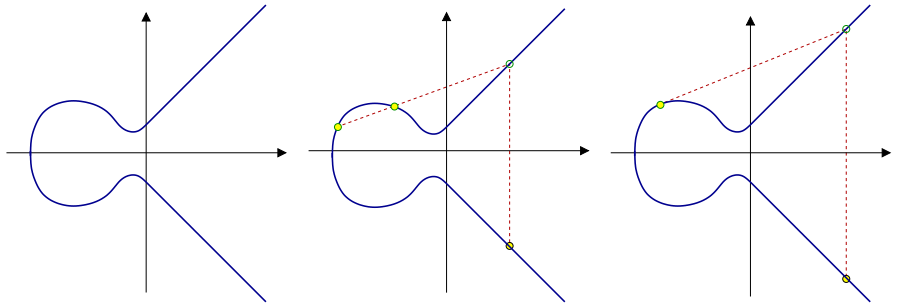
Una curva elíptica está definida por el conjunto de puntos afines $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, donde p es un primo impar grande, que satisface la ecuación corta de Weierstrass,

$$E : y^2 = x^3 + ax + b,$$

junto con un punto al infinito denotado por $\mathcal{O}$. El conjunto de puntos que satisfacen la anterior ecuación forman un grupo abeliano denotado por $E(\mathbb{F}_p)$ con orden $\#E(\mathbb{F}_p) = h \cdot r$, donde r es un primo grande y el cofactor h es un entero pequeño.



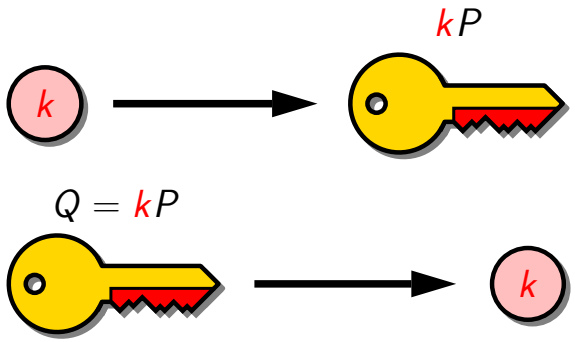
Criptografía basada en curvas elípticas



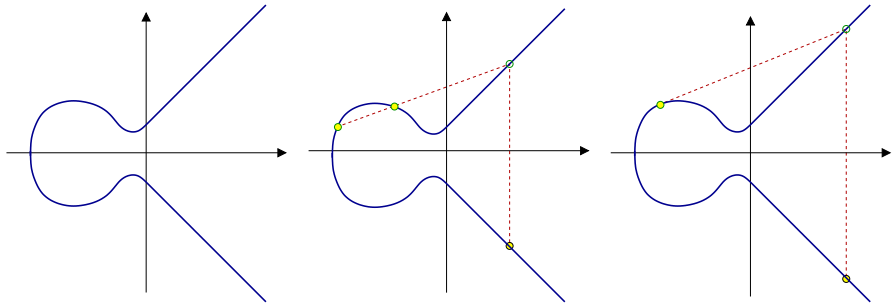
Una curva elíptica está definida por el conjunto de puntos afines $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, donde p es un primo impar grande, que satisface la ecuación corta de Weierstrass,

$$E : y^2 = x^3 + ax + b,$$

junto con un punto al infinito denotado por $\mathcal{O}$. El conjunto de puntos que satisfacen la anterior ecuación forman un grupo abeliano denotado por $E(\mathbb{F}_p)$ con orden $\#E(\mathbb{F}_p) = h \cdot r$, donde r es un primo grande y el cofactor h es un entero pequeño.



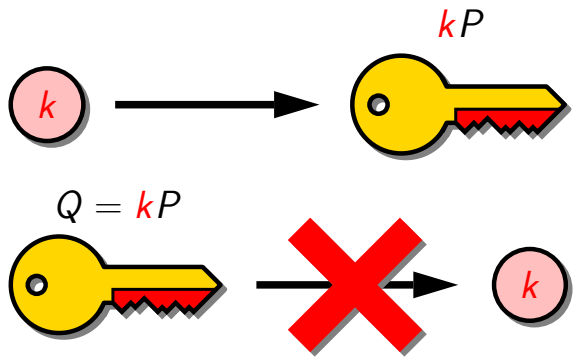
Criptografía basada en curvas elípticas



Una curva elíptica está definida por el conjunto de puntos afines $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, donde p es un primo impar grande, que satisface la ecuación corta de Weierstrass,

$$E : y^2 = x^3 + ax + b,$$

junto con un punto al infinito denotado por $\mathcal{O}$. El conjunto de puntos que satisfacen la anterior ecuación forman un grupo abeliano denotado por $E(\mathbb{F}_p)$ con orden $\#E(\mathbb{F}_p) = h \cdot r$, donde r es un primo grande y el cofactor h es un entero pequeño.



Protocolo Diffie-Hellman con curvas elípticas [protocolo ECDH]

Algorithm 1 Protocolo Diffie-Hellman con curvas elípticas

Parámetros públicos: primo p, curva $E/\mathbb{F}_p$, punto generador $P = (x, y) \in E(\mathbb{F}_p)$ de orden primo r

Fase 1: Generación de llaves

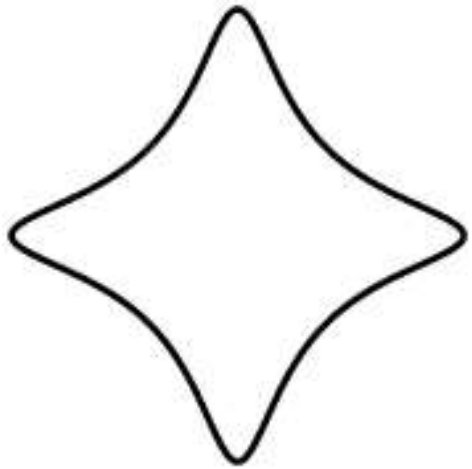
	Alicia		**Beto**
1:	Selecciona su llave privada $d_A \xleftarrow{\$} [1, r-1]$	1:	Selecciona su llave privada $d_B \xleftarrow{\$} [1, r-1]$
2:	Calcula su llave pública $Q_A \leftarrow d_A P$	2:	Calcula su llave pública $Q_B \leftarrow d_B P$

Fase 2: Cómputo del secreto compartido

	Alicia		**Beto**
3:	Envía Q_A a Beto	3:	Envía Q_B a Alicia
4:	Calcula $R \leftarrow d_A Q_B$	4:	Calcula $R \leftarrow d_B Q_A$

fase final: El secreto compartido es la coordenada x del punto R

Curvas famosas: Curve25519 [La curva elíptica escogida en TLS 1.3, WhatsApp...]

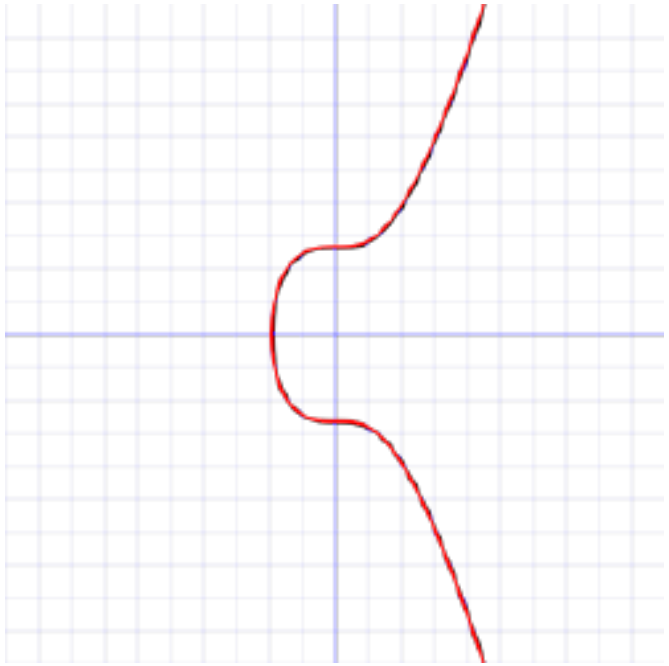


- Esta curva fue propuesta por Daniel J. Bernstein en 2005. Adquirió una popularidad estelar a paritr del año 2013.
- Esta curva satisface la ecuación:

$$E : y^2 = x^3 + 48666 \cdot x^2 + x,$$

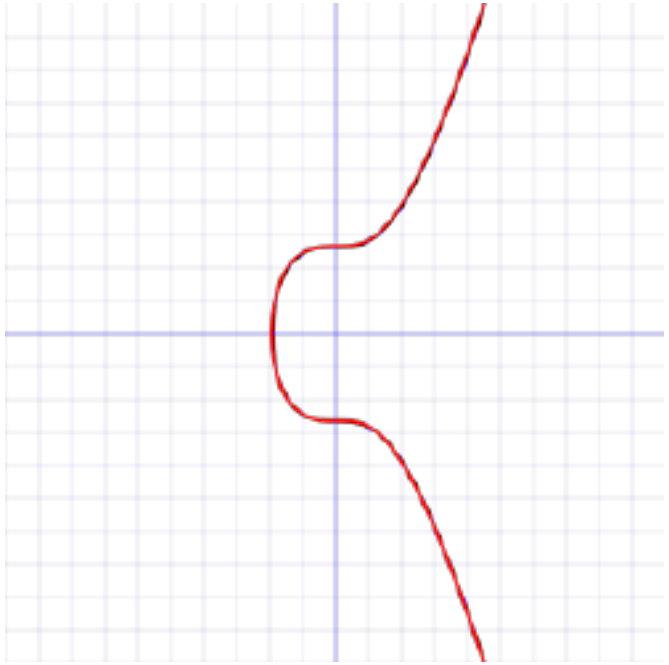
- Curve25519 es utilizada para generar secretos compartidos y verificar/firmar documentos miles de millones de veces todos los días en aplicaciones masivas tales como TLS 1.3 y WhatsApp, entre otras muchas.

