Lección 8: Protocolo de reparto de secretos

intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Dr. Luis Hernández Encinas
luis@iec.csic.es

Consejo Superior de Investigaciones Científicas
Científico Titular

Esquemas de reparto de secretos (I)

- Un *esquema de reparto de secretos* es un protocolo que permite obtener una serie de datos o sombras a partir de un secreto, de forma que sea posible recuperar el secreto original a partir de sólo algunas de esas sombras.
- Estos esquemas fueron propuestos para salvaguardar las claves criptográficas de su posible deterioro, robo o pérdida.

Esquemas de reparto de secretos (II)

- Estos protocolos también se conocen como *de compartición de secretos* y, en general, como *secret sharing*.
- En particular, es posible proteger claves secretas, claves privadas, documentos, etc.
- Actualmente tienen aplicaciones en:
  - El control de accesos,
  - La apertura de cajas de seguridad,
  - La inicialización de dispositivos militares, etc.

Esquemas umbrales *k* de *n* (I)

- El ejemplo básico de los esquemas para el reparto de secretos son los esquemas (*k*, *n*)-umbrales, con *k* y *n* enteros y $1 \leq k \leq n$.
- En estos protocolos, el usuario determina *n* sombras a partir del secreto que desea proteger: S_1, …, S_n, y las almacena o esconde de manera segura.
- Utilizando *k* sombras cualesquiera, o más, se podrá recuperar el secreto *S*.

Esquemas umbrales *k* de *n* (II)

- Dicho de otro modo, en un esquema umbral (*k*, *n*), no es posible obtener información alguna del secreto si sólo se poseen *k*-1 sombras o menos.
- Un esquema se dice *ideal* si cada una de las sombras tiene el mismo tamaño que el secreto original.

Realización de un protocolo de reparto de secretos

- Estos protocolos constan de dos fases:
- Fase 1: generación de sombras.
- Fase 2: recuperación del secreto.

- Una de las formas más sencillas de realizar los protocolos de reparto de secretos es mediante polinomios.

Fase 1: Generación de las sombras (I)

1. Se deciden los valores del esquema: el valor umbral, k, y el número de sombras, n.
2. Se considera un polinomio de grado k-1:

$$p(x) = a_{k-1}\, x^{k-1} + a_{k-2}\, x^{k-2} + \ldots + a_1\, x + a_0 = \Sigma^{k-1}_{j=0}\, a_j\, x^j,$$

de modo que el secreto sea el coeficiente $a_0 = S$.

3. A continuación se eligen aleatoriamente los restantes coeficientes, a_i, de $p(x)$.

Fase 1: Generación de las sombras (II)

4. Una vez conocido el polinomio, se calcula su valor para n valores diferentes de x, por ejemplo, para $x = 1,\ldots,n$, de modo que se tienen n parejas de valores:

$$(x_i, y_i) = (i, p(x_i)), \quad i = 1,\ldots, n.$$

5. Cada uno de estos pares es una sombra.

Ninguno de los valores de las sombras guarda relación con el valor del secreto S.

Fase 2: Recuperación del secreto (I)

1. Se eligen k sombras cualesquiera de las n de que se disponen, por ejemplo:

$$(x_j, y_j), \quad j = 1,\ldots,k.$$

2. Se calculan los siguientes k polinomios auxiliares, cada uno de grado k-1:

$$q_j(x) = \prod^{k}_{i=1, i\neq j} (x-x_i)/(x_j-x_i), \quad j = 1,\ldots,k.$$

Fase 2: Recuperación del secreto (II)

3. Se determina el polinomio buscado:

$$p(x) = \Sigma^{k}_{j=1}\ y_j\, q_j(x).$$

4. Una vez que se ha calculado el polinomio

$$p(x) = a_{k-1}\, x^{k-1} + a_{k-2}\, x^{k-2} + \ldots + a_1\, x + a_0,$$

su término independiente es el secreto recuperado: $a_0 = S$.

Ejemplo (I): Generación de sombras

a) Se elige como umbral $k = 3$, como número de sombras $n = 5$ y como secreto $S = a_0 = 263$.

b) Se considera el polinomio de grado k-1 = 2:

$$p(x) = 167\,x^2 + 227\,x + 263.$$

c) Se calculan las $n = 5$ sombras, es decir, los 5 puntos siguientes: $(x_i, y_i) = (i, p(x_i))$, $i = 1,\ldots,5$:

(1, 657), (2, 1385), (3, 2447), (4, 3843), (5, 5573).

Ejemplo (II): Recuperación del secreto (I)

a) Se seleccionan $k = 3$ sombras cualesquiera de las $n = 5$ que se tienen:

(2, 1385), (3, 2447), (5, 5573).

b) Se calculan los $k = 3$ polinomios auxiliares:

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

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

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

Ejemplo (II): Recuperación del secreto (II)

c) Se determina el polinomio buscado:

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

$$= 1385\, q_2(x) + 2447\, q_3(x) + 5573\, q_5(x)$$

$$= 167x^2 + 227x + 263.$$

d) El secreto recuperado es $S = a_0 = 263$.

Ejemplo (III): Seguridad (I)

a) Si se seleccionan menos de $k = 3$ sombras es imposible recuperar el secreto. Si se suponen conocidas sólo 2 sombras:

(1, 657) y (4, 3843).

b) Entonces, sólo se pueden calcular 2 polinomios auxiliares:

$$q_1(x) = (x - x_4)/(x_1 - x_4) = -x/3 + 4/3,$$

$$q_4(x) = (x - x_1)/(x_4 - x_1) = x/3 - 1/3.$$

Ejemplo (III): Seguridad (II)

c) A partir de los cuales se puede calcular el siguiente polinomio:

$$q(x) = y_1\ q_1(x) + y_4\ q_4(x)$$
$$= 657\ q_1(x) + 3843\ q_4(x)$$
$$= 1062x - 405.$$

d) Pero es imposible obtener el secreto original. De hecho, este polinomio es sólo de grado 1.

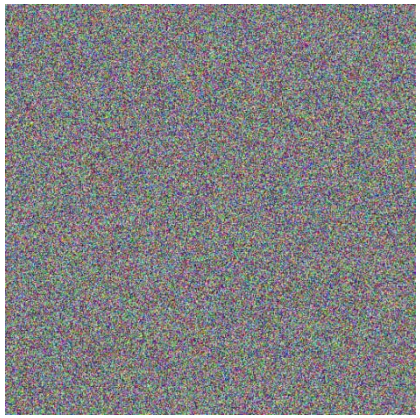
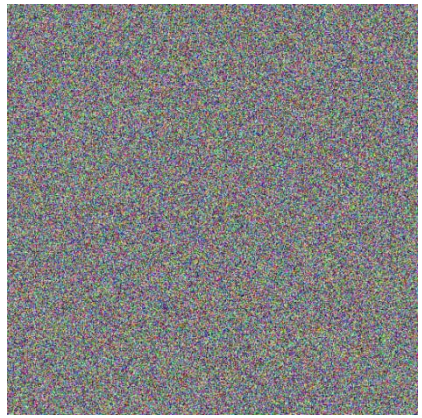
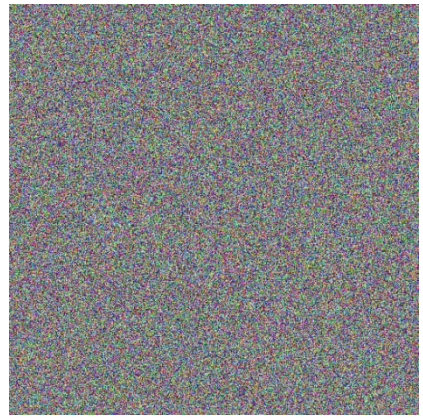
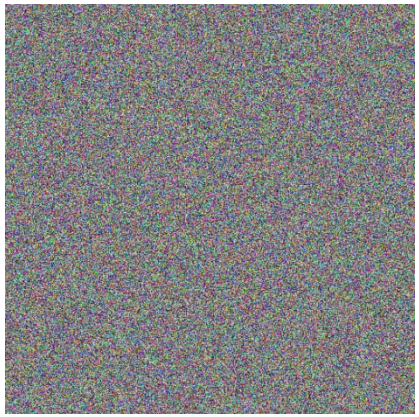
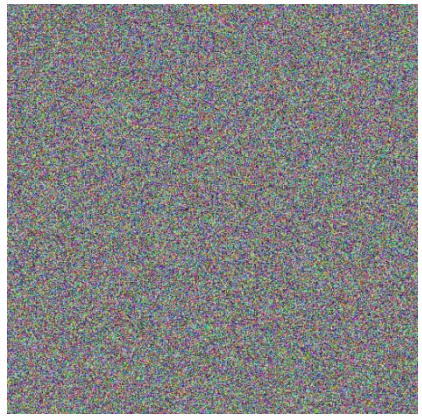
Aplicación gráfica

- Además de las aplicaciones mencionadas, los protocolos de repartos de secretos se pueden emplear para repartir imágenes secretas.

- En este caso, se determinan *n* sombras o imágenes del mismo tamaño que la original, pero a partir de las cuales no se obtiene información de la imagen secreta salvo que se unan *k* de ellas.

Ejemplo: Esquema gráfico umbral 5 de 5

- Las 5 sombras y la imagen original secreta


intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Contacto: info@intypedia.com