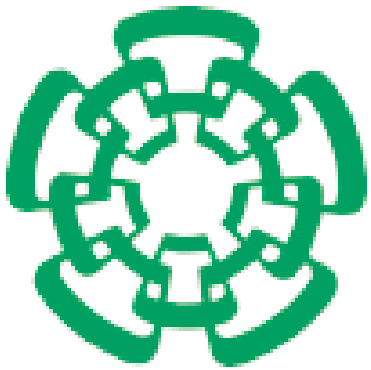
Sobre el diseño de sistemas de votación electrónica seguros

Francisco Rodríguez-Henríquez



Cuarta Semana Nacional de Ciberseguridad, 24 de octubre de 2018

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

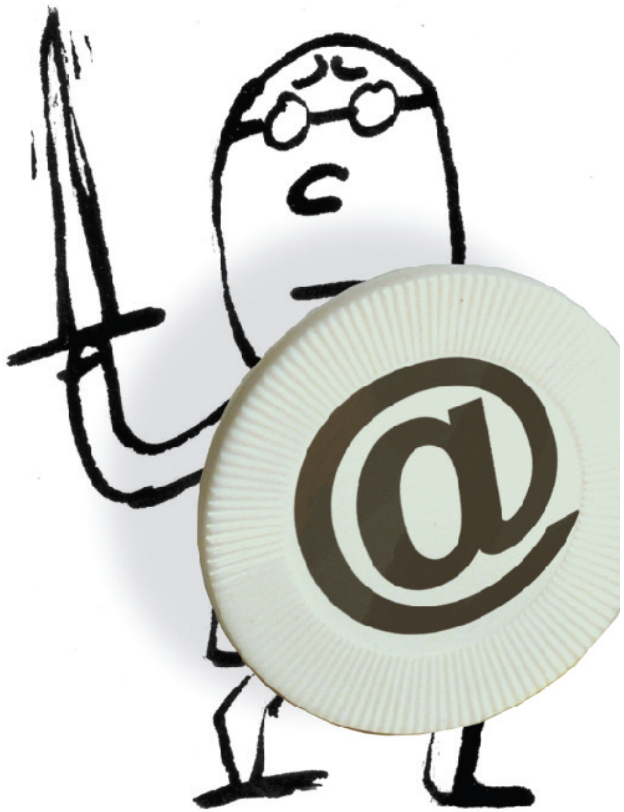
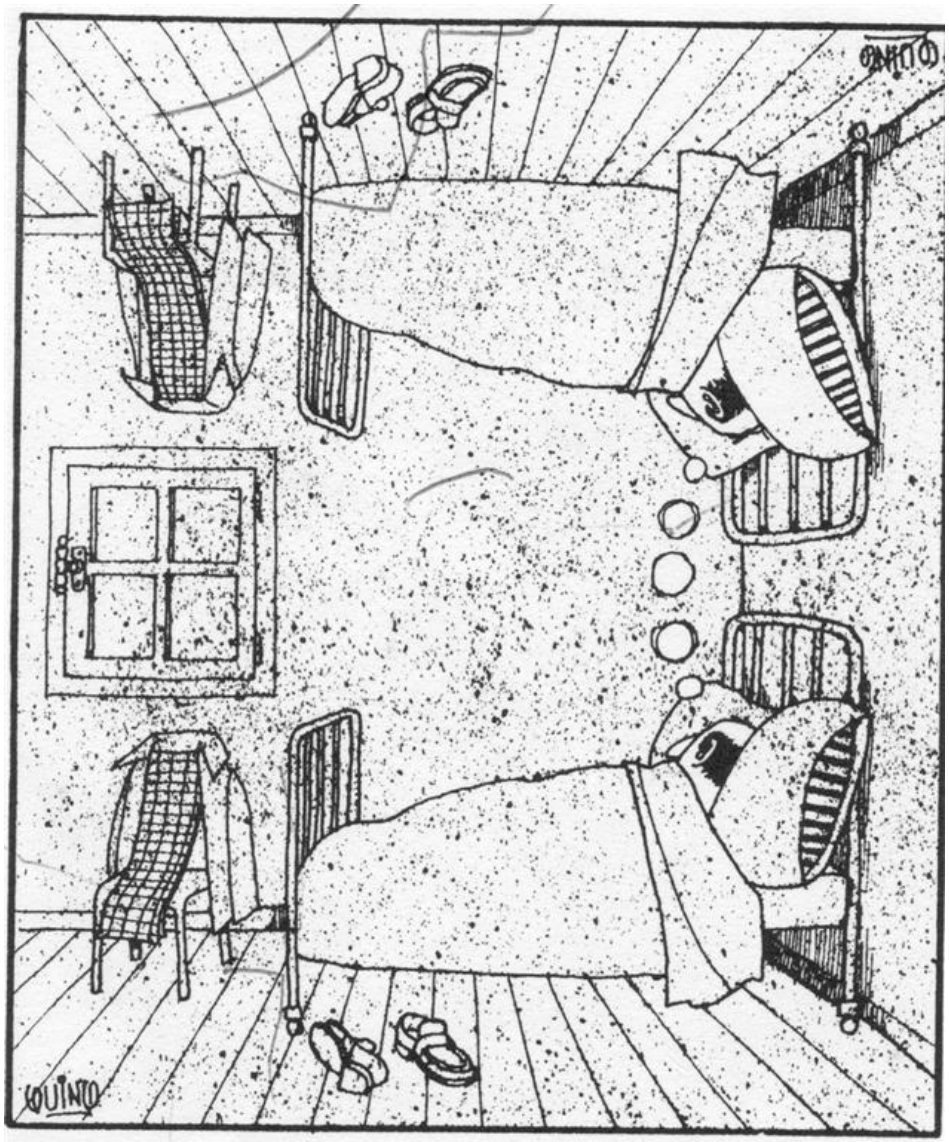


Figure: Tercera ley: Típicamente la criptografía no es vulnerada sino más bien brincada

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]

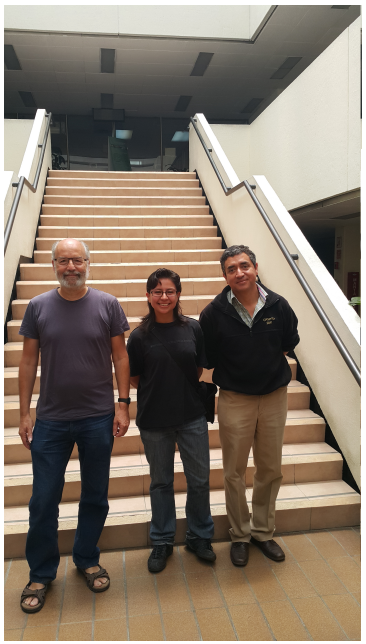
Primitivas y bloques básicos fundamentales en criptografía moderna

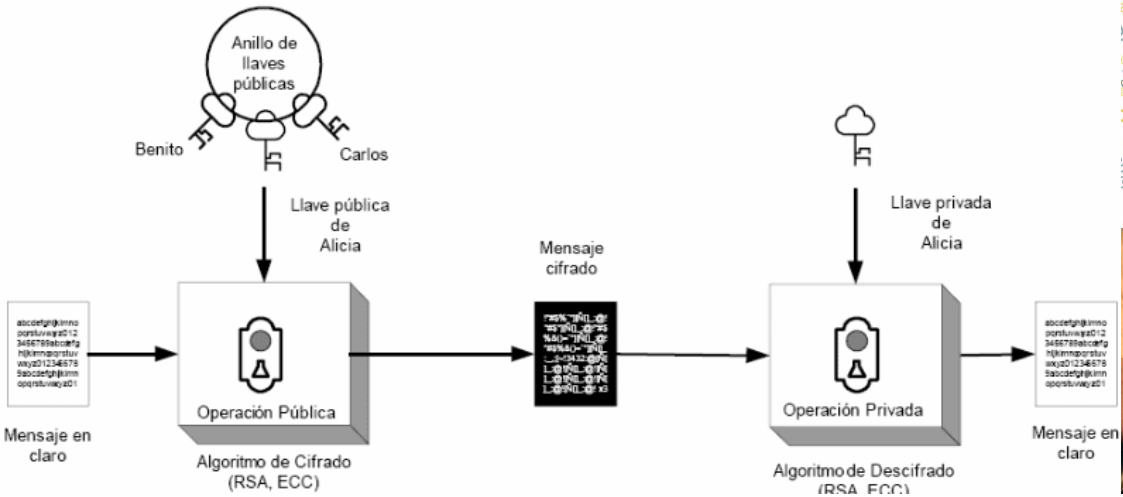
- Primitivas:
  - Cifrado/descifrado de documentos digitales [típicamente se resuelve utilizando criptografía de llave secreta]
  - Establecimiento de un secreto compartido entre dos entidades [se resuelve invocando al protocolo Diffie-Hellman]
  - Firma/verificación de documentos digitales [típicamente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

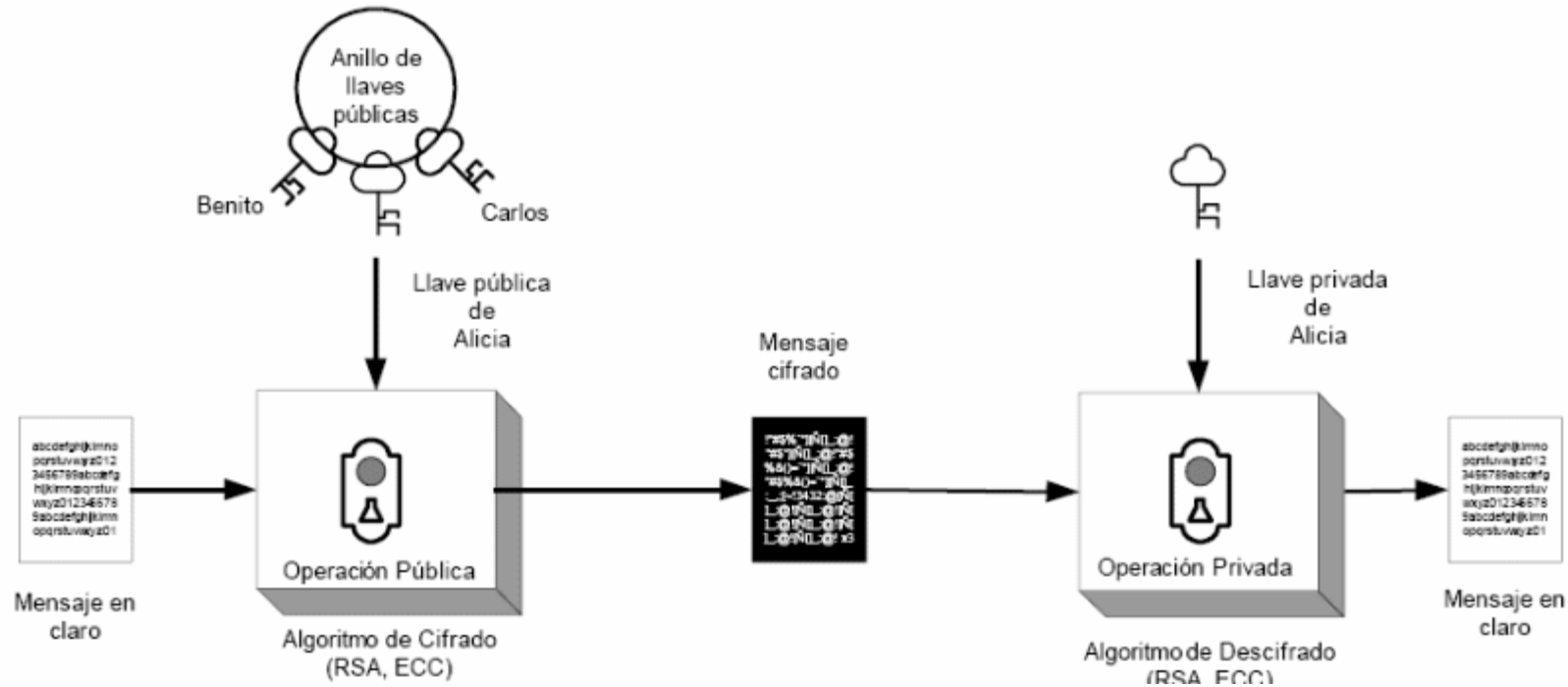
Criptografía de llave pública





- Conceptualmente, fue inventada en 1976 por Diffie y Hellman.
- En 1977 (¡Hace 41 años!) se inventa el primer criptosistema de llave pública RSA.
- Notas históricas:
  - Rivest-Shamir-Addleman utilizaron un teorema publicado hace más de 300 años por el gran matemático ciego Leonhard Euler
  - Rivest-Shamir-Addleman recibieron el premio Turing 2002 debido a esta invención

Criptografía de llave pública



Sistemas de voto electrónico

Voto Electrónico: Primeras propuestas

- Las primeras construcciones de sistemas de voto electrónicos fueron planteadas por David Chaum en los años ochentas del siglo pasado
- Para la realización de estos cripto-sistemas, Chaum propuso utilizar una primitiva criptográfica conocida como firmas a ciegas

Voto Electrónico: Primeras propuestas

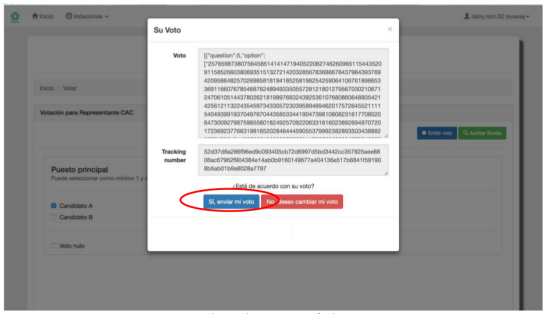
[1]

[1] Dra. María de Lourdes López García, "Diseño de un protocolo para votaciones electrónicas basado en firmas a ciegas definidas sobre emparejamientos bilineales", junio de 2011, Supervisor: Dr. Francisco Rodríguez Henríquez.

Clasificación de sistemas de voto electrónico

- Sistemas de votación electrónica (E-Voto): Suelen estar circunscritos a la instalación de urnas electrónicas por parte de la autoridad a cargo del proceso electoral
- el único componente digital en un sistema de E-Voto es la urna electrónica, mientras que los otros elementos en la votación se implementan de una manera tradicional.
- Los electores deben votar de manera personal y no por internet.

Clasificación de sistemas de voto electrónico



- Sistemas de votación por Internet (I-Voto): Permite que los electores puedan emitir su voto desde cualquier ubicación haciendo uso de computadoras o dispositivos móviles con conexión a internet, con lo que los electores puedan participar en el proceso electoral sin necesidad de acudir personalmente a los recintos electorales.
- Las boletas digitales asociadas a este esquema permiten ahorrar papel y minimizar la intervención de seres humanos en la administración del sistema.

Características de seguridad informática que deben de ser satisfechas por sistemas de votación electrónica

Los sistemas de votación electrónica deben garantizar los siguientes servicios de seguridad:

- **Privacidad o anonimato del votante**: No deberá ser posible que ninguna entidad relacione al votante con el valor de su voto.

Características de seguridad informática que deben de ser satisfechas por sistemas de votación electrónica

Los sistemas de votación electrónica deben garantizar los siguientes servicios de seguridad:

- **Autenticación**: Sólo los votantes válidos podrán sufragar su voto.

Características de seguridad informática que deben de ser satisfechas por sistemas de votación electrónica

Los sistemas de votación electrónica deben garantizar los siguientes servicios de seguridad:

- **Verificación**: Cada votante podrá comprobar que su voto fue correctamente contabilizado.

Características de seguridad informática que deben de ser satisfechas por sistemas de votación electrónica

Los sistemas de votación electrónica deben garantizar los siguientes servicios de seguridad:

- **Integridad**: El valor del voto capturado por el sistema deberá ser el mismo que aquel emitido por el votante.

Características de seguridad informática que deben de ser satisfechas por sistemas de votación electrónica

Los sistemas de votación electrónica deben garantizar los siguientes servicios de seguridad:

- **Exactitud**: El sistema no permitirá que votos inválidos sean contados, ni que votos válidos no estén incluidos en los resultados finales.

