Buenas prácticas en e-Democracy e i-Voting. Nociones básicas de criptografía.

Carlos Rossique

Preámbulo y extracto

Los avances tecnológicos en las tecnologías de la información y comunicación (TICs) incluyendo su gran impacto en las áreas de seguridad y criptografía, hoy hacen posible sistemas más fiables y seguros de democracia digital, impensables hace unas décadas, que pueden poner de manifiesto la voluntad de conjuntos humanos de una manera más participativa y frecuente.

La ley de la fractura impone que los avances tecnológicos son seguidos por un retraso creciente en las esferas sociales, empresariales y políticas, respectivamente. Pero, brecha digital mediante, hoy se están dando cada vez más casos de aplicación de estas tecnologías y se generalizan consultas y votaciones electrónicas incluso en la esfera política, donde comienzan a ser frecuentes procesos de primarias, votación de documentos etc. incluyendo más o menos también la participación presencial.

Sin embargo, si hablamos específicamente de voto electrónico, según muchos observadores se está aún muy lejos de conseguir aplicaciones 100% seguras, y menos cuando hablamos de voto por internet, debido a la aparente contradicción de requisitos respecto a la integridad y privacidad de los votos, tema del que hablaremos más adelante.

Capítulo aparte merece el tema de la comprobación de identidad de votantes y la robustez ante suplantaciones, votos duplicados etc., que exigen certificación de identidad y control de censo, en su caso.

Dado que estamos en un área donde hasta ahora hay pocos ejemplos, nos parece un buen momento para plantear un código de buenas prácticas deseables, no sólo desde el punto de vista técnico, en su mayoría entendible exclusivamente por los expertos en la materia, sino también haciendo hincapié en los aspectos de comunicación, explicando los procesos en un lenguaje pedagógico y asequible al conjunto de los votantes y observadores.

En este breve trabajo, se enumeran algunas características deseables, en opinión del autor, en función de la seguridad, de la verificabilidad y sobre todo de la transparencia de estos procesos de democracia digital, enfocándose en e-voting. Por supuesto que hay otra gran rama de la democracia digital en la que no es tan importante la privacidad, como son las aplicaciones orientadas a propuestas, construcción de programa, etc, pero de momento nos vamos a circunscribir a la necesidad de privacidad.

El problema de la democracia digital y el voto por internet

A estas alturas, tras el desarrollo de múltiples soluciones de democracia digital en todo el mundo, es ampliamente sabido que el principal problema reside en la aparente contradicción de términos entre dos importantes requisitos exigibles a las votaciones.

Integridad ←→ Privacidad

Mientras que el requisito de integridad exige que pueda comprobarse por cualquiera (o incluso por el propio votante) que los votos no son manipulados (añadidos, borrados, o cambiados) el secreto de voto exige anonimizar cada voto de tal manera que no pueda rastrearse en qué sentido ha votado cualquier votante, impidiendo así, además, la posible coerción o venta de votos. Esa contradicción es, en dos palabras, la principal fuente de problemas de cualquier votación electrónica.

No hablaremos aquí, al menos de momento, de otro problema contiguo y bastante común, digamos que estaría en segundo lugar, que podría ser la "elegibilidad" (o mejor, quien puede elegir), es decir, quienes pueden votar en cada elección, que implica la construcción y robustez de censos y problemas de certificación de identidad, no repetición del voto, etc. Obviaremos esto por ahora.

