



VÍDEO intypedia008es

LECCIÓN 8: PROTOCOLO DE REPARTO DE SECRETOS

AUTOR: Dr. Luis Hernández Encinas

Consejo Superior de Investigaciones Científicas, Madrid, España

BERNARDO

Hola, bienvenidos a intypedia. Hasta ahora hemos aprendido muchas cosas relacionadas con los sistemas de cifra y la seguridad en redes. Hoy vamos a ver cómo es posible proteger un secreto sin utilizar sistemas de cifrado. ¡Acompáñanos!

ESCENA 1. CÓMO PROTEGER UN SECRETO

ALICIA

Hola. Hoy vamos a ver cómo es posible diseñar y llevar a cabo un protocolo para proteger un secreto contra su posible pérdida, robo o deterioro. En particular, vamos a ver cómo proteger, por ejemplo, una clave secreta con la que hemos cifrado un documento, o la clave privada que usamos para firmar digitalmente.

BERNARDO

¿Quieres decir que si pierdo o se deteriora mi clave secreta puedo volver a recuperarla? ¿O que puedo impedir que me la roben aunque la tenga escondida en mi casa? Eso sería fantástico.

ALICIA

No es eso exactamente. Lo que quiero decir es que es posible tomar precauciones para evitar que pierdas las claves que mantienes en secreto o que alguien pueda hacerse con ellas si las guardas en algún lugar que no esté adecuadamente protegido.

Para ello existen protocolos que permiten que un secreto se pueda recuperar a partir de determinadas piezas de información que se han elaborado previamente, se conocen como protocolos de compartición o de reparto de secretos.

En inglés estos protocolos se llaman *secret sharing*, es decir “compartición de secretos”, pero no se trata de compartir o repartir un secreto con otros, sino de dividir el secreto en partes de modo que éstas te permitan recuperarlo más tarde.

BERNARDO

Suena muy bien pero todavía no lo veo claro.

ALICIA

No te preocupes Bernardo, verás que es fácil. Te lo enseñaré en el siguiente capítulo.

ESCENA 2. PROTOCOLO DE REPARTO DE UN SECRETO

ALICIA

La idea inicial para poder recuperar un secreto consiste en dividir el secreto en varias partes de modo que si luego se tienen algunas de estas partes, no necesariamente todas ellas, sea posible volver a generar el secreto que se había ocultado inicialmente.

BERNARDO

Vamos a ver si te entiendo. Supongamos que tengo escrita mi clave secreta en un papel. Lo que me dices es que tengo que romper ese papel en varios trozos, de modo que luego seré capaz de volver a obtener la clave con sólo pegar los trozos en los que rompí el papel original. Pues si es así, no me parece una idea muy brillante.

ALICIA

El ejemplo que planteas no sirve porque el método que propones es excesivamente simple y poco seguro. De hecho, no es un buen método porque tiene varios problemas. Por ejemplo, no podrás recuperar la clave si pierdes aunque sólo sea un trozo de los que has obtenido al romper el papel original y, además, si alguien se hace con uno de los trozos de papel, conocerá parte de tu clave.

En la práctica, un protocolo para compartir o repartir secretos es un procedimiento criptográfico que permite obtener una serie de valores o *sombras* a partir de un secreto dado, de forma que es posible recuperar el secreto original utilizando un número prefijado de antemano de esas sombras, pero es imposible si se tienen menos sombras de las prefijadas.

BERNARDO

Si lo entiendo bien, hablas de sombras que se obtienen a partir del secreto original, no que sean partes del secreto. ¿Quiere eso decir que las sombras no contienen trozos de información del secreto, como los trozos de papel que yo mencionaba antes?

ALICIA

En efecto, se trata de obtener a partir de los datos del secreto, otros valores diferentes que no den pistas acerca del contenido del secreto. Tampoco he dicho nada acerca de cuál es el tamaño de las sombras. En el caso en que las sombras tengan el mismo tamaño que el secreto, el protocolo se dice que es *ideal*.

Además no hace falta usar todas las sombras que se generaron al principio para recuperar el secreto. Para ser más preciso, si en un protocolo de reparto de secretos se generan, por ejemplo, n sombras y hacen falta k de ellas para recuperar el secreto, se dice que k es un valor *umbral* y el protocolo se llama protocolo umbral k de n . Además, si se conocen menos de k sombras, es decir $k-1$ o menos, es imposible recuperar el secreto.

BERNARDO

Entonces, por ejemplo, ¿si tengo un protocolo “3 de 5” para repartir mi clave secreta, obtendré 5 sombras a partir de mi clave secreta y usando 3 sombras cualesquiera, podré recuperar la clave completa original? ¿Puedo guardar una sombra de mi secreto en el portátil, otra en un pendrive, otra en casa, una más en el despacho y la última en un CD?