Características de seguridad informática que deben de ser satisfechas por sistemas de votación electrónica

Los sistemas de votación electrónica deben garantizar los siguientes servicios de seguridad:

- **Simplicidad**: Los votantes podrán emitir su voto de forma rápida y con un mínimo de conocimientos técnicos.

Características de seguridad informática que deben de ser satisfechas por sistemas de votación electrónica

Los sistemas de votación electrónica deben garantizar los siguientes servicios de seguridad:

- **Flexibilidad**: El sistema deberá ser compatible con diversos sistemas operativos, plataformas, dispositivos digitales y tecnologías.

Características de seguridad informática que deben de ser satisfechas por sistemas de votación electrónica

Los sistemas de votación electrónica deben garantizar los siguientes servicios de seguridad:

- **Detección de votos duplicados**: El sistema deberá ser capaz de detectar si un votante ha emitido su voto en más de una ocasión, así como de conocer la identidad del votante tramposo.

Características de seguridad informática que deben de ser satisfechas por sistemas de votación electrónica

Los sistemas de votación electrónica deben garantizar los siguientes servicios de seguridad:

- **Transparencia**: Los votantes deberán contar con un conocimiento razonable del proceso de votación.

Características de seguridad informática que deben de ser satisfechas por sistemas de votación electrónica

Los sistemas de votación electrónica deben garantizar los siguientes servicios de seguridad:

- **Equidad**: Ninguna entidad podrá obtener ningún resultado parcial mientras se lleva a cabo el proceso de votación.

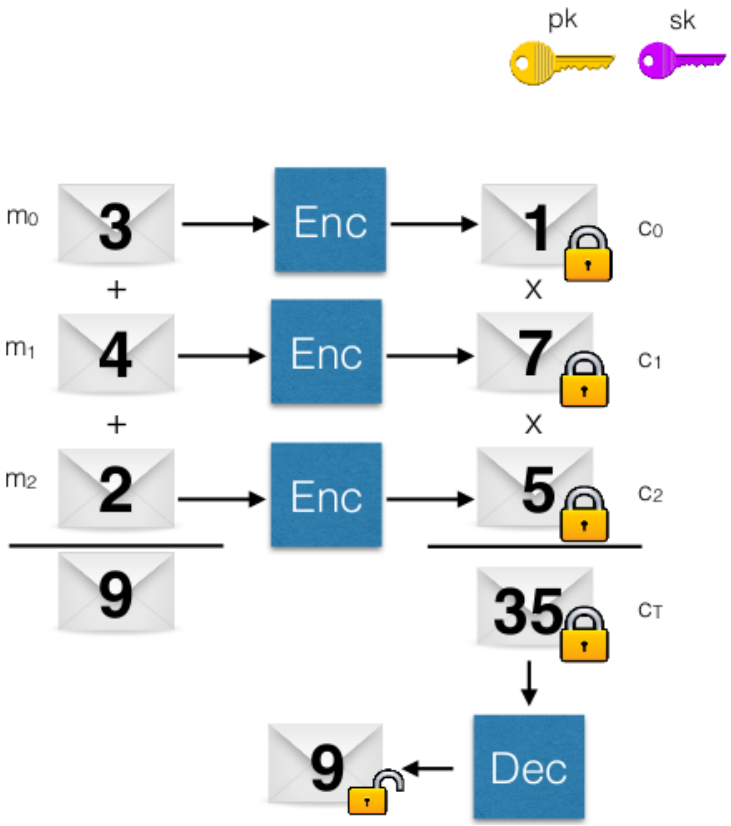
Características de seguridad informática que deben de ser satisfechas por sistemas de votación electrónica

Los sistemas de votación electrónica deben garantizar los siguientes servicios de seguridad:

- **Auditoría**: Cualquier entidad podrá determinar si se llevaron a cabo todas las etapas de votación de manera correcta. Se suelen considerar dos tipos de auditorías: auditoría individual, en la cual cada uno de los participantes puede verificar si su propio voto fue contado adecuadamente, y la auditoría universal, en la cual una entidad cualquiera puede verificar algunas fases de la elección o inclusive todo el proceso de votación.

