

REIVINDICACIONES:

1. Un método implementado por computadora de determinación en un primer nodo (C), un secreto común (CS) que es común con el primer nodo (C) y un segundo nodo (S), en donde el primer nodo (C) está asociado con un primer par de criptografía asimétrica que tiene una clave privada maestra de primer nodo (V_{1C}) y una clave pública maestra de primer nodo (P_{1C}), y el segundo nodo (S) está asociado con un segundo par de criptografía asimétrica que tiene una segunda clave privada maestra de segundo nodo (V_{1S}) y una clave pública maestra de segundo nodo (P_{1S}), en donde el método comprende:

- determinar una segunda clave privada de primer nodo (V_{2C}) con base en por lo menos la clave privada maestra de primer nodo (V_{1C}) y una clave determinista (DK);
- determinar una segunda clave pública de segundo nodo (P_{2S}) con base en por lo menos la clave pública maestra de segundo nodo (P_{1S}) y la clave determinista (DK); y
- determinar el secreto común (CS) con base en la segunda clave privada de primer nodo (V_{2C}) y la segunda clave pública de segundo nodo (P_{2S}),

en donde el segundo nodo (S) tiene el mismo secreto común (CS) con base en una segunda clave pública de primer nodo (P_{2C}) y una segunda clave privada de segundo nodo (V_{2S}), en donde:

- la segunda clave pública de primer nodo (P_{2C}) se basa en por lo menos la clave pública maestra de primer nodo (P_{1C}) y la clave determinista (DK); y
- la segunda clave privada de segundo nodo (V_{2S}) se basa en por lo menos la clave privada maestra de segundo nodo (V_{1S}) y la clave determinista (DK).

2. Un método de acuerdo con la reivindicación 1, caracterizado porque la clave determinista (DK) se basa en un mensaje (M).

3. El método de acuerdo con la reivindicación 2, que comprende además:

- generar un primer mensaje firmado (SM1) con base en el mensaje (M) y la segunda clave privada de primer nodo (V_{2C}); y
- enviar, a través de la red de comunicaciones, el primer mensaje firmado (SM1) al segundo nodo (S),

en donde el primer mensaje firmado (SM1) se puede validar con una segunda clave pública de primer nodo (P_{2C}) para autenticar el primer nodo (C).

4. Un método de acuerdo con la reivindicación 2 o 3, que comprende además:

- recibir, a través de la red de comunicaciones, un segundo mensaje firmado (SM2) procedente del segundo nodo (S);
- validar el segundo mensaje firmado (SM2) con la segunda clave pública de segundo nodo (P_{2S}); y

- autenticar el segundo nodo (S) con base en el resultado de validar el segundo mensaje firmado (SM2),

en donde el segundo mensaje firmado (SM2) se generó con base en el mensaje (M), o un segundo mensaje (M2) y la segunda clave privada de segundo nodo (V_{2S}).

5. Un método de acuerdo con cualquiera de las reivindicaciones 2 a 4, que comprende además:

- generar un mensaje (M); y
- enviar, a través de una red de comunicaciones, el mensaje (M) al segundo nodo (S).

6. Un método de acuerdo con cualquiera de las reivindicaciones 2 a 4, que comprende además:

- recibir el mensaje (M), a través de la red de comunicaciones, procedente del segundo nodo (S).

7. Un método de acuerdo con cualquiera de las reivindicaciones 2 a 4, que comprende además:

- recibir el mensaje (M), a través de la red de comunicaciones, procedente de otro nodo.

8. Un método de acuerdo con cualquiera de las reivindicaciones 2 a 4, que comprende además:

- recibir el mensaje (M) procedente de un almacén de datos y/o una interfaz de entrada asociada con el primer nodo (C).

9. Un método de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado porque la clave pública maestra de primer nodo (P_{1C}) y la clave pública maestra de segundo nodo (P_{1S}) se basan en una multiplicación de puntos de curva elíptica de la clave privada maestra de primer nodo (V_{1C}) y la clave privada maestra de segundo nodo (V_{1S}) respectivas y un generador (G).

10. Un método de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende además las etapas de:

- recibir, a través de la red de comunicaciones, la clave pública maestra de segundo nodo (P_{1S}); y
- almacenar, en un almacén de datos asociado con el primer nodo (C), la clave pública maestra de segundo nodo (P_{1S}).

11. Un método de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende además las etapas de:

- generar, en un primer nodo (C), la clave privada maestra de primer nodo (V_{1C}) y la clave pública maestra de primer nodo (P_{1C});
- enviar, a través de la red de comunicaciones, la clave pública maestra de primer nodo (P_{1C}) al segundo nodo (S) y/u otro nodo; y
- almacenar, en un primer almacén de datos asociado con el primer nodo (C), la clave privada maestra de primer nodo (V_{1C}).

12. Un método de acuerdo con la reivindicación 11, que comprende además:

- enviar, a través de la red de comunicaciones, al segundo nodo, un aviso indicativo de utilizar un sistema de criptografía de curva elíptica (ECC) común con un generador (G) común para el método de determinación de un secreto común (CS), y

- en donde la etapa de generar la clave privada maestra de primer nodo (V_{1C}) y la clave pública maestra de primer nodo (P_{1C}) comprende:

- generar la clave privada maestra de primer nodo (V_{1C}) con base en un número entero aleatorio en un intervalo permisible especificado en el sistema ECC común; y

- determinar la clave pública maestra de primer nodo (P_{1C}) con base en una multiplicación de puntos de curva elíptica de la clave privada maestra de primer nodo (V_{1C}) y el generador común (G) de acuerdo con la siguiente fórmula:

$$P_{1C} = V_{1C} \times G.$$

13. Un método de acuerdo con la reivindicación 12, que comprende además:

- determinar la clave determinista (DK) con base en una determinación de un hash (función de resumen) del mensaje (M), y

en donde la etapa de determinar una segunda clave privada de primer nodo (V_{2C}) se basa en una adición escalar de la clave privada maestra de primer nodo (V_{1C}) y la clave determinista (DK) de acuerdo con la siguiente fórmula:

$$V_{2C} = V_{1C} + DK, \text{ y}$$

en donde la etapa de determinar una segunda clave pública de segundo nodo (P_{2S}) se basa en la clave pública maestra de segundo nodo (P_{1S}) con una adición de puntos de curva elíptica a la multiplicación de puntos de curva elíptica de la clave determinista (DK) y el generador común (G) de acuerdo con la siguiente fórmula:

$$P_{2S} = P_{1S} + DK \times G.$$

14. Un método de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado porque la clave determinista (DK) se basa en la determinación de un hash (función de resumen) de una clave determinista previa.

15. Un método de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado porque el primer par de criptografía asimétrica y el segundo par de criptografía asimétrica se basan en una función de primer par de criptografía asimétrica previo y segundo par de criptografía asimétrica previo respectivos.

16. Un método de comunicación segura entre un primer nodo y un segundo nodo con algoritmo de clave simétrica, en donde el método comprende:

- determinar una clave simétrica con base en el secreto común determinado de acuerdo con el método de acuerdo con cualquiera de las reivindicaciones anteriores;

- encriptar un primer mensaje de comunicación, con la clave simétrica, en un primer mensaje de comunicación encriptado; y

- enviar, a través de una red de comunicaciones, el primer mensaje de comunicación encriptado desde el primer nodo (C) al segundo nodo (S).

17. El método de acuerdo con la reivindicación 16, caracterizado porque el método comprende además:

- recibir, a través de una red de comunicaciones, un segundo mensaje de comunicación encriptado procedente del segundo nodo (S); y

- desencriptar el segundo mensaje de comunicación encriptado, con la clave simétrica, en un segundo mensaje de comunicación.