Pero antes de seguir, hay que tener en cuenta que existen dos escenarios muy distintos en votación electrónica. Una es la votación en mesas previamente anunciadas y mediante máquinas de voto y el segundo escenario sería la votación en internet (donde cada votante usas su PC o Smartphone para ello). Está claro que el segundo escenario plantea aún más problemas que el primero. Si bien en el primer caso las máquinas necesitan ser securizadas, comprobar que no incluyen malware o incluso pueden afectarse unas a otras, en el voto por internet está el problema añadido de la posible coerción, el robo de credenciales, la suplantación de identidad, o incluso de sitios, los virus o malware y el uso de bots. Además, en el lado del servidor hay que protegerse de ataques que causen denegaciones de servicio, intrusiones e incluso ataques de por parte de los propios administradores, la NSA o el Estado. (Aunque todos estos riesgos en el lado servidor sean comunes a elecciones con máquinas de voto, en el caso de voto por internet es claro que los servidores están más expuestos a algunos riesgos)

Siguiendo con el problema principal, hay varios esquemas o estrategias para atacar, conjuntamente el problema la integridad y privacidad de la votación electrónica. Para hacer la historia corta, las principales cuatro estrategias que se citan comúnmente son la firma ciega, el uso de mix-nets, la compartición de secreto y el cifrado homomórfico (Hay más detalle en los apéndices). El gran problema de todas estas técnicas es que son bastante abstrusas y difícilmente comprendidas por el gran público e incluso por aquellos que tienen ciertos conocimientos de informática y son usuarios de la red.

Así, las complejas operaciones para securizar y anonimizar los votos alejan, también paradójicamente, a la población de la posibilidad de hacer auditoría de todo el proceso, tanto es así que cada vez se escuchan más voces contra el voto electrónico en su conjunto (p.ej: en este enlace

(pdf en castellano) o este otro). Las críticas vienen sobre todo por la dificultad de auditoría, (además, e incluso por encima, de los riesgos contra la privacidad e integridad de los votos) y por la intrusión de la industria privada en sistemas y dispositivos. Así que no se trata simplemente de un par de conceptos antagónicos (privacidad e integridad) a conciliar, sino que nos encontramos con un triángulo donde la transparencia ocupa un vértice importante, si no se quiere que todo eso se base en artículos de fe, porque pareciera que cuanto más "puristas" se vuelven los criterios de privacidad e integridad, más se aleja la transparencia, el control de los votantes y la confianza.

Como punto extremo, son desilusionantes las conclusiones de un serio estudio del sistema de iVoting en Estonia por un grupo de expertos y que pueden leerse aquí. Viene a decir que la tecnología de eVoting aún no está suficientemente madura para cumplir todos los requisitos de integridad, privacidad, verificabilidad y transparencia, mostrando vulnerabilidades de seguridad. Se suele citar la necesidad de verificabilidad E2E (end to end, de cabo a rabo) que suele implicar máquinas de voto y papeletas de voto enmascaradas, como guía para salir de estos sistemas muy complicados para ser superseguros (que al final resulta no lo son) y que nadie entiende como para confiar. Se haría más justicia a la eDemocracy y al eVoting, aplicando estrategias más preocupadas por la sencillez, la transparencia y la cercanía a la ciudadanía

CONDICIONES DE TRANSPARENCIA, INTEGRIDAD, PRIVACIDAD Y OTRAS PARA UNA HERRAMIENTA DE VOTO POR INTERNET:

1) TRANSPARENCIA

Al igual que las elecciones tradicionales, las votaciones electrónicas deben de contar con observadores o interventores durante el proceso, así como la posibilidad de auditorías una vez acabado éste. Procedimientos de auditoría restringidos, inadecuados o insuficiente atención dados al sistema o al diseño del proceso de la votación, producen elecciones abiertas al error y al fraude electoral. Todos los pasos esenciales de la elección deben estar sujetos al control público, mientras otros derechos no justifiquen una excepción. En suma, **el ciudadano debe poder controlar cada paso esencial del acto electoral y la deter-minación del resultado de manera fiable y sin conocimientos técnicos especiales (1.0)**. Así, sería deseable:

Antes de la votación:

- 1.1. Documentación fácilmente accesible del sistema en lenguaje claro y asequible.
- 1.2. Esto incluye requisitos técnicos, cuestiones de elegibilidad, etc

Durante la votación:

- 1.3. Progreso en el número de votos, en detalle por circunscripciones o cortes. (hora, provincia, etc.)

Después de la votación:

- 1.4. Resultados completos del escrutinio incluyendo:

    - Resultados en detalle por campos.
    - Tablas completa de votos.
- Verificabilidad individual del voto y su sentido. (Requisito también asociado a integridad. Este punto es discutible si conviene hacerlo antes y/o después del cierre de la votación.)

RELATIVAS AL CENSO

- 1.5. Datos del censo con cortes por circunscripción (provincia, localidad, etc)
- (4.1). Censo bloqueado durante la votación e incluso un margen de tiempo T antes de la votación.
- (4.2). Si la votación es abierta, criterios claros de inclusión en el censo y medidas anti-duplicidad.

RELATIVAS A LA INTERVENCION

- 1.6. Autoridades e interventores técnicos independientes durante el proceso.
- 1.7. Facilidad para incluirse como interventor para cualquier persona (evidentemente con un límite)

2) INTEGRIDAD

2.1. VERIFICABILIDAD UNIVERSAL

Cualquier observador debe poder ser convencido de que la elección es precisa y que el escrutinio publicado está calculado correctamente a partir de votos correctamente emitidos. Y que los votos no han sido manipulados (añadidos, borrados, o cambiados) por ningún atacante, autoridad o administrador. Normalmente, la integridad y protección ante un administrador "tramposo", es lo más difícil de asegurar.

2.2. VERIFICABILIDAD INDIVIDUAL

Cualquier observador debe poder ser convencido de que su voto ha sido correctamente emitido y contado, y no ha habido manipulación.

2.3. INCOERCIBILIDAD ("*Incoercibility*")

Propiedad que asegura la no existencia de presiones de un agente externo para la imposición o compra del voto a los votantes. Esta propiedad es imposible de asegurar en votaciones por internet (I-voting) ya que si el usuario usa un ordenador para votar no puede asegurarse que alguien físicamente pueda estar viéndole y ejerciendo coerción, **aunque la posibilidad de cambiar el voto posteriormente mitiga en gran parte esta posible coerción** y anula el valor de la posible "venta". En el resto de ocasiones (voto en cabinas, etc.) está relacionada con la imposibilidad de demostrar el sentido del voto imprimiendo un recibo Si no se puede imprimir un comprobante con el sentido del voto en claro ("*receipt freeness*") se hace difícil la coerción.

3) PRIVACIDAD

Todos los votos deben ser secretos y cada voto individual no puede enlazarse al votante que lo emite (exceptuando el propio votante si así lo decidiese, pero sólo para su propia verificación y de nadie más). Nadie debe poder jamás comprobar el sentido de voto de un votante (ni siquiera los administradores) (3.0)

4) ELEGIBILIDAD

Sólo los votantes autorizados, existentes en un censo, pueden votar (4.0). Ningún votante puede emitir más de un voto (4.1). Es necesario asegurar que nadie pueda suplantar la identidad de otro votante. (4.2) En votaciones sin censo (abiertas) sería recomendable asegurar una edad mínima para votar. En realidad ya han sido expresados otros criterios y recomendaciones en el punto de la transparencia

- (1.5). Datos del censo con cortes por circunscripción (provincia, localidad, etc)
- 4.3. Censo bloqueado durante la votación e incluso un margen de tiempo T antes de la votación.
- 4.4. Si la votación es abierta, criterios claros de inclusión en el censo y medidas anti-duplicidad.

5) ROBUSTEZ ANTE ATAQUES Y SEGURIDAD GENÉRICA

Aunque este es un capitulo que puede comprometer a otros (integridad y privacidad) merece un capítulo aparte porque también el sistema ha de ser bastante robusto para estar protegido al menos parcialmente ante ataques de denegación de servicio, “phising”, “sql injection”, y otras vulnerabilidades genéricas del software y hardware involucrado (5.0).