Curvas famosas: Secp256k1 [La curva elíptica escogida por Satoshi Nakamoto]



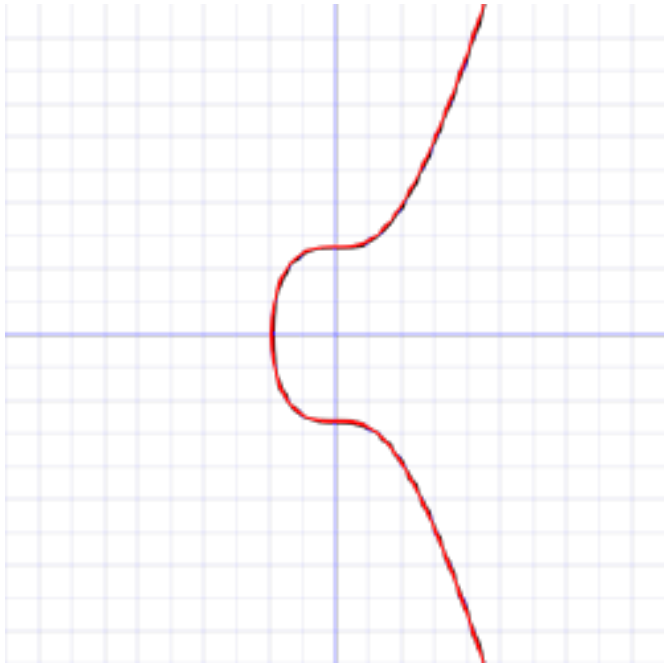
- La curva elíptica utilizada en Bitcoin se conoce como la curva de Koblitz Secp256k1

Curvas famosas: Secp256k1 [La curva elíptica escogida por Satoshi Nakamoto]



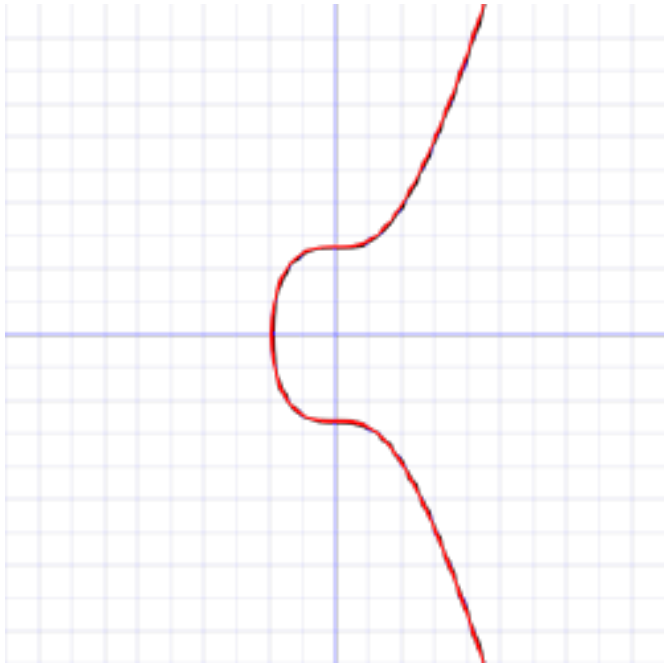
- Se considera que la capacidad de cómputo de todo el planeta tierra no puede vulnerar un esquema con una seguridad superior a 2^{90} operaciones en un tiempo razonable (digamos menos de un siglo)

Curvas famosas: Secp256k1 [La curva elíptica escogida por Satoshi Nakamoto]



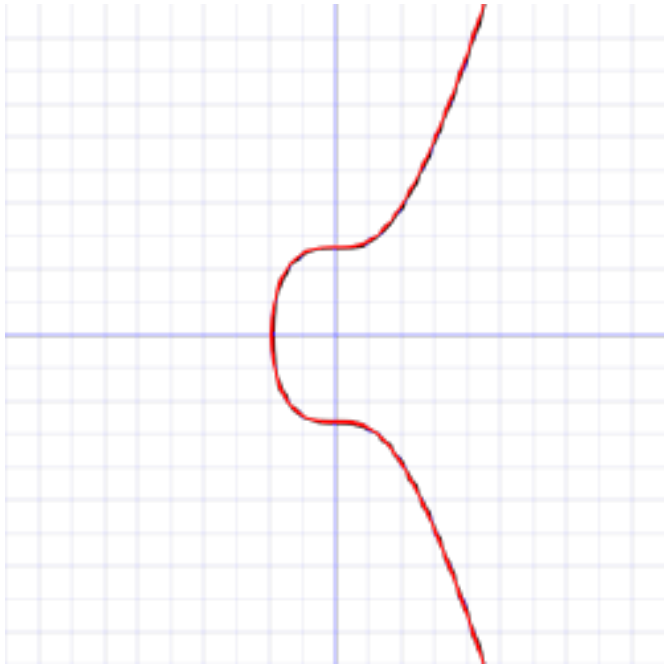
- Secp256k1 ofrece una seguridad estimada de 2^{128} operaciones, por lo que actualmente se considera invulnerable

Curvas famosas: Secp256k1 [La curva elíptica escogida por Satoshi Nakamoto]



- Una llave secreta típica de Bitcoin es un número de 256 bits que puede escribirse con unos 78 dígitos decimales

Curvas famosas: Secp256k1 [La curva elíptica escogida por Satoshi Nakamoto]

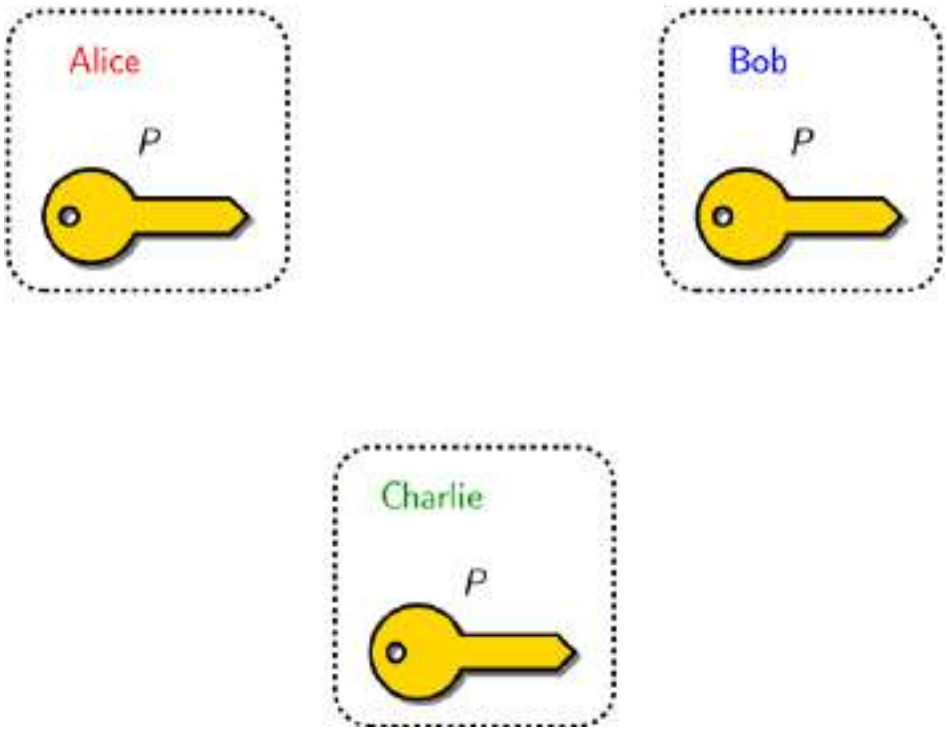


- Ejemplo de una llave secreta de Bitcoin:
  5005556725169192523536902815980714287876713442113715730946427341032850666964 6

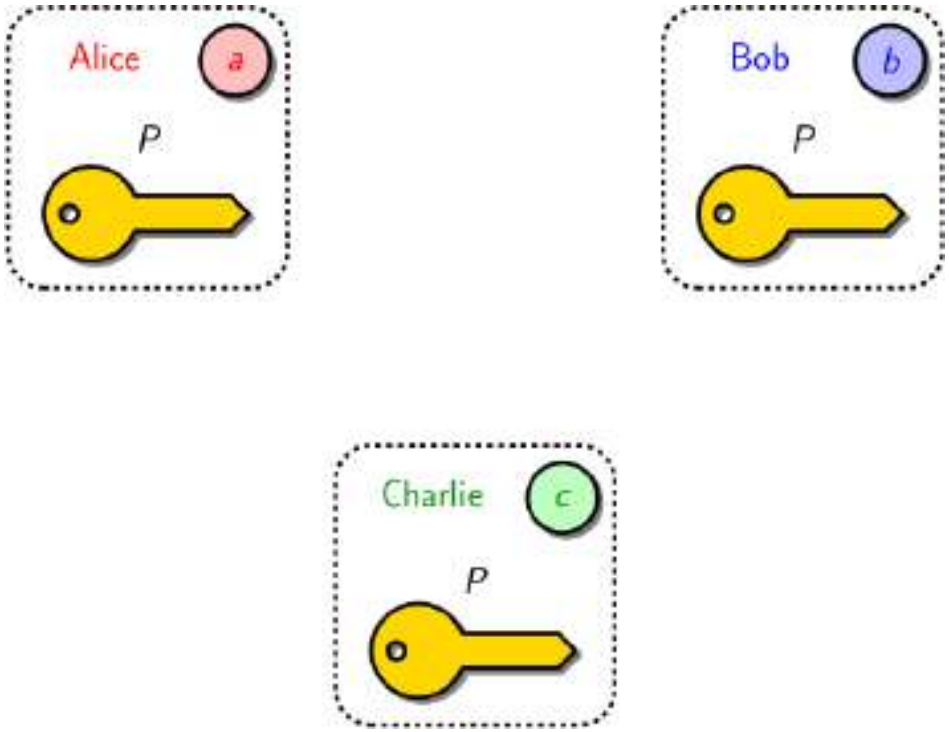
Tamaños de llave recomendados (circa 2013)

Security in bits	RSA $\|\|N\|\|_2$	DL: $\mathbb{F}_p$ $\|\|p\|\|_2$	DL: $\mathbb{F}_{2^m}$ m	ECC $\|\|q\|\|_2$
80	1024	1024	1500	160
112	2048	2048	3500	224
128	3072	3072	4800	256
192	7680	7680	12500	384
256	15360	15360	25000	512

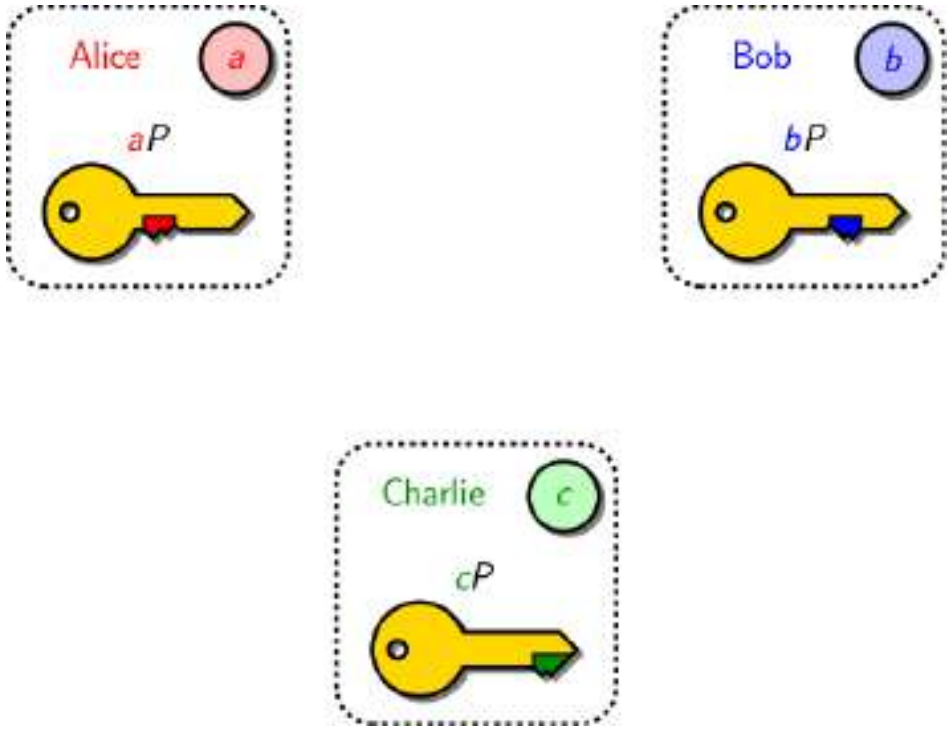
Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?



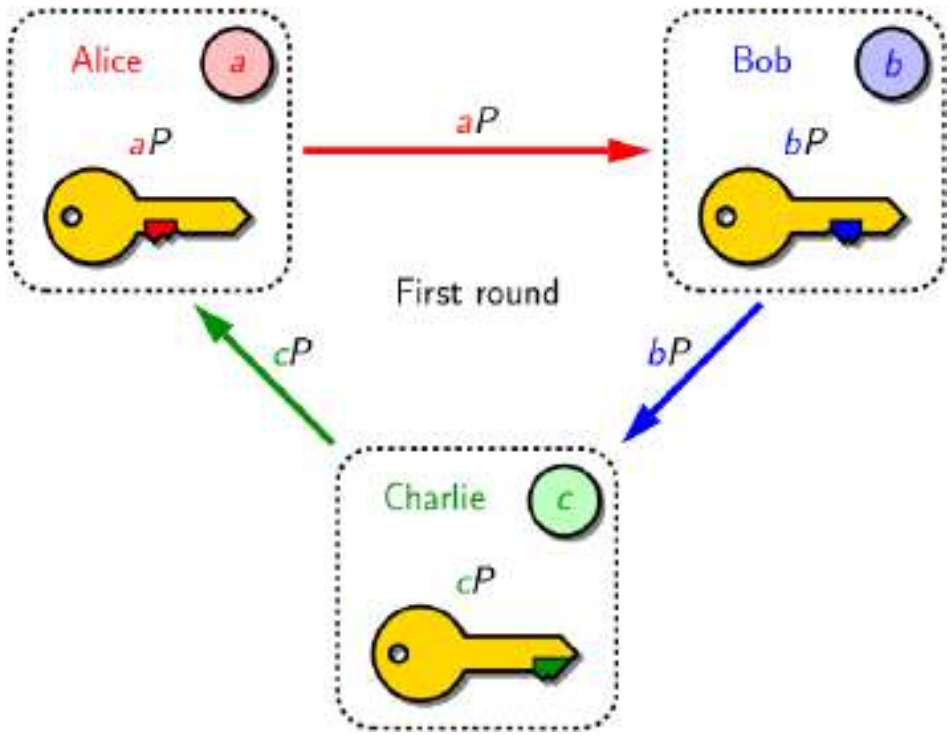
Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?



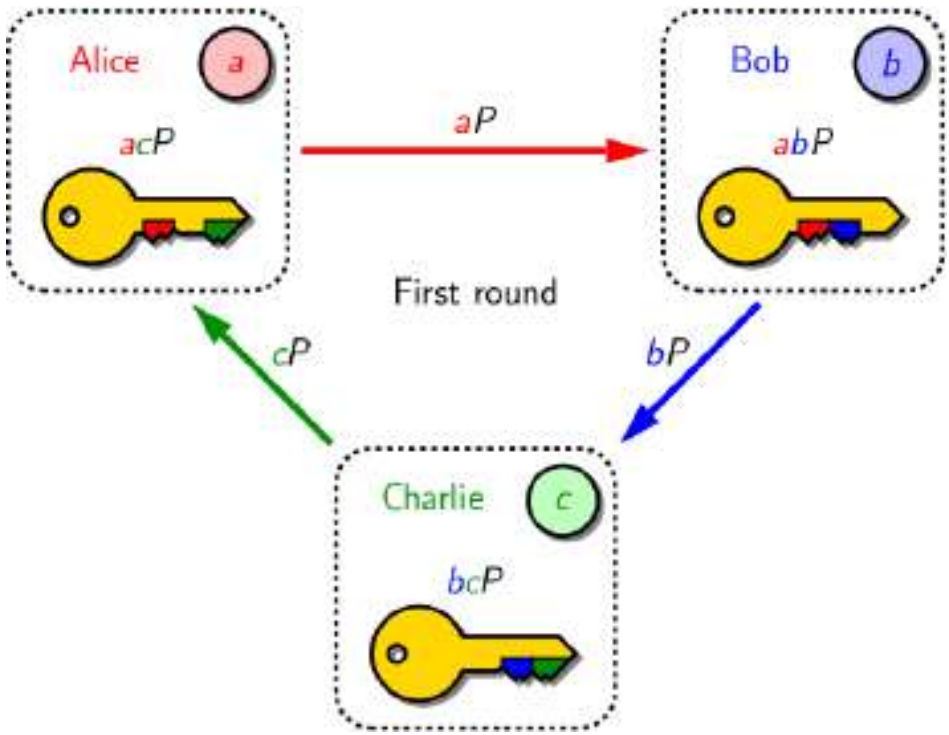
Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?



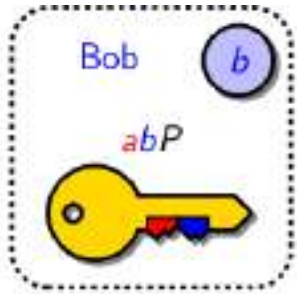
Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?

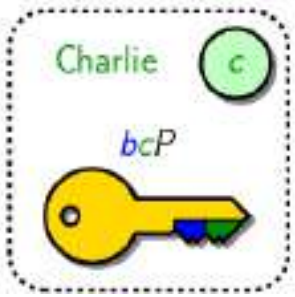


Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?

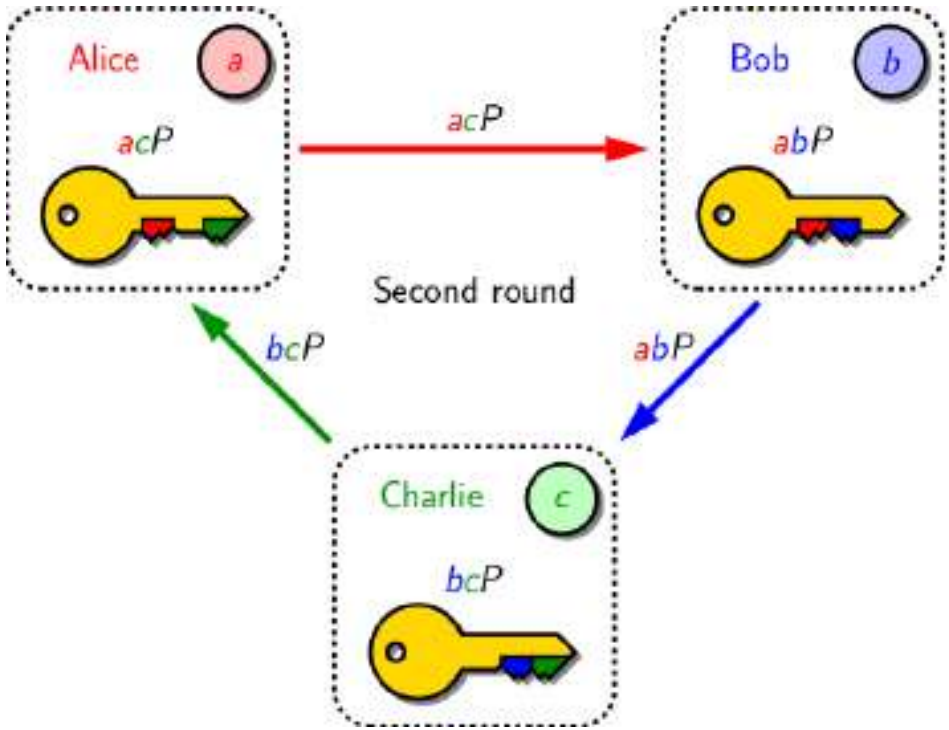


Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?

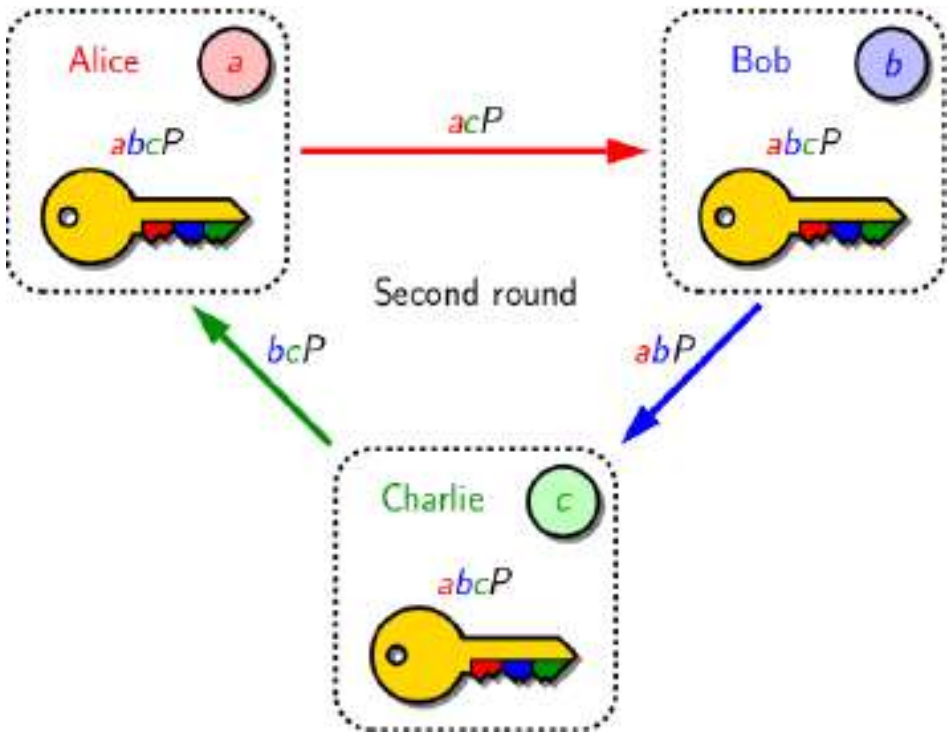




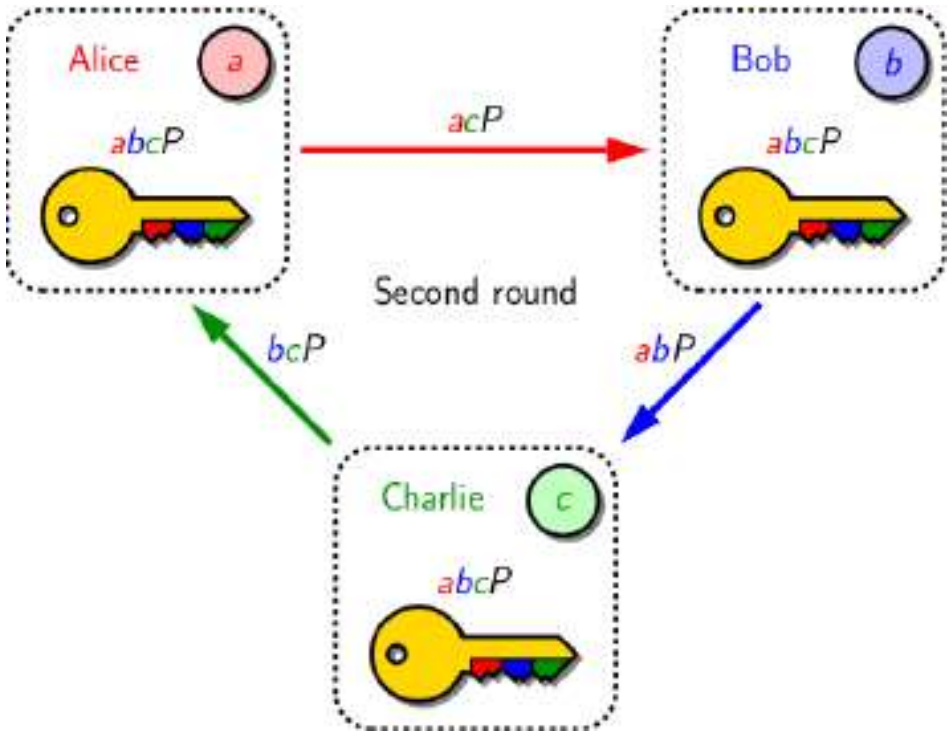
Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?



Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?



Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?



- Problema abierto desde el artículo de Diffie y Hellman de 1976: ¿Existe un protocolo de Diffie-Hellman que pueda ser ejecutado en una sola ronda?