18. Un método para llevar a cabo una transacción en línea entre un primer nodo y un segundo nodo, en donde el método comprende:

- determinar una clave simétrica con base en el secreto común determinado de acuerdo con el método de acuerdo con cualquiera de las reivindicaciones 1 a 15;

- encriptar un primer mensaje de transacción, con la clave simétrica, en un primer mensaje de transacción encriptado;

- enviar, a través de una red de comunicaciones, el primer mensaje de transacción encriptado desde el primer nodo (C) al segundo nodo (S);

- recibir, a través de una red de comunicaciones, un segundo mensaje de transacción encriptado procedente del segundo nodo (S); y

- desencriptar el segundo mensaje de transacción encriptado, con la clave simétrica, en un segundo mensaje de transacción.

19. Un dispositivo para la determinación de, en un primer nodo (C), un secreto común (CS) que es común con un segundo nodo (S), en donde el primer nodo (C) está asociado con un primer par de criptografía asimétrica que tiene una clave privada maestra de primer nodo (V_{1C}) y una clave pública maestra de primer nodo (P_{1C}), y el segundo nodo (S) está asociado con un segundo par de criptografía asimétrica que tiene una clave privada maestra de segundo nodo (V_{1S}) y una clave pública maestra de segundo nodo (P_{1S}), en donde el dispositivo comprende un primer dispositivo de procesamiento para llevar a cabo el método de acuerdo con cualquiera de las reivindicaciones anteriores para determinar el secreto común.

20. Un dispositivo para la comunicación segura, o la realización de una transacción en línea segura entre un primer nodo y un segundo nodo, en donde el dispositivo incluye un primer dispositivo de procesamiento para:

- llevar a cabo el método de cualquiera de las reivindicaciones 16 a 18.

21. Un dispositivo de acuerdo con la reivindicación 19 o 20, caracterizado porque comprende además un primer almacén de datos para almacenar una o más de la clave privada maestra de primer nodo (V_{1C}).

22. Un dispositivo de acuerdo con la reivindicación 21, caracterizado porque el primer almacén de datos almacena además una o más de la clave pública maestra de primer nodo (P_{1C}), la clave pública maestra de segundo nodo (P_{1S}) y el mensaje (M).

23. Un dispositivo de acuerdo con cualquiera de las reivindicaciones 19 a 22, que comprende además un módulo de comunicaciones para enviar y/o recibir, a través de una red de comunicaciones, uno o más del mensaje (M), la clave pública maestra de primer nodo (P_{1C}), la clave pública maestra de segundo nodo (P_{1S}), el primer mensaje firmado (SM1), el segundo mensaje firmado (SM2), el aviso indicativo de utilizar un sistema de criptografía de curva elíptica (ECC) con un generador común (G).

24. Un sistema para la determinación de un secreto común entre un primer nodo (C) y un segundo nodo (S), en donde:

- el primer nodo (C) está asociado con un primer par de criptografía asimétrica que tiene una clave privada maestra de primer nodo (V_{1C}) y una clave pública maestra de primer nodo (P_{1C}); y

- el segundo nodo (S) está asociado con un segundo par de criptografía asimétrica que tiene una clave privada maestra de segundo nodo (V_{1S}) y una clave pública maestra de segundo nodo (P_{1S}) y el sistema comprende:

- un primer dispositivo de procesamiento, asociado con el primer nodo (C), configurado para:

- determinar una segunda clave privada de primer nodo (V_{2C}) con base en por lo menos la clave privada maestra de primer nodo (V_{1C}) y una clave determinista (DK);

- determinar una segunda clave pública de segundo nodo (P_{2S}) con base en por lo menos la clave pública maestra de segundo nodo (P_{1S}) y la clave determinista (DK); y

- determinar el secreto común (CS) con base en la segunda clave privada de primer nodo (V_{2C}) y la segunda clave pública de segundo nodo (P_{2S}); y

- un segundo dispositivo de procesamiento, asociado con el segundo nodo (S), configurado para:

- determinar una segunda clave pública de primer nodo (P_{2C}) con base en por lo menos la clave pública maestra de primer nodo (P_{1C}) y la clave determinista (DK); y

- determinar una segunda clave privada de segundo nodo (V_{2S}) con base en por lo menos la clave privada maestra de segundo nodo (V_{1S}) y la clave determinista (DK); y

- determinar el secreto común con base en la segunda clave pública de primer nodo (P_{2C}) y una segunda clave privada de segundo nodo (V_{2S}),

en donde el primer dispositivo de procesamiento y el segundo dispositivo de procesamiento determinan el mismo secreto común.

25. El sistema de acuerdo con la reivindicación 24, caracterizado porque la clave determinista (DK) se basa en un mensaje (M) y el primer dispositivo de procesamiento está configurado además para:

- generar un primer mensaje firmado (SM1) con base en el mensaje (M) y la segunda clave privada de primer nodo (V_{2C}); y

- enviar, a través de la red de comunicaciones, el primer mensaje firmado (SM1) al segundo nodo (S),

en donde el segundo dispositivo de procesamiento está configurado además para:

- recibir el primer mensaje firmado (SM1);
- validar el primer mensaje firmado (SM1) con la segunda clave pública de primer nodo (P_{2C}); y
- autenticar el primer nodo (C) con base en un resultado del primer mensaje firmado (SM1) validado.

26. El sistema de acuerdo con cualquiera de la reivindicación 25, caracterizado porque el segundo dispositivo de procesamiento está configurado además para:

- generar un segundo mensaje firmado (SM2) con base en el mensaje (M), o un segundo mensaje (M2) y la segunda clave privada de segundo nodo (V_{2S}); y

- enviar el segundo mensaje firmado (SM2) al primer nodo (C),

en donde el primer dispositivo de procesamiento está configurado además para:

- recibir el segundo mensaje firmado (SM2);
- validar el segundo mensaje firmado (SM2) con la segunda clave pública de segundo nodo (P_{2S}); y

- autenticar el segundo nodo (S) con base en un resultado del segundo mensaje firmado (SM2) validado.

27. El sistema de acuerdo con la reivindicación 25 o 26, caracterizado porque el primer dispositivo de procesamiento está configurado para:

- generar el mensaje (M); y

- enviar el mensaje (M),

en donde el segundo dispositivo de procesamiento está configurado para:

- recibir el mensaje (M).

28. El sistema de acuerdo con la reivindicación 25 o 26, caracterizado porque el mensaje es generado por otro nodo, en donde el primer dispositivo de procesamiento está configurado para:

- recibir el mensaje (M),

en donde el segundo dispositivo de procesamiento está configurado para:

- recibir el mensaje (M).

29. El sistema de acuerdo con cualquiera de las reivindicaciones 25 a 28, que comprende además un almacén de datos de sistema e/o interfaz de entrada, en donde el primer dispositivo de procesamiento y el segundo dispositivo de procesamiento reciben el mensaje (M), o el segundo mensaje (M2) procedente del almacén de datos de sistema e/o interfaz de entrada.

30. El sistema de acuerdo con la reivindicación 29, caracterizado porque el primer dispositivo de procesamiento recibe la clave pública maestra de segundo nodo (P_{1S}) procedente del almacén de datos de sistema y/o dispositivo de entrada y el segundo dispositivo de procesamiento recibe la clave pública maestra de primer nodo (P_{1C}) procedente del almacén de datos de sistema y/o dispositivo de entrada.

31. El sistema de acuerdo con cualquiera de las reivindicaciones 24 a 30, caracterizado porque la clave pública maestra de primer nodo (P_{1C}), la clave pública maestra de segundo nodo (P_{1S}) se basan en una multiplicación de puntos de curva elíptica de clave privada maestra de primer nodo (V_{1C}) y clave privada maestra de segundo nodo (V_{1S}) respectivas y un generador (G).