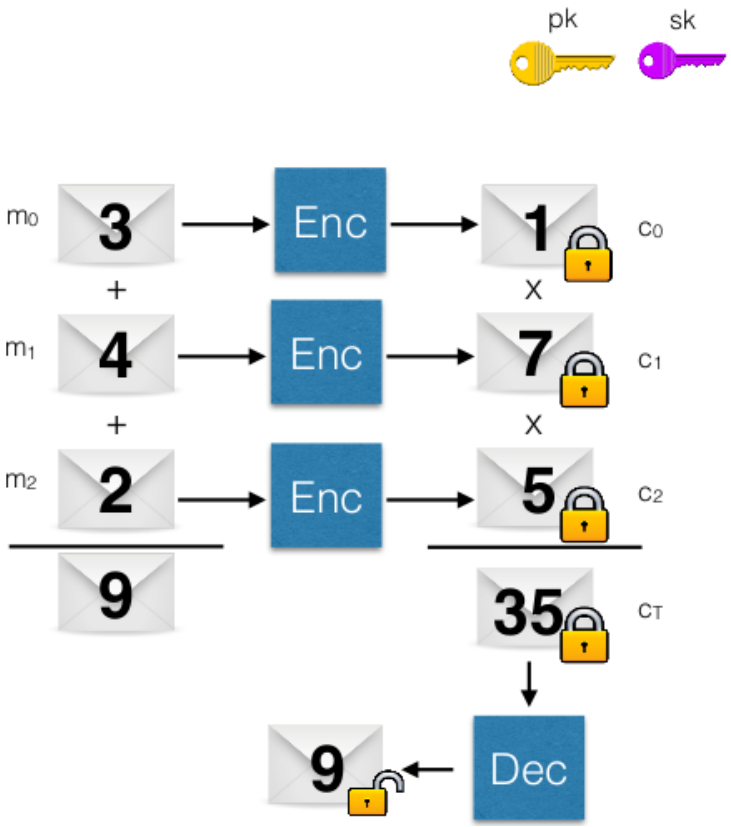
Caso de Estudio: Sistema de I-voto FIDELIS

Características de seguridad informática provistas por FIDELIS



Para asegurar la secrecía de los votos, FIDELIS utiliza el cripto-esquema de Paillier de cifrado homomórfico. Ello permite que el servidor de votos de FIDELIS reciba votos cifrados los cuales no puede leer

Características de seguridad informática provistas por FIDELIS



FIDELIS utiliza llaves pública/privada de 1024 bits (equivalentes a aproximadamente 310 dígitos decimales)

Características funcionales de FIDELIS

- El voto puede ser enviado desde cualquier dispositivo con conexión a Internet: computadoras personales, teléfonos celulares, tabletas, etc.

Características funcionales de FIDELIS

- Para enviar su voto, el elector puede utilizar su Navegador preferido: Chrome, Firefox, Safari, Microsoft explorer, etc. Sin embargo FIDELIS ha sido optimizado para ser utilizado con el navagador Chrome

Características funcionales de FIDELIS

- Cada voto es enviado desde el dispositivo del elector hasta el servidor de votos de FIDELIS de manera cifrada. El cripto-esquema utilizado por FIDELIS utiliza llaves pública/privada de un tamaño de 1024 bits (unos 310 dígitos decimales)

Características funcionales de FIDELIS

- FIDELIS le entraga a cada elector un recibo de su voto. Posteriormente, en la fase de "develación de resultados", dicho recibo puede ser utilizado por el elector para verificar que su voto sí fue contabilizado.

Características funcionales de FIDELIS

- FIDELIS envía correos electrónicos a todos los miembros del padrón electoral para informarles del inicio/finalización de cada fase de la elección. En particular, cada votante recibirá un enlace donde podrá consultar los resultados finales de la elección, número de votos recibidos, número de correos electrónicos considerados, etc.

Dramatis personae: Trustee

Encargado de generar las llaves maestras de cifrado y descifrado de votos. Sus roles principales ocurren en la primera fase: "Generación de llaves" y en la última fase: "Develación de resultados" del proeso electoral.

Dramatis personae: Administrador

Encargado de configurar la votación mediante la definición de:

- Padrón electoral
- Boleta electoral y calendario de votación
- Sellado de la elección

Asimismo el administrador inicia la votación y la finaliza de acuerdo al calendario especificado durante la configuración del proceso electoral.