Emparejamientos bilineales en criptografía

- Sea $(\mathbb{G}_2, \times)$, un grupo cíclico escrito multiplicativamente de orden $\#\mathbb{G}_2 = \#\mathbb{G}_1 = \ell$

Emparejamientos bilineales en criptografía

- Sea $(\mathbb{G}_2, \times)$, un grupo cíclico escrito multiplicativamente de orden $\#\mathbb{G}_2 = \#\mathbb{G}_1 = \ell$
- Un emparejamiento bilineal en $(\mathbb{G}_1, \mathbb{G}_2)$ es una proyección

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$$

que satisface las siguientes condiciones:

Emparejamientos bilineales en criptografía

- Sea $(\mathbb{G}_2, \times)$, un grupo cíclico escrito multiplicativamente de orden $\#\mathbb{G}_2 = \#\mathbb{G}_1 = \ell$
- Un emparejamiento bilineal en $(\mathbb{G}_1, \mathbb{G}_2)$ es una proyección

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$$

que satisface las siguientes condiciones:

  - No degenerado: $\hat{e}(P, P) \neq 1_{\mathbb{G}_2}$ (equivalentemente $\hat{e}(P, P)$ genera $\mathbb{G}_2$)

Emparejamientos bilineales en criptografía

- Sea $(\mathbb{G}_2, \times)$, un grupo cíclico escrito multiplicativamente de orden $\#\mathbb{G}_2 = \#\mathbb{G}_1 = \ell$
- Un emparejamiento bilineal en $(\mathbb{G}_1, \mathbb{G}_2)$ es una proyección

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$$

que satisface las siguientes condiciones:

  - No degenerado: $\hat{e}(P, P) \neq 1_{\mathbb{G}_2}$ (equivalentemente $\hat{e}(P, P)$ genera $\mathbb{G}_2$)
  - bilineal:
    $\hat{e}(Q_1+Q_2, R) = \hat{e}(Q_1, R)\cdot\hat{e}(Q_2, R) \quad \hat{e}(Q, R_1+R_2) = \hat{e}(Q, R_1)\cdot\hat{e}(Q, R_2)$

Emparejamientos bilineales en criptografía

- Sea $(\mathbb{G}_2, \times)$, un grupo cíclico escrito multiplicativamente de orden $\#\mathbb{G}_2 = \#\mathbb{G}_1 = \ell$
- Un emparejamiento bilineal en $(\mathbb{G}_1, \mathbb{G}_2)$ es una proyección

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$$

que satisface las siguientes condiciones:

  - No degenerado: $\hat{e}(P, P) \neq 1_{\mathbb{G}_2}$ (equivalentemente $\hat{e}(P, P)$ genera $\mathbb{G}_2$)
  - bilineal:
    $\hat{e}(Q_1+Q_2, R) = \hat{e}(Q_1, R)\cdot\hat{e}(Q_2, R) \quad \hat{e}(Q, R_1+R_2) = \hat{e}(Q, R_1)\cdot\hat{e}(Q, R_2)$
  - computable: $\hat{e}$ puede ser eficientemente computado

Emparejamientos bilineales en criptografía

- Sea $(\mathbb{G}_2, \times)$, un grupo cíclico escrito multiplicativamente de orden $\#\mathbb{G}_2 = \#\mathbb{G}_1 = \ell$
- Un emparejamiento bilineal en $(\mathbb{G}_1, \mathbb{G}_2)$ es una proyección

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$$

que satisface las siguientes condiciones:

  - No degenerado: $\hat{e}(P, P) \neq 1_{\mathbb{G}_2}$ (equivalentemente $\hat{e}(P, P)$ genera $\mathbb{G}_2$)
  - bilineal:
    $\hat{e}(Q_1+Q_2, R) = \hat{e}(Q_1, R)\cdot\hat{e}(Q_2, R) \quad \hat{e}(Q, R_1+R_2) = \hat{e}(Q, R_1)\cdot\hat{e}(Q, R_2)$
  - computable: $\hat{e}$ puede ser eficientemente computado

- Propiedad multiplicativa: Para cualesquiera dos enteros, k_1 and k_2

$$\hat{e}(k_1 Q, k_2 R) = \hat{e}(Q, R)^{k_1 k_2}$$

Emparejamientos bilineales en criptografía

- Sea $(\mathbb{G}_2, \times)$, un grupo cíclico escrito multiplicativamente de orden $\#\mathbb{G}_2 = \#\mathbb{G}_1 = \ell$
- Un emparejamiento bilineal en $(\mathbb{G}_1, \mathbb{G}_2)$ es una proyección

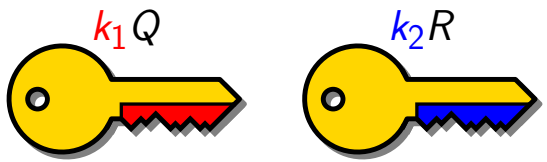
$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$$

que satisface las siguientes condiciones:

  - No degenerado: $\hat{e}(P, P) \neq 1_{\mathbb{G}_2}$ (equivalentemente $\hat{e}(P, P)$ genera $\mathbb{G}_2$)
  - bilineal:
    $\hat{e}(Q_1+Q_2, R) = \hat{e}(Q_1, R)\cdot\hat{e}(Q_2, R) \quad \hat{e}(Q, R_1+R_2) = \hat{e}(Q, R_1)\cdot\hat{e}(Q, R_2)$
  - computable: $\hat{e}$ puede ser eficientemente computado

- Propiedad multiplicativa: Para cualesquiera dos enteros, k_1 and k_2

$$\hat{e}(k_1 Q, k_2 R) = \hat{e}(Q, R)^{k_1 k_2}$$



Emparejamientos bilineales en criptografía

- Sea $(\mathbb{G}_2, \times)$, un grupo cíclico escrito multiplicativamente de orden $\#\mathbb{G}_2 = \#\mathbb{G}_1 = \ell$
- Un emparejamiento bilineal en $(\mathbb{G}_1, \mathbb{G}_2)$ es una proyección

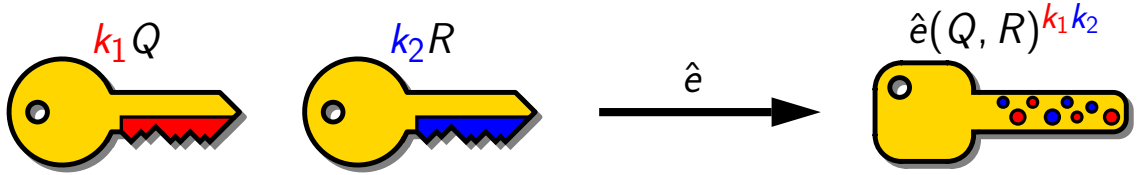
$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$$

que satisface las siguientes condiciones:

  - No degenerado: $\hat{e}(P, P) \neq 1_{\mathbb{G}_2}$ (equivalentemente $\hat{e}(P, P)$ genera $\mathbb{G}_2$)
  - bilineal:
    $\hat{e}(Q_1+Q_2, R) = \hat{e}(Q_1, R)\cdot\hat{e}(Q_2, R) \quad \hat{e}(Q, R_1+R_2) = \hat{e}(Q, R_1)\cdot\hat{e}(Q, R_2)$
  - computable: $\hat{e}$ puede ser eficientemente computado

- Propiedad multiplicativa: Para cualesquiera dos enteros, k_1 and k_2

$$\hat{e}(k_1 Q, k_2 R) = \hat{e}(Q, R)^{k_1 k_2}$$



Emparejamientos bilineales en criptografía

- Primeor fueron utilizados para atacar a las curvas elípticas supersingulares
  - ataques de Menezes-Okamoto-Vanstone y Frey-Rück en 1993 y 1994

$$\mathrm{PLD}_{\mathbb{G}_1} \quad <_{\mathrm{P}} \quad \mathrm{PLD}_{\mathbb{G}_\tau}$$

$$kP \quad \longrightarrow \quad \hat{e}(kP, P) = \hat{e}(P, P)^k$$

  - for aplicaciones criptográficas, requerimos también que el PLD en $\mathbb{G}_\tau$ sea intratable

Emparejamientos bilineales en criptografía

- Primeor fueron utilizados para atacar a las curvas elípticas supersingulares
  - ataques de Menezes-Okamoto-Vanstone y Frey-Rück en 1993 y 1994

$$\mathrm{PLD}_{\mathbb{G}_1} \quad <_{\mathrm{P}} \quad \mathrm{PLD}_{\mathbb{G}_\tau}$$

$$kP \quad \longrightarrow \quad \hat{e}(kP, P) = \hat{e}(P, P)^k$$

  - for aplicaciones criptográficas, requerimos también que el PLD en $\mathbb{G}_\tau$ sea intratable
- protocolo tripartito de una sola ronda para computar un secreto compartido (Joux, 2000)