ALICIA

¡Claro que sí! De ese modo si pierdes el CD, por ejemplo, no perderás la clave, sólo habrás perdido una de las sombras. Puedes usar cualesquiera de las 3 sombras restantes para recuperar el secreto. De este modo tienes protegida la clave contra posibles pérdidas, deterioro, robo, etc. Piensa que un atacante nunca podrá recuperar tu clave si recupera, en este ejemplo, 2 o menos sombras.

BERNARDO

Alicia, de momento me has convencido sobre la utilidad de estos protocolos. Pero... ¿Cómo se utilizan en la práctica? ¿Son complejos?

ALICIA

Es muy fácil de entenderlo. Vamos a verlo con un ejemplo en el siguiente capítulo.

ESCENA 3. REALIZACIÓN EFECTIVA DE UN PROTOCOLO DE REPARTO DE SECRETOS

ALICIA

Una de las formas más sencillas para llevar a cabo un protocolo de reparto de secretos usa como herramienta matemática los polinomios. Ojo, que no es la única forma de hacerlo, hay más, pero son algo más complicadas.

BERNARDO

Bueno, con los polinomios todavía me atrevo, no eran muy difíciles, de modo que explícame cómo se usan para repartir secretos.

ALICIA

En primer lugar hay que recordar que un polinomio puede utilizarse para representar una curva mediante los puntos que verifiquen dicho polinomio y que un polinomio de un grado fijado queda completamente determinado si se conocen los valores que ese polinomio toma en tantos puntos como uno más del valor de su grado.

BERNARDO

¿Quieres decir que para conocer los tres coeficientes de un polinomio de grado 2, por ejemplo, me basta con saber cuánto vale el polinomio en tres puntos, es decir, para tres valores de la x ?

ALICIA

Esa es la idea. Recuerda que dos puntos determinan una única recta, es decir, un polinomio de grado 1; tres puntos una única parábola, que es un polinomio de grado 2, etc. De este modo que si se conocen los valores de un polinomio para determinados puntos, se puede determinar el polinomio que pasa por esos puntos y cuyo grado es uno menos del número de puntos conocido. El proceso para determinar el polinomio a partir de los puntos, se conoce como método de interpolación de Lagrange.

BERNARDO

Lo siento Alicia pero aún no veo cómo se pueden usar los polinomios para ocultar secretos.

ALICIA

Paciencia, vamos a ello. La idea de usar polinomios para este protocolo se debe a Adi Shamir, uno de los criptógrafos más importantes de la actualidad. Se trata de ocultar un secreto dentro de un polinomio de modo que con una determinada información parcial del polinomio se pueda recuperar el secreto que se ocultó en él.

BERNARDO

De acuerdo, pero hay dos problemas. El primero es ocultar el secreto en el polinomio y el segundo es recuperar el polinomio para obtener el secreto. Vamos con el primero. Si mi secreto fuera por ejemplo el número 263 y el protocolo es 3 de 5, ¿cómo lo ocultas en un polinomio?

ALICIA

Bernardo, has elegido como umbral el valor $k=3$, por lo que vamos a utilizar un polinomio de grado 2, que tiene 3 coeficientes: $p(x)=ax^2+bx+c$. Es decir, el umbral coincide con el número de coeficientes del polinomio. Una vez decidido esto, se considera como término independiente

del polinomio el valor secreto, es decir $c = 263$. Para los otros dos coeficientes se eligen dos números aleatorios, por ejemplo, $a=167$ y $b=227$, con lo que nuestro polinomio sería $p(x)=167x^2+227x+263$. Ahora, simplemente calculamos el polinomio para 5 valores de x cualesquiera (5 sombras). Por ejemplo, podemos elegir por simplicidad para x los valores 1, 2, 3, 4 y 5, aunque puede ser cualquier otro conjunto de 5 números.

BERNARDO

Déjame, eso lo hago yo. Si sustituyo el valor $x=1$ en el polinomio me da, veamos,

$$p(1)=167 \cdot 1+227 \cdot 1+263=657.$$

Y los otros valores serían 1385, 2447, 3843 y 5573.

ALICIA

¡Bien hecho! Ya has construido las 5 sombras que necesitabas. Cada sombra es la pareja formada por el valor de la x y el correspondiente valor del polinomio. Es decir, tus 5 sombras son los siguientes pares de números (1, 657), (2, 1385), (3, 2447), (4, 3843) y (5, 5573). Ahora puedes guardarlas en cinco lugares diferentes. Como puedes ver en este ejemplo ninguna de las sombras se parece a tu secreto, no hay forma de que alguien pueda deducir tu valor secreto 263 si roba o encuentra alguna pareja de los números anteriores.

Eso sí, no debes olvidarte de destruir el papel en el que tenías escrito tu número secreto o borrar el fichero donde lo habías guardado. Por cierto, también deberías eliminar cualquier rastro del polinomio para que nadie pueda encontrarlo y ver tu número secreto en él.

ESCENA 4. RECUPERANDO EL SECRETO

BERNARDO

Esto ha sido fácil pero ahora viene la segunda parte, ¿cómo recupero el valor secreto usando sólo 3 de las 5 sombras?

ALICIA

Para recuperar el secreto hay que obtener el polinomio y considerar su término independiente. Para hacer esto se consideran 3 de las 5 sombras ($x, p(x)$), por ejemplo, la segunda (2, 1385), la tercera (3, 2.447) y la quinta (5, 5.573), y empleamos el método de interpolación de Lagrange para recuperar el polinomio. Hagamos unos cálculos:

En general se tendrían k puntos: $(x_1, y_1) \dots (x_k, y_k)$ y el polinomio se determina calculando

$$p(x) = \sum_{j=1}^k y_j \cdot q_j(x), \text{ siendo } q_j(x) = \prod_{i=1, i \neq j}^k (x-x_i)/(x_j-x_i), \text{ con } j=1, \dots, k.$$

En nuestro ejemplo los 3 puntos son: $(x_2, y_2), (x_3, y_3), (x_5, y_5)$, de modo que el cálculo es más sencillo. Para cada punto se calcula el polinomio auxiliar $q_j(x)$ correspondiente y se tiene:

Punto $(x_2, y_2)=(2, 1385)$

$$q_2(x) = ((x-x_3)/(x_2-x_3)) \cdot ((x-x_5)/(x_2-x_5)) = ((x-3)/(2-3)) \cdot ((x-5)/(2-5)) = x^2/3 - 8x/3 + 5,$$

Punto $(x_3, y_3) = (3, 2447)$

$$q_3(x) = ((x-x_2)/(x_3-x_2)) \cdot ((x-x_5)/(x_3-x_5)) = ((x-2)/(3-2)) \cdot ((x-5)/(3-5)) = -x^2/2 + 7x/2 - 5,$$

Punto $(x_5, y_5) = (5, 5573)$

$$q_5(x) = ((x-x_2)/(x_5-x_2)) \cdot ((x-x_3)/(x_5-x_3)) = ((x-2)/(5-2)) \cdot ((x-3)/(5-3)) = x^2/6 - 5x/6 + 1.$$

El polinomio original se obtiene calculando $p(x) = \sum_{j=2,3,5} y_j \cdot q_j(x)$

$$p(x) = y_2 \cdot q_2(x) + y_3 \cdot q_3(x) + y_5 \cdot q_5(x),$$

de modo que al final resulta

$$p(x) = 1385 \cdot q_2(x) + 2447 \cdot q_3(x) + 5573 \cdot q_5(x) = 167x^2 + 227x + 263.$$

Con lo que tu número secreto es el 263. Esta misma cuenta la puedes hacer con cualesquiera otras 3 sombras. No importa las que elijas, siempre obtendrás el mismo polinomio.

BERNARDO

Me encanta, lo encuentro genial. Es claro que con 3 sombras se recupera mi secreto y tendré que vigilar para que nadie consiga 3 de las sombras. Me imagino que el protocolo de reparto o compartición de secretos tiene otras utilidades.

ALICIA

Tienes razón. La protección que mencionas fue su motivación original. Sin embargo, hoy en día estos protocolos sirven y se aplican en otras situaciones. Por ejemplo, se puede dividir un secreto y entregar cada sombra a una persona diferente, de modo que el secreto sólo se recupera si un determinado número de personas acuerdan compartir sus sombras y generar el secreto. Esta forma de actuar se utiliza por ejemplo, para el control de accesos, la apertura de cajas de seguridad o la inicialización de dispositivos militares.

BERNARDO

Alicia, me queda sólo una duda: ¿qué tan seguro es este protocolo? ¿Nadie ha intentado romperlo?

ALICIA

La seguridad del protocolo está demostrada. Es cierto que se han hecho intentos para romperlo, pero hasta ahora no se conoce ninguna forma de vulnerar el protocolo siempre que se sigan las pautas establecidas y su implementación no contenga errores.

Bueno con esto es suficiente, en próximas lecciones veremos otros protocolos diferentes que permiten realizar otras interesantes acciones. En la página Web de intypedia se encuentra documentación adicional a esta lección, como por ejemplo, una muestra de que con $k-1$ sombras no es posible reconstruir un secreto. ¡Adiós!

BERNARDO

¡Hasta luego!

Guión adaptado al formato intypedia a partir del documento entregado por el Dr. Luis Hernández Encinas del Consejo Superior de Investigaciones Científicas en Madrid, España.

Madrid, España, Junio de 2011

<http://www.intypedia.com>

<http://twitter.com/intypedia>