APÉNDICES Y GLOSARIO DE CONCEPTOS ASOCIADOS AL E-VOTING*

A.CONCEPTOS GENERALES

E-VOTING ó VOTO ELECTRONICO

Proceso de votación con el auxilio de herramientas informáticas ya sea para la emisión y captura de los datos del voto como para su recopilación telemática de datos, recuento y escrutinio.

I-VOTING ó VOTO POR INTERNET

En el voto por internet se asegura además la conectividad remota para el votante.

E-DEMOCRACY ó DEMOCRACIA DIGITAL

El concepto de democracia digital es más amplio y va más allá del simple voto; incluye o puede incluir además la deliberación, la elaboración colaborativa de propuestas, la construcción de consenso, la inteligencia colectiva, etc.

FASES DEL PROCESO DE VOTACIÓN:

Fase previa

1) Comunicación y apertura: Comunicación de reglas, opciones y características del proceso.

2) Registro: Previo a la elección para probar la elegibilidad del futuro votante. (El censo puede ser incluso anterior)

Elección propiamente dicha

3) Autenticación: Durante la elección para validar la identidad antes de la emisión del voto.

4) Emisión del voto: Durante la elección, los votantes emiten su voto.

Fases finales

5) Escrutinio: Tras el periodo de votación, se cuentan todos los votos.

6) Comunicación de Resultados: Tras el escrutinio, se comunica el recuento y publica toda la documentación.

TIPOS DE ELECCION

Existe una gran variedad de tipos de elección. Se describen a continuación las más comunes:

- **Sí / No**. El votante debe escoger la respuesta a una pregunta cerrada. (P.ej. consultas ciudadanas)
- **1 de N**. El votante debe escoger una entre N opciones posibles. (Elección de listas o partidos)

- **K de N**. El votante debe escoger (hasta) K (K>1) entre N opciones posibles. (Primarias abiertas)
- **K de N con preferencia**. Se debe escoger preferencialmente (hasta) K (K>1) entre N opciones.
- **N de N con preferencia**. El votante selecciona preferencialmente el total de las opciones.
- **Abierta**. El votante plantea su propia opción de voto o puede ser combinado con otros, p. ej. 1 de N.

B. CRIPTOGRÁFIA BÁSICA

Las principales características de las comunicaciones seguras:

- La **privacidad** se refiere a que la información sólo pueda ser leída por personas autorizadas.
- La **integridad** se refiere a que la información no pueda ser alterada en el transcurso de ser enviada.
- La **autenticidad** se refiere a que se pueda confirmar que el mensaje recibido haya sido mandado por quien dice lo mando o que el mensaje recibido es el que se esperaba.
- El **no rechazo** se refiere a que no se pueda negar la autoría de un mensaje enviado.

Algunas características básicas de las técnicas criptográficas:

La palabra **criptografía** proviene del griego kryptos (esconder) y (gráphein) escribir, es decir, escritura escondida. La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje. Los problemas de seguridad que resuelve la criptografía son los antedichos: privacidad, integridad, autenticación y no rechazo.

La **criptografía simétrica** se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado una clave que es la misma tanto para cifrar como para descifrar. (Es conocida también como criptografía de clave privada) Los algoritmos más usados en esta clase son DES, TDES, RC5, AES [1] (cifrado por bloque) RC4 y SEAL (cifrado bit a bit).

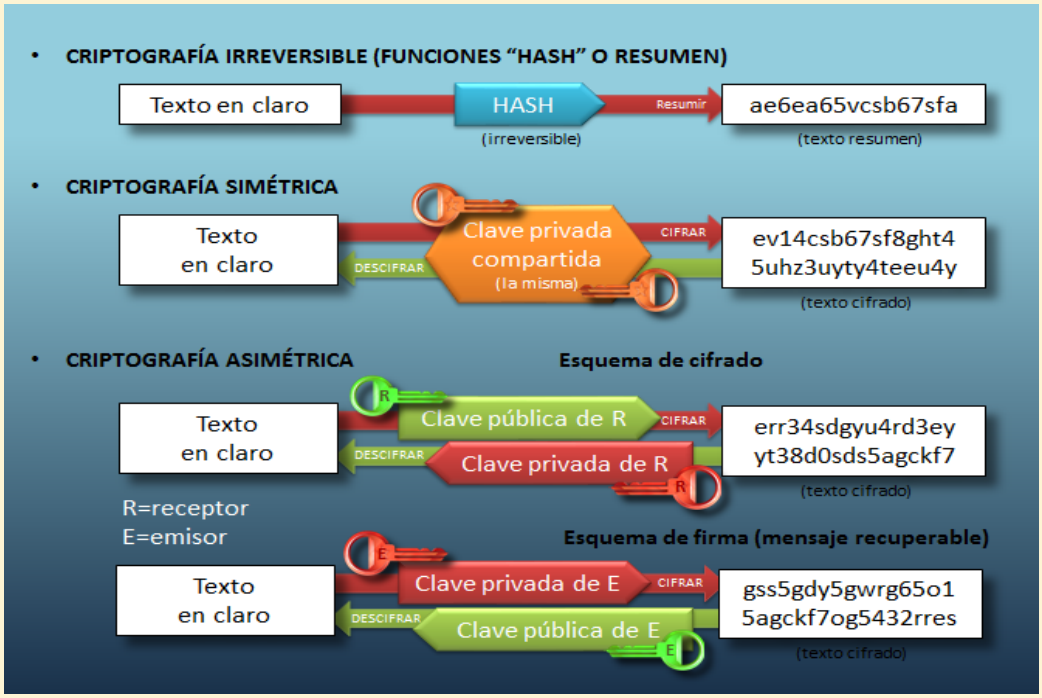
Las **funciones hash** o funciones "resumen" transforman de manera irreversible (no como los cifrados que si son reversibles) un mensaje de longitud arbitraria de forma "única" a un mensaje de longitud constante. Se emplean para asegurar la integridad de un mensaje (MDC) o su autenticidad (MAC). [2]

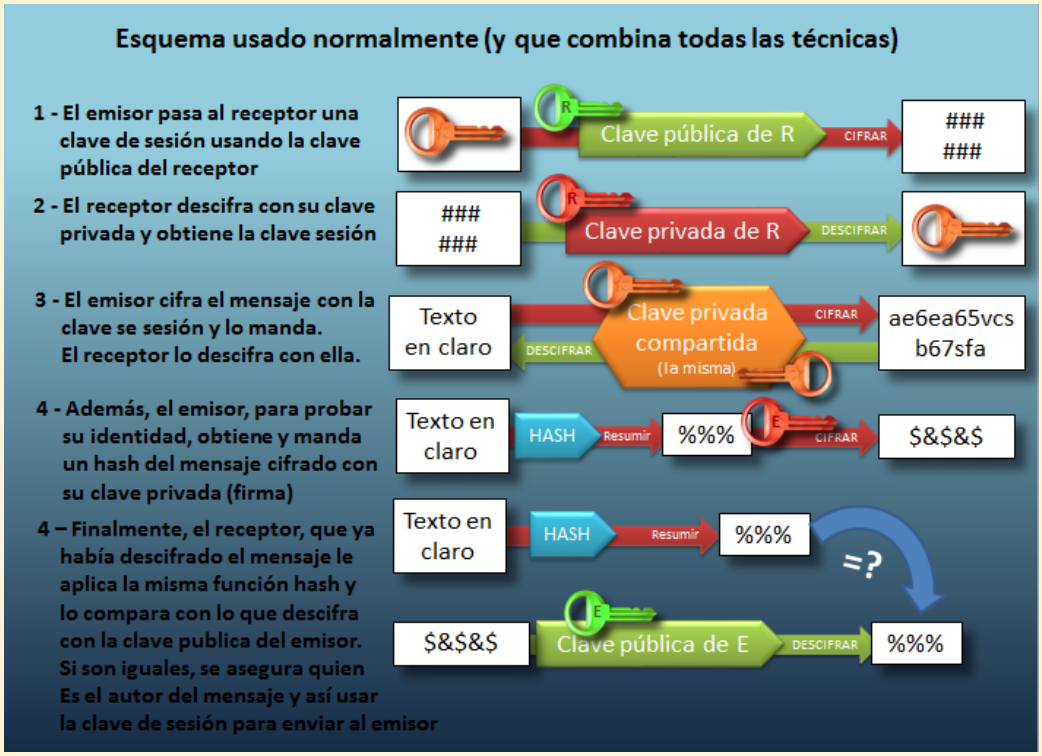
- **Integridad:** Al mensaje se le aplica un MDC (una función hash) y se manda junto con el propio mensaje, al recibirlo el receptor aplica la función hash al mensaje y comprueba que sea igual al hash que se envió antes. La funciones más conocidas de este tipo son MD5, SHA-1, SHA-2, etc.

- **Autenticidad:** Un hash MDC no tiene ningún parámetro adicional, pero un hash MAC usa una clave privada como semilla. Se cifra el mensaje con esa clave y luego se le aplica y envía un hash (MAC) y al llegar a su destino se comprueba que el origen es solo el que tiene la misma clave probando así no sólo la integridad sino también a autenticidad del mensaje. HMAC-SHA-256 es el más conocido.

La **criptografía asimétrica** es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada. (Es conocida también como criptografía de clave pública) Es muy usada y sus dos principales aplicaciones son precisamente el intercambio cifrado de claves privadas simétricas y la firma digital. La más comunes son RSA[3] y CCE[4]

- **Esquema de cifrado:** El mensaje se cifra con la clave pública del destinatario así que sólo él (que dispone de su clave privada) puede descifrarlo.
- **Esquema de firma digital:** El originante firma (cifra) el mensaje con su clave privada. Todo el mundo puede descifrarlo si tiene la clave pública del originante, comprobándose además que sólo él es el origen del mensaje. Ese es un primer esquema (mensaje recuperable) pero es también usual que en la práctica se envía el mensaje M en claro (aquí no se aplica privacidad) y un cifrado (con la clave privada) del hash del mensaje. El destinatario descifra el hash con la clave pública del originante y comprueba que el hash del mensaje M coincide con el que él ha descifrado.





Certificados digitales:

El certificado digital da identidad a una clave pública identificándola como una persona en el espacio cibernético. Surgió para solventar ll problema de administrar las claves públicas y que la identidad del dueño no pueda ser falsificada. La idea es que una tercera entidad (AC) intervenga en la administración de las claves públicas y asegure que las claves públicas tengan asociado un usuario claramente identificado.

Así, las tres partes más importantes de un certificado digital son:

- Una clave pública
- La identidad del implicado: nombre y datos generales,
- La firma privada de una tercera entidad llamada autoridad certificadora (AC), que todos reconocen como tal, que valida la asociación de la clave pública con la persona.

El formato estándar de certificado digital es conocido como X509 v.3. Un certificado digital se reduce a un archivo de uno o dos k de tamaño, que autentica a un usuario de la red donde se consigna identidad, clave pública, caducidad, versión y parámetros del cifrado, emisor del certificado y firma de la autoridad.

El papel de la Autoridad certificadora (AC) es de firmar los certificados digitales de los usuarios, generar los certificados y mantener el status correcto de los certificados. Esto incluye también renovarlos o revocarlos y así mismo comunicarse con otras autoridades certificadoras. [5]

Protocolos de seguridad:

Un protocolo de seguridad es la parte visible de una aplicación, es el conjunto de programas y actividades programadas que cumplen con un objetivo específico y que usan esquemas de seguridad criptográfica. El ejemplo más común es SSL (Secure Sockets Layer) que vemos integrado en el navegador y hace su aparición cuando el candado de la barra de herramientas se cierra o sí la dirección de Internet cambia de http a https.

SSL es el protocolo de comunicación segura más conocido y usado actualmente, actúa en la capa de comunicación y es como un túnel que protege a toda la información enviada y recibida. Usa diferentes algoritmos de cifrado y hash (RC4, SHA-256, DH y RSA,… pero se van actualizando). Bajo SSL la información que se cifra incluye URLs, contenido, cookies enviadas y recibidas, cabeceras, etc.

El procedimiento que se lleva acabo para establecer una comunicación segura con SSL es el siguiente:

- El cliente (browser) envía un mensaje de saludo al Server "ClientHello"
- El servidor responde con un mensaje "ServerHello"
- El servidor envía su certificado
- El servidor solicita el certificado del cliente
- El cliente envía su certificado: si es válido continúa la comunicación (siguientes pasos)
  (si no, para o sigue la comunicación sin certificado del cliente)
- El cliente envía un mensaje "ClientKeyExchange" solicitando un intercambio de claves simétricas.
- El cliente envía un mensaje "CertificateVerify" si se ha verificado el certificado del servidor.
- Cliente y servidor envían un mensaje "ChangeCipherSpec" y comienza la comunicación segura.
- Al final ambos envían el mensaje "finished" con lo que termina la comunicación segura. En dicho mensaje intercambian el hash de toda la conversación, asegurando su integridad.

Otras Herramientas criptográficas:

Uno de los mejores métodos de **comparación de secretos** y más conocido es el esquema (n,k) límite de Shamir. Este método consiste en partir una clave K en n partes, y se tiene como mínimo (límite) el número k de partes (no necesariamente todos, aunque también k puede ser igual a n) para reconstruir la clave, es decir cualquiera k de los n custodios pueden reconstruir la clave K, pero ningún subgrupo de k-1 custodios podrá hacerlo. Está basado en cálculo y resolución de polinomios. La compartición de secretos puede ser usada para compartir la combinación de una caja fuerte, la clave de lanzamiento de algún proyectil o dispositivo de alto riesgo, etc.,

Una idea ingeniosa es usar un método de compartición de secretos con un esquemas límite (n,k) es la **criptografía visual**, esto consiste en lo siguiente: una imagen es partida en n partes, y si se sobreponen al menos k de estas partes (en forma de máscaras) se puede reconstruir la imagen.

Esquemas criptográficos que usualmente se aplican a votación electrónica:

- **Firma ciega:**
  Aún con dos dominios separados de autenticación (AA) y voto (donde se reciben, almacenan y cuentan) (AV) estos pueden confabularse. Para evitar esto, el votante "firma" su voto. AA valida el voto y la firma sin conocer el sentido del voto (sólo mira si el remitente está en el censo pero no enlaza el remitente a la firma, sólo el voto). En la urna de AV están todos los votos validados y las firmas pero sólo los votantes saben cada uno cuál es su firma, y así, su voto.
- **Mix-Nets:**
  Terceras partes de confianza ("autoridades") "barajan" los votos mediante mensajes de tal manera que nadie es capaz de identificar el emisor o receptor de mensaje. Se suele usar fundamentalmente para anonimizar los votos.
- **Cifrado homomórfico:**
  Básicamente es un cifrado donde una operación de votos cifrados equivale al cifrado de otra operación entre votos sin cifrar. Sirve para poder hacer contajes con votos aun sin cifrar. Solo es posible utilizarlo para conjuntos cerrados de elecciones (Si/NO, etc) pero no para voto preferencial.
- **Papeletas precifradas:**
  En este esquema todo el cifrado se hace anterior a la votación y se envían a los votantes ya autenticados los códigos personalizados para la votación. Tiene el inconveniente que incluye un envío previo (incluso físico) por parte de la autoridad de votación y la ralentiza.