Emparejamientos bilineales en criptografía

- Primeor fueron utilizados para atacar a las curvas elípticas supersingulares
  - ataques de Menezes-Okamoto-Vanstone y Frey-Rück en 1993 y 1994

$$\mathrm{PLD}_{\mathbb{G}_1} \quad <_{\mathrm{P}} \quad \mathrm{PLD}_{\mathbb{G}_\tau}$$

$$kP \quad \longrightarrow \quad \hat{e}(kP, P) = \hat{e}(P, P)^k$$

  - for aplicaciones criptográficas, requerimos también que el PLD en $\mathbb{G}_\tau$ sea intratable
- protocolo tripartito de una sola ronda para computar un secreto compartido (Joux, 2000)
- cifrado basado en la identidad
  - Boneh–Franklin, 2001
  - Sakai–Kasahara, 2001

Emparejamientos bilineales en criptografía

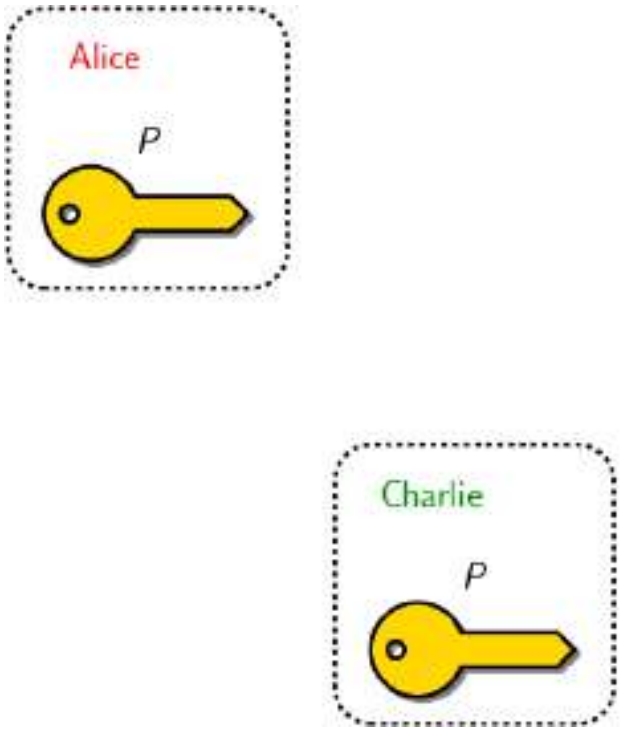
- Primeor fueron utilizados para atacar a las curvas elípticas supersingulares
  - ataques de Menezes-Okamoto-Vanstone y Frey-Rück en 1993 y 1994

$$\mathrm{PLD}_{\mathbb{G}_1} \quad <_{\mathrm{P}} \quad \mathrm{PLD}_{\mathbb{G}_\tau}$$

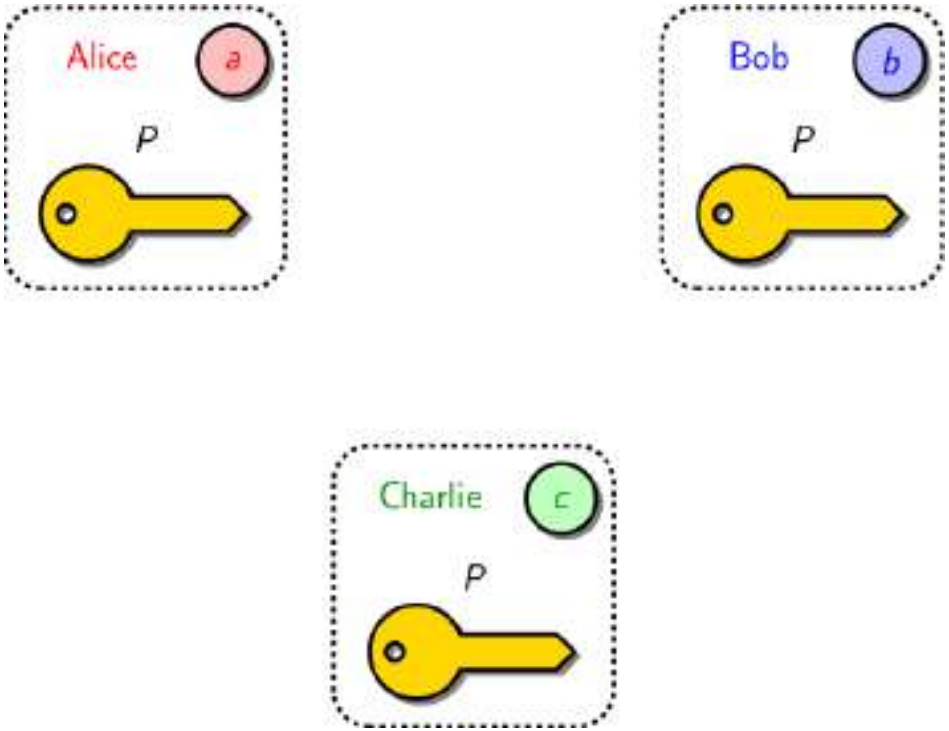
$$kP \quad \longrightarrow \quad \hat{e}(kP, P) = \hat{e}(P, P)^k$$

  - for aplicaciones criptográficas, requerimos también que el PLD en $\mathbb{G}_\tau$ sea intratable
- protocolo tripartito de una sola ronda para computar un secreto compartido (Joux, 2000)
- cifrado basado en la identidad
  - Boneh–Franklin, 2001
  - Sakai–Kasahara, 2001
- Firmas digitales cortas
  - Boneh–Lynn–Shacham, 2001
  - Zang–Safavi-Naini–Susilo, 2004
- ...

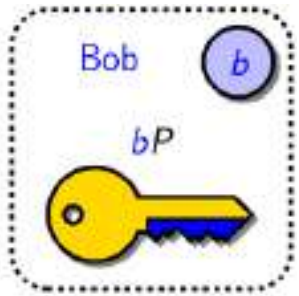
Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?. Solución: Protocolo DH tripartito de Antoine Joux



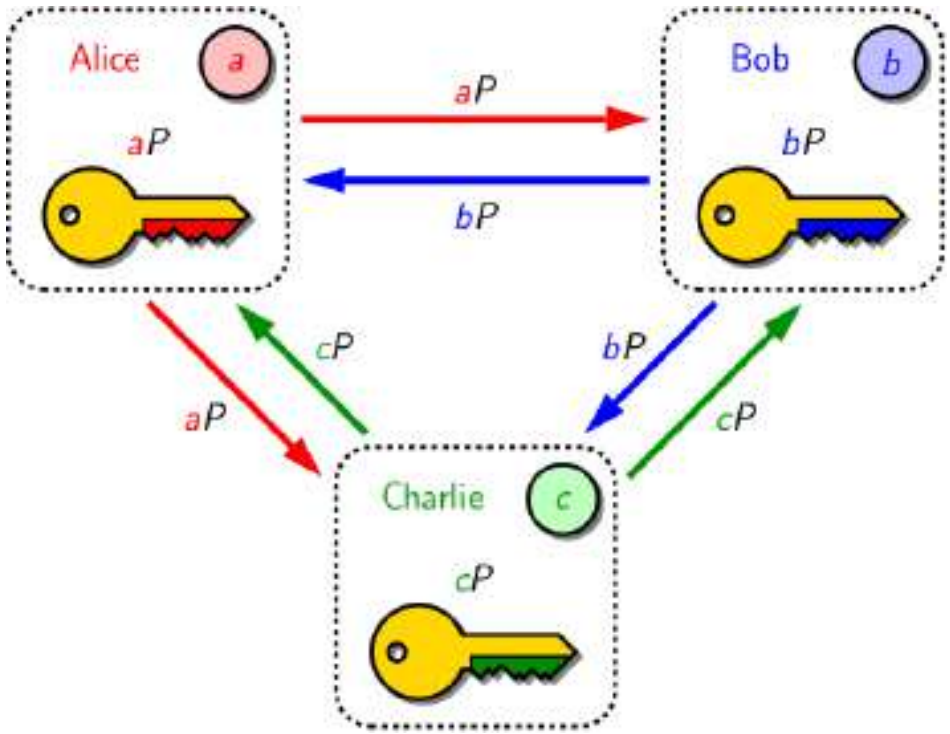
Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?. Solución: Protocolo DH tripartito de Antoine Joux