Dramatis personae: Votante

Personas con derecho a voto. Durante la fase de votación FIDELIS envía un correo electrónico a cada votante incluido en el padrón electoral. En este correo electrónico se incluye un enlace para acceder a la boleta electoral en la que el elector pueda enviar su voto de manera cifrada al servidor de conteo de FIDELIS

Fases de votación en FIDELIS

1. Fase de generación de llaves [a cargo del trustee]

Fases de votación en FIDELIS

1. Fase de generación de llaves [a cargo del trustee]
2. Fase de configuración de la elección [a cargo del administrador o coordinador]

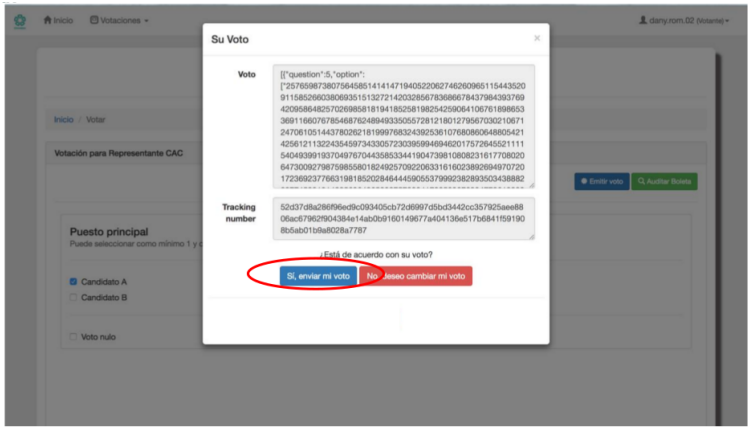
Fases de votación en FIDELIS

1. Fase de generación de llaves [a cargo del trustee]
2. Fase de configuración de la elección [a cargo del administrador o coordinador]
   - Configuración del padrón electoral
   - Configuración de la boleta electoral y calendario de votación
   - Sellado de la elección
3. Fase de votación [el inicio y finalización de esta fase está a cargo del administrador o coordinador]

Fases de votación en FIDELIS

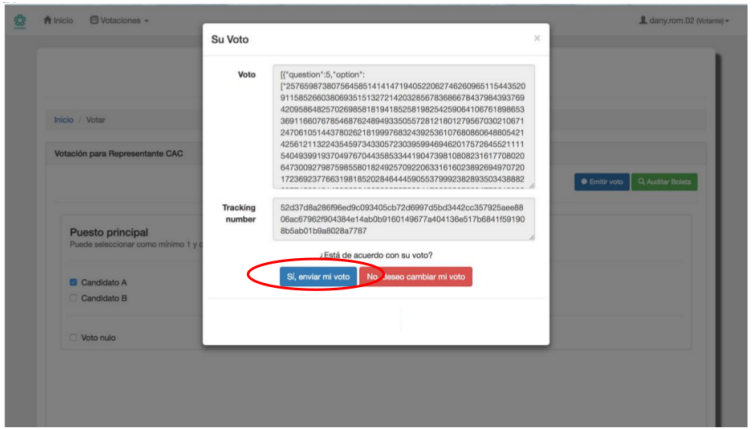
1. Fase de generación de llaves [a cargo del trustee]
2. Fase de configuración de la elección [a cargo del administrador o coordinador]
   - Configuración del padrón electoral
   - Configuración de la boleta electoral y calendario de votación
   - Sellado de la elección
3. Fase de votación [el inicio y finalización de esta fase está a cargo del administrador o coordinador]
4. Fase de develación de los resultados [a cargo del trustee]