NOTAS TÉCNICAS ACLARATORIAS ADICIONALES A CRIPTOGRAFÍA BÁSICA:

[1] **DES** es un sistema criptográfico que toma como entrada un bloque de 64 bits del mensaje y este se somete a 16 interacciones, una clave de 56 bits, en la práctica el bloque de la clave tiene 64 bits, ya que a cada conjunto de 7 bits se le agrega un bit que puede ser usada como de paridad. No se ha podido romper el sistema DES deduciendo la clave simétrica a partir de la información interceptada, pero sí por método de fuerza bruta, es decir probando alrededor de 256 posibles claves, se pudo romper DES en Enero de 1999. O sea que es posible obtener la clave del sistema DES en un tiempo relativamente corto, por lo que lo hace inseguro para propósitos de alta seguridad y ya no se usa. La opción que se tomó para poder sustituir a DES ha sido usar cifrado múltiple, aplicando varias veces el mismo algoritmo para fortalecer la longitud de la clave. Así, el funcionamiento de triple-DES o **TDES** consiste en aplicar 3 veces DES de la siguiente manera: la primera vez se usa una clave K1 junto con el bloque B0, de forma ordinaria E, obteniendo el bloque B1. La segunda vez se toma a B1 con la clave K2 (roja), diferente a K1 de forma inversa, llamada D (de Descencription) y la tercera vez a B2 con una clave K3 (verde) diferente a K1 y K2, de forma ordinaria E (de Encription), es decir, aplica de la interacción 1 a la 16 a B0 con la clave K1, después aplica de la 16 a la 1, a B1 con la clave K2, finalmente aplica una vez más de la 1 a la 16 a B2 usando la clave K3, obteniendo finalmente a B3. **AES** es el sucesor de DES como algoritmo de cifrado simétrico estándar para las organizaciones federales de USA. (Y también como estándar para casi todos los demás). AES acepta claves de 128, 192 o 256 bits (128 bits ya son muy irrompibles), utiliza bloques de 128 bits, y es eficiente tanto en software como en hardware. Fue seleccionado a través de una competencia abierta que involucró a cientos de criptógrafos durante varios años. Básicamente, es el mejor y más seguro algoritmo de cifrado y si son necesarios cifrados asimétricos, en muchas ocasiones son para compartir las claves AES.

[2] Las funciones hash más conocidas son **MD5**, **SHA-1** y RIPEMD 160. Actualmente se ha podido encontrar debilidades en las funciones hash que tienen como salida una cadena de 128 bits, por lo que se ha recomendado usar salidas de 160bits. Así mismo se han encontrado ataques a MD5 y SHA-0 (antecesora de SHA-1), esto ha dado lugar a que se dirija la atención sobre la función has RIPEMD-160.

[3] **RSA** (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente. RSA está basado en el problema de la factorización de números grandes (producto de dos primos), pero otros esquemas de cifrado asimétrico están basados en otros problemas matemáticos como son el Problema del Logaritmo Discreto Elíptico o PLDE usado por el método CCE [5]

[4] Los **CCE** son el mejor candidato para reemplazar a las aplicaciones que tienen implementado RSA, estas definen también esquemas de firma digital, Intercambio de claves simétricas AES y otros. Se puede mostrar que mientras en RSA se tiene que usar una clave de 1024 para ofrecer una considerable seguridad, los CCE solo usan 163 bits para ofrecer la misma seguridad, así también las claves RSA de 2048 son equivalentes en seguridad a 210 de CCE. Esto es porque para resolver el PLDE el único algoritmo conocido toma tiempo de ejecución exponencial, mientras que los que resuelven la factorización toman un tiempo subexponencial.

[5] La cantidad de certificados digitales revocados crece considerablemente, el problema está en que cada vez que se piensa realizar una comunicación y es necesario validar un certificado se debe de comprobar que este no está revocado. La solución que se ha venido usando es la de crear una lista de certificados revocados LCR y así verificar que el certificado no está en esa lista, para poder iniciar la comunicación. El manejo de las listas de certificados revocados ha llegado a tener un gran costo que sin embargo aún no se ha reemplazar por otra técnica a pesar que se han propuesto ya salidas al problema.