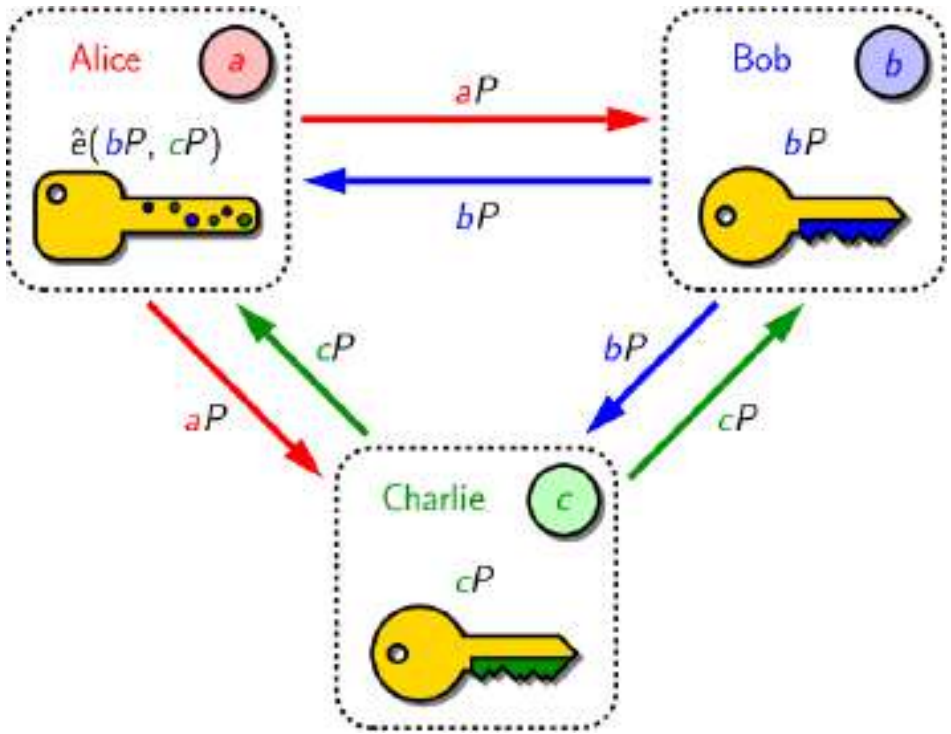
Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?. Solución: Protocolo DH tripartito de Antoine Joux



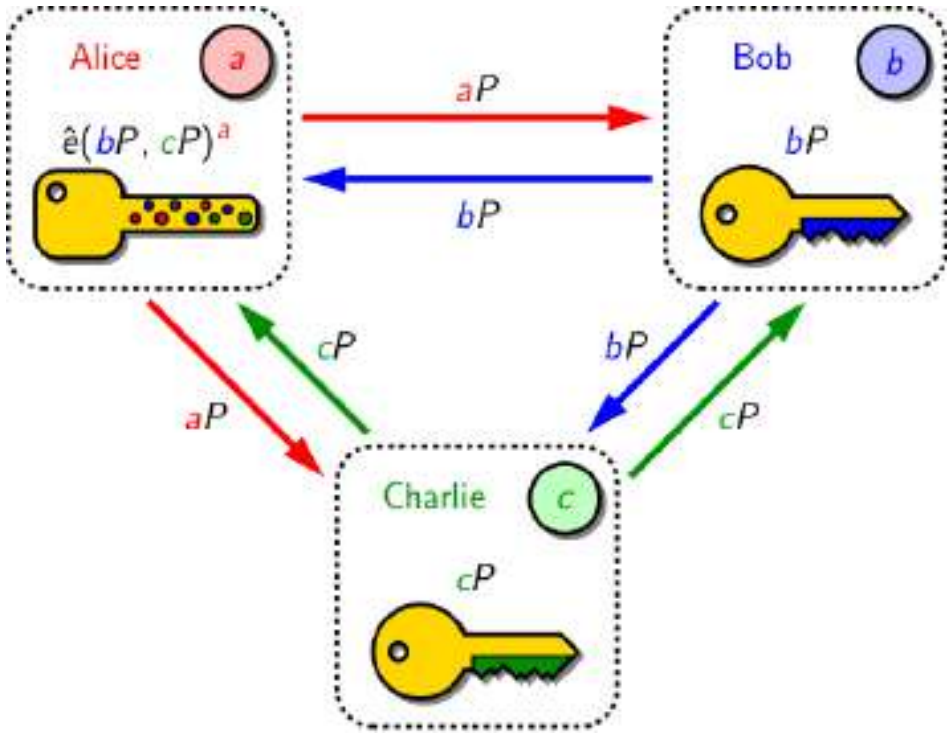
Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?. Solución: Protocolo DH tripartito de Antoine Joux



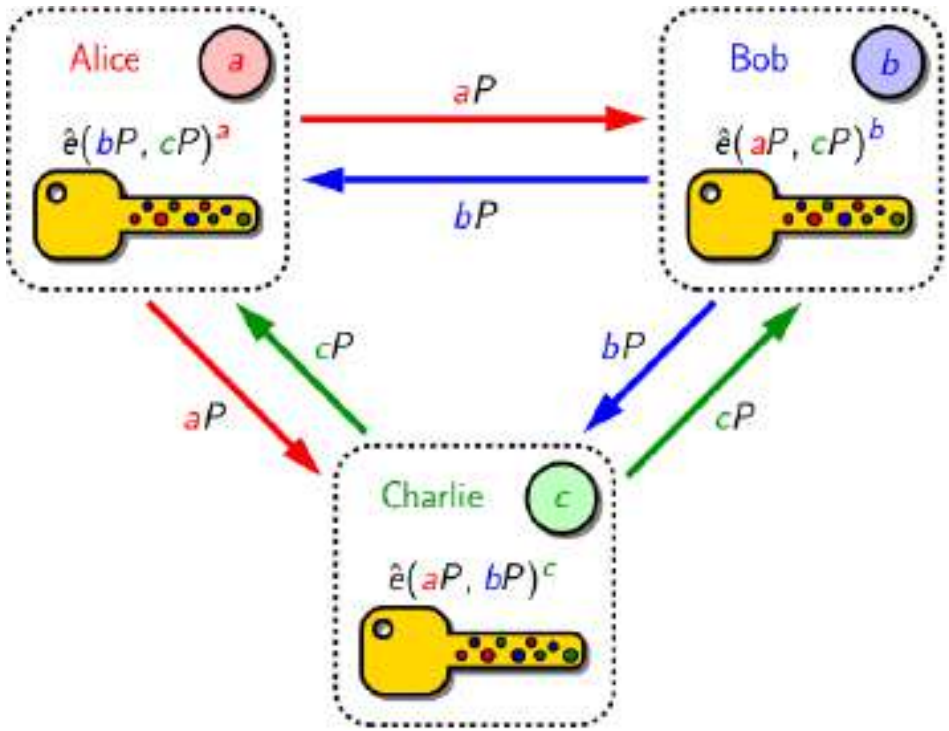
Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?. Solución: Protocolo DH tripartito de Antoine Joux



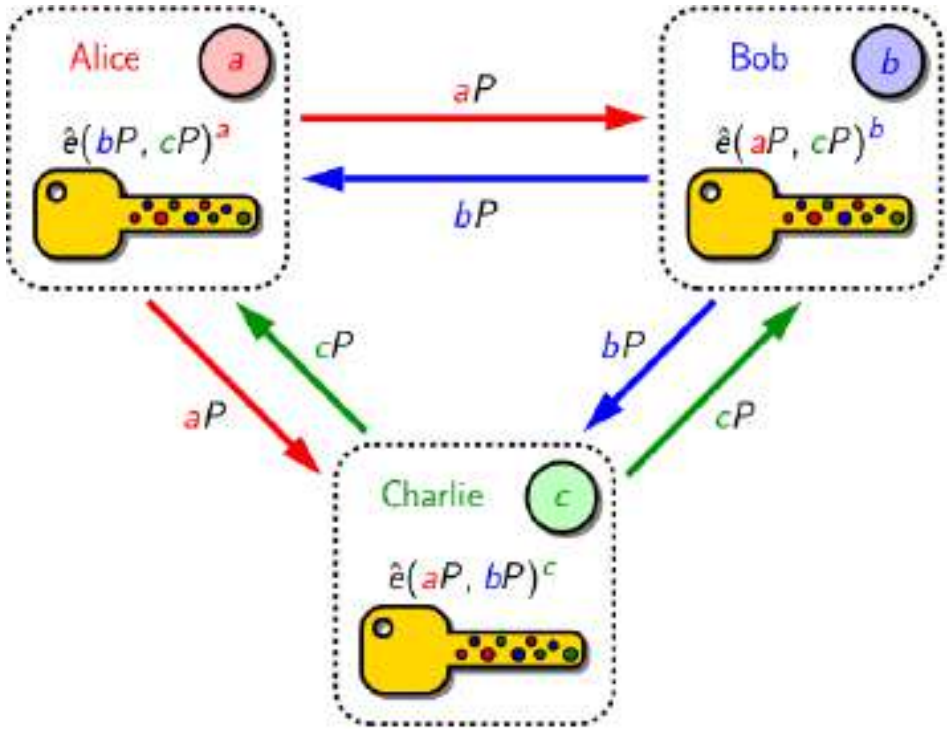
Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?. Solución: Protocolo DH tripartito de Antoine Joux



Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?. Solución: Protocolo DH tripartito de Antoine Joux

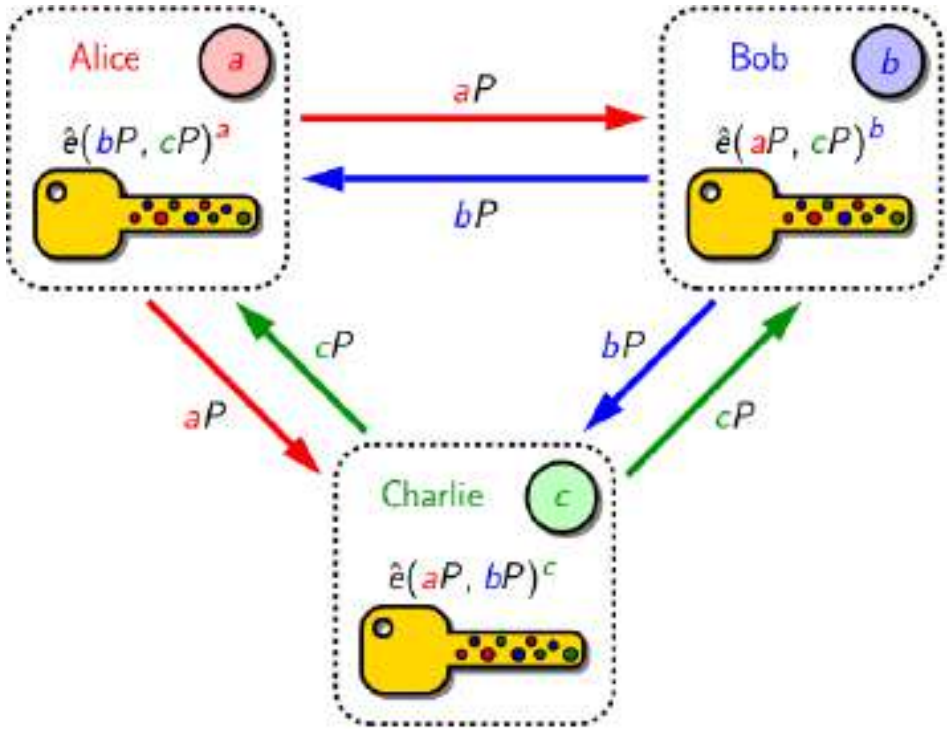


Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?. Solución: Protocolo DH tripartito de Antoine Joux



- Problema abierto desde el artículo de Diffie y Hellman de 1976: ¿Existe un protocolo de Diffie-Hellman que pueda ser ejecutado en una sola ronda?

Problema de diseño: ¿Cómo establecer un secreto compartido tripartito de una sola ronda?. Solución: Protocolo DH tripartito de Antoine Joux

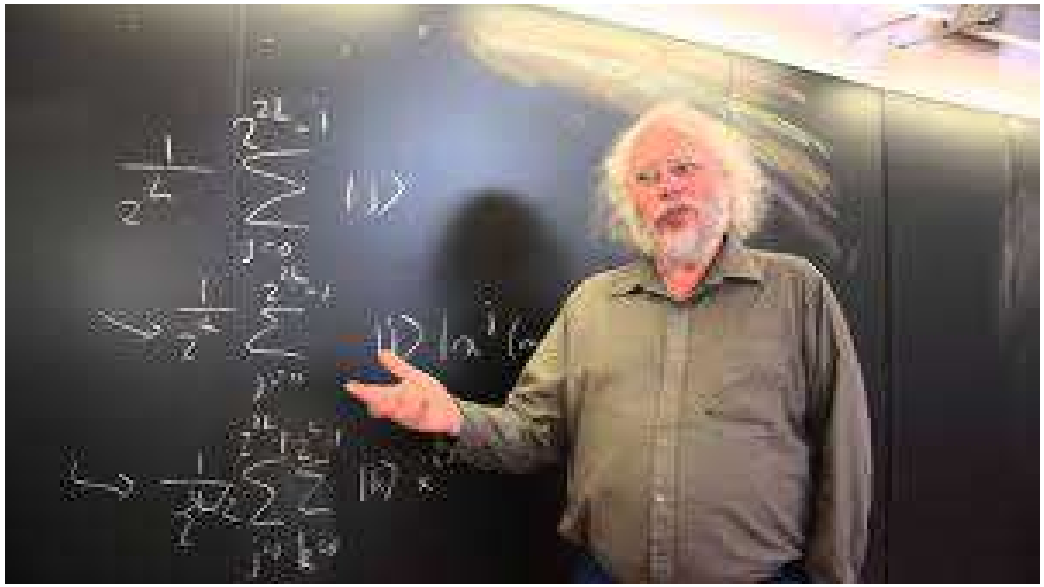


- El protocolo funciona debido a que:

$$\hat{e}(bP, cP)^a = \hat{e}(aP, cP)^b = \hat{e}(aP, bP)^c = \hat{e}(P, P)^{abc}$$

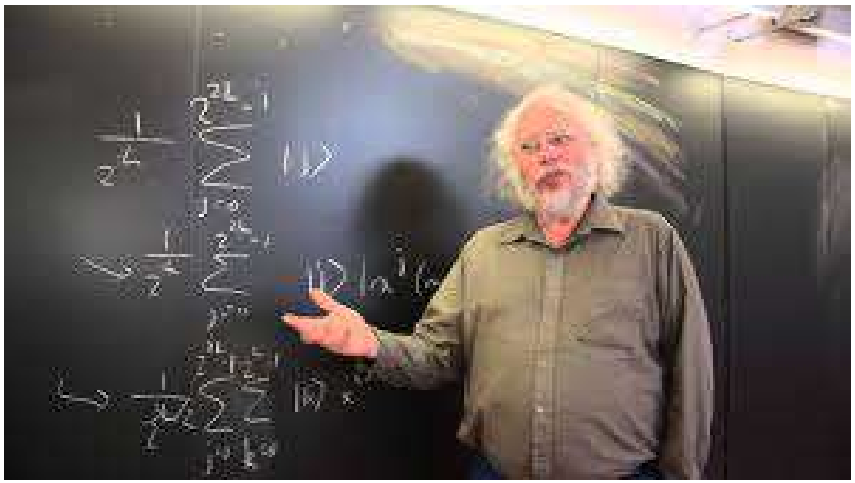
Escenario [Apocalíptico] para los próximos años: Llegan las computadoras cuánticas

Escenario [Apocalíptico] para los próximos años



Una implementación cuántica del algoritmo de Peter Shor para factorización de números enteros hace que el esfuerzo computacional para romper la criptografía de curvas elípticas se reduzca de miles de millones de años a cientos de horas.

Escenario [Apocalíptico] para los próximos años



Junto con la criptografía basada en curvas elípticas perecen RSA y cualquier esquema basado en la dificulta de romper el PLD.

Escenario [Apocalíptico] para los próximos años

- Posibles bestias sobrevivientes: NTRU

Respuestas al escenario [Apocalíptico]: criptografía post-cuántica

- Concurso del NIST para determinar el nuevo estándar de criptografía post-cuántica. Se desea encontrar esquemas confiables que ejecuten en computadoras tradicionales que sepan resistir los embates de ataques lanzados desde artefactos cuánticos
- El interés principal reside en hallar nuevos esquemas de firma/verificación y de establecimiento de secretos compartidos

Respuestas al escenario [Apocalíptico]: Criptografía post-cuántica

- Se inscribieron 79 candidatos al concurso del NIST, los cuales fueron clasificados en las siguientes categorías:
  - Sistemas basado en retículas
  - sistemas basados en códigos de corrección de error
  - Sistemas basados en la resolución de ecuaciones simultáneas multi-variable definidas sobre campos finitos
  - sistemas basados en funciones picadillo
  - sistemas basados en el grafo de isogenias formado por curvas elípticas supersingulares

A manera de conclusiones

- Desde que Al-Kindi inventara el criptoanálisis por frecuencia en Bagdad en el siglo IX inició, parafraseando al famoso libro, una eterna trenza dorada entre esa subdisciplina y la criptografía.

A manera de conclusiones

- Después de Al-Kindi durante cerca de 600 años los criptoanalistas prevalecieron sobre los criptógrafos. Sin embargo, con la invención del código de Vigènere, la situación dio la vuelta a favor de estos últimos por cerca de 300 años.

A manera de conclusiones

- Tras una larga batalla que duró todo el siglo XX, los criptógrafos lograron retomar el control con la invención de la criptografía de llave pública y el desarrollo de modernos cifradores simétricos.

A manera de conclusiones

- Sin embargo la nueva arma de los criptoanalistas, el cómputo cuántico luce poderoso y amenaza con volver a cambiar el orden de las cosas.

A manera de conclusiones

- Pero ya los criptógrafos se aprestan a contra-atacar estudiando nuevos métodos de criptografía post-cuántica.

Gracias

- Mis sinceros agradecimientos al Dr. Jean-Luc Beuchat por el diseño de las animaciones que hermosean esta presentación