32. El sistema de acuerdo con cualquiera de las reivindicaciones 24 a 31, que comprende además:

- un primer almacén de datos asociado con el primer nodo (C) para almacenar la clave privada maestra de primer nodo (V_{1C}); y
- un segundo almacén de datos asociado con el segundo nodo (S) para almacenar la clave privada maestra de segundo nodo (V_{1S}).

33. El sistema de acuerdo con la reivindicación 32, caracterizado porque el primer dispositivo de procesamiento está configurado para:

- generar la clave privada maestra de primer nodo (V_{1C}) y la clave pública maestra de primer nodo (P_{1C});

- enviar la clave pública maestra de primer nodo (P_{1C}); y

- almacenar la clave privada maestra de primer nodo (V_{1C}) en el primer almacén de datos,

en donde el segundo dispositivo de procesamiento está configurado para:

- generar la clave privada maestra de segundo nodo (V_{1S}) y la clave pública maestra de segundo nodo (P_{1S});

- enviar la clave pública maestra de segundo nodo (P_{1S}); y

- almacenar la clave privada maestra de segundo nodo (V_{1S}) en el segundo almacén de datos.

34. El sistema de acuerdo con la reivindicación 32 o 33, caracterizado porque:

- el primer almacén de datos recibe y almacena la clave pública maestra de segundo nodo (P_{1S}); y

- el segundo almacén de datos recibe y almacena la clave pública maestra de primer nodo (P_{1C}).

35. El sistema de acuerdo con cualquiera de las reivindicaciones 24 a 34, caracterizado porque el primer dispositivo de procesamiento está configurado además para:

- generar la clave privada maestra de primer nodo (V_{1C}) con base en un número entero aleatorio en un intervalo permisible especificado en un sistema de criptografía de curva elíptica (ECC) común; y
- determinar la clave pública maestra de primer nodo (P_{1C}) con base en una multiplicación de puntos de curva elíptica de la clave privada maestra de primer nodo (V_{1C}) y un generador común (G) de acuerdo con la fórmula:

$$P_{1C} = V_{1C} \times G$$

Y en donde el segundo dispositivo de procesamiento está configurado además para:

- generar la clave privada maestra de segundo nodo (V_{1S}) con base en un número entero aleatorio en el intervalo permisible especificado en el sistema ECC común; y
- determinar la clave pública maestra de segundo nodo (P_{1S}) con base en una multiplicación de puntos de curva elíptica de la clave privada maestra de segundo nodo (V_{1S}) y el generador común (G) de acuerdo con la fórmula:

$$P_{1S} = V_{1S} \times G$$

36. El sistema de acuerdo con cualquiera de las reivindicaciones 25 a 35, caracterizado porque el primer dispositivo de procesamiento está configurado para:

- determinar la clave determinista (DK) con base en un hash (función de resumen) del mensaje (M), y en donde:
 - la segunda clave privada de primer nodo (V_{2C}) se basa en una adición escalar de la clave privada maestra de primer nodo (V_{1C}) y la clave determinista (DK) de acuerdo con la fórmula:

$$V_{2C} = V_{1C} + DK; \text{ y}$$

- la segunda clave pública de segundo nodo (P_{2S}) se basa en la clave pública maestra de segundo nodo (P_{1S}) con una adición de puntos de curva elíptica a la multiplicación de puntos de curva elíptica de la clave determinista (DK) y el generador común (G) de acuerdo con la siguiente fórmula:

$$P_{2S} = P_{1S} + DK \times G$$

y en donde el segundo dispositivo de procesamiento está configurado para:

- determinar la clave determinista (DK) con base en un hash (función de resumen) del mensaje (M), y en donde:
 - la segunda clave privada de segundo nodo (V_{2S}) se basa en una adición escalar de la clave privada maestra de segundo nodo (V_{1S}) y la clave determinista (DK) de acuerdo con la fórmula:

$$V_{2S} = V_{1C} + DK; y$$

- la clave pública de primer nodo (P_{2C}) se basa en la clave pública maestra de primer nodo (P_{1C}) con una adición de puntos de curva elíptica a la multiplicación de puntos de curva elíptica de la clave determinista (DK) y el generador común (G) de acuerdo con la siguiente fórmula:

$$P_{2C} = P_{1C} + DK \times G$$

37. Un sistema de acuerdo con cualquiera de las reivindicaciones 24 a 36, que comprende además:

- un primer módulo de comunicaciones asociado con el primer dispositivo de procesamiento para enviar y/o recibir, a través de una red de comunicaciones, uno o más del mensaje (M), la clave pública maestra de primer nodo (P_{1C}), la clave pública maestra de segundo nodo (P_{1S}), el primer mensaje firmado (SM1), el segundo mensaje firmado (SM2) y un aviso indicativo de utilizar un sistema de criptografía de curva elíptica (ECC) común con un generador (G); y
- un segundo módulo de comunicaciones asociado con el segundo dispositivo de procesamiento para enviar y/o recibir, a través de una red de comunicaciones, uno o más del mensaje (M), la clave pública maestra de primer nodo (P_{1C}), la clave pública maestra de segundo nodo (P_{1S}), el primer mensaje firmado (SM1), el segundo mensaje firmado (SM2) y el aviso indicativo de utilizar un sistema de criptografía de curva elíptica (ECC) común con un generador (G).

38. Un sistema de acuerdo con cualquiera de las reivindicaciones 24 a 37, caracterizado porque la clave determinista (DK) se basa en la determinación de un hash (función de resumen) de una clave determinista previa.

39. Un método de acuerdo con cualquiera de las reivindicaciones 24 a 38, caracterizado porque el primer par de criptografía asimétrica y el segundo par de criptografía asimétrica se basan en una función de primer par de criptografía asimétrica previo y segundo par de criptografía asimétrica previo respectivos.

40. Un sistema para la comunicación segura entre un primer nodo y un segundo nodo con algoritmo de clave simétrica, en donde el sistema comprende:

- un sistema de acuerdo con cualquiera de las reivindicaciones 24 a 39 para determinar un secreto común con el primer dispositivo de procesamiento y el segundo dispositivo de procesamiento, en donde el primer dispositivo de procesamiento está configurado además para:

- determinar una clave simétrica con base en el secreto común;
- encriptar un primer mensaje de comunicación, con la clave simétrica, en un primer mensaje de comunicación encriptado; y
- enviar el primer mensaje de comunicación encriptado;

en donde el segundo dispositivo de procesamiento está configurado además para:

- determinar la misma clave simétrica con base en el secreto común;

- recibir el primer mensaje de comunicación encriptado; y
- desencriptar el primer mensaje de comunicación encriptado, con la clave simétrica, en el primer mensaje de comunicación.

41. Un sistema para la comunicación segura entre un primer nodo y un segundo nodo con algoritmo de clave simétrica, en donde el segundo dispositivo de procesamiento está configurado además para:

- encriptar un segundo mensaje de comunicación, con la clave simétrica, en el segundo mensaje de comunicación encriptado; y

- enviar el segundo mensaje de comunicación encriptado;

en donde el primer dispositivo de procesamiento está configurado además para:

- recibir el segundo mensaje de comunicación encriptado;
- desencriptar el segundo mensaje de comunicación encriptado, con la clave simétrica, en el segundo mensaje de comunicación.

42. Un sistema de acuerdo con la reivindicación 40 o 41, caracterizado porque el primer y el segundo mensaje de comunicación son mensajes de transacción entre el primer nodo y el segundo nodo para una transacción en línea entre el primer nodo y el segundo nodo.

43. Un programa de computadora que comprende instrucciones legibles por máquina para hacer que un dispositivo de procesamiento implemente el método de acuerdo con cualquiera de las reivindicaciones 1 a 18.