Resumen de características funcionales de FIDELIS



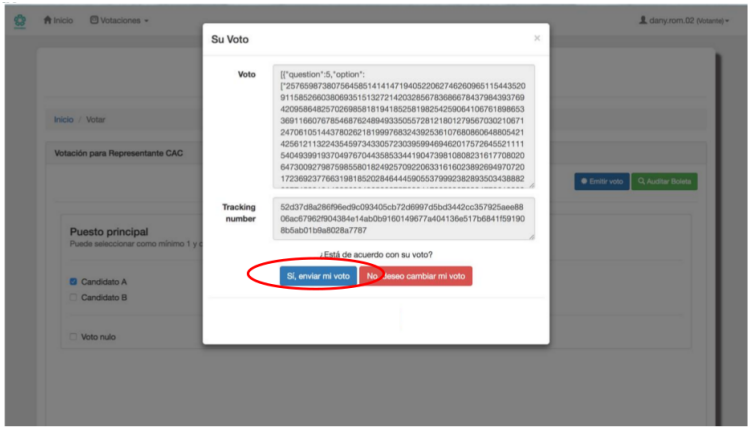
- El voto puede ser enviado desde cualquier dispositivo con conexión a Internet: computadoras personales, teléfonos celulares, tabletas, etc.

Resumen de características funcionales de FIDELIS



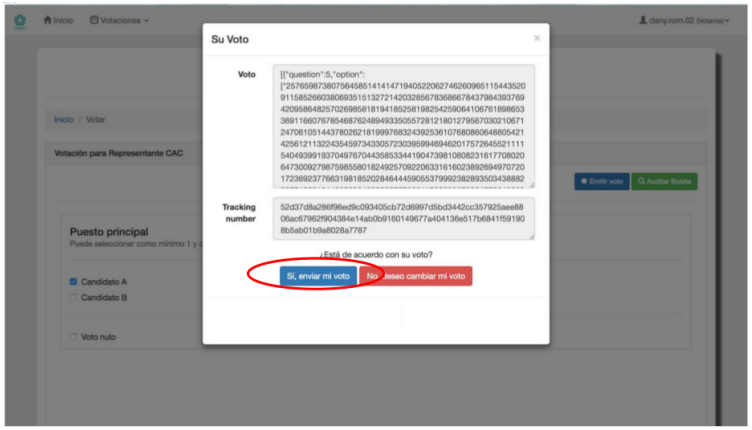
- Para enviar su voto, el elector puede utilizar su Navegador preferido: Chrome, Firefox, Safari, Microsoft explorer, etc. Sin embargo FIDELIS ha sido optimizado para ser utilizado con el navagador Chrome

Resumen de características funcionales de FIDELIS



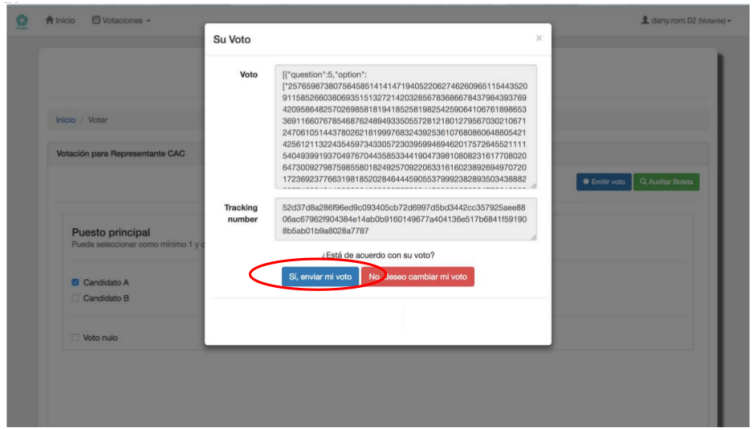
- Cada voto es enviado desde el dispositivo del elector hasta el servidor de votos de FIDELIS de manera cifrada. El cripto-esquema utilizado por FIDELIS utiliza llaves pública/privada de un tamaño de 1024 bits (unos 310 dígitos decimales)

Resumen de características funcionales de FIDELIS



- FIDELIS le entraga a cada elector un recibo de su voto. Posteriormente, en la fase de "develación de resultados", dicho recibo puede ser utilizado por el elector para verificar que su voto sí fue contabilizado.

Resumen de características funcionales de FIDELIS



- FIDELIS envía correos electrónicos a todos los miembros del padrón electoral para informarles del inicio/finalización de cada fase de la elección. En particular, cada votante recibirá un enlace donde podrá consultar los resultados finales de la elección, número de votos recibidos, número de correos electrónicos considerados, etc.

Gracias