Análisis y desarrollo de esquemas para la compartición e intercambio de secretos

Javier Areitio Bertolín

El Prof. Dr. Javier Areitio Bertolín es Catedrático de la Facultad de Ingeniería ESIDE y Director del Grupo de Investigación Redes y Sistemas de la Universidad de Deusto
jareitio@eside.deusto.es

En el presente artículo se sintetizan y analizan diferentes protocolos criptográficos del tipo esquemas de compartición-reparto de secretos (contraseñas, claves, ficheros, etc.) entre un colectivo de N entidades con vistas a que la recuperación de dicho secreto implique la presencia de K (K<N) entidades y que con sólo (K-1) entidades no se pueda recuperarlo, ni si quiera poder inferir algo de información. Por último se desarrolla un mecanismo para intercambiar un secreto entre dos entidades comunicantes a través de una red no segura utilizando polinomios de Chebyshev y se especifica un criptosistema estilo RSA basado en polinomios de Chebyshev.

En criptografía, la compartición de secretos es una técnica para distribuir un secreto (fichero, clave, contraseña, etc.) entre un grupo de participantes, restringiendo el acceso a los participantes que conocen un porcentaje predeterminado del secreto. En un esquema de secreto compartido, existe un repartidor y N participantes. El repartidor da un secreto a los participantes pero sólo cuando se cumplen las condiciones específicas. Para realizar esto, el repartidor da a cada participante un fragmento de dicho secreto de forma que cualquier grupo de K (valor umbral) o más participantes pueden juntos reconstruir el secreto pero ningún grupo de menos de K participantes puede hacerlo, ni siquiera puede inferir algo acerca del secreto. Este tipo de sistema se denomina esquema umbral (K, N).

Esquema de compartición de secretos defectuoso

Un verdadero esquema de compartición de secretos distribuye el secreto de modo que con menos de K fragmentos no se obtenga información alguna sobre dicho secreto, es decir como si no se tuviese ningún fragmento. Consideremos el siguiente esquema simplista: un repartidor divide el secreto "password" en cuatro fragmentos "pa", "ss", "wo", "rd" y los distribuye entre cuatro participantes. Una persona que carezca de fragmentos puede saber que el secreto consta de ocho letras pero no tiene ni idea de que letras contiene, debería averiguar el secreto a partir de $26^8 = 208$ billones de posibles combinaciones. Una persona que posea un fragmento debería averiguar sólo seis letras es decir $26^6 = 308$ millones de combinaciones. Una persona que posea tres fragmentos sólo tendría que averiguar $26^2 = 676$ posibilidades. Este sistema no es un verdadero esquema de compartición de secretos debido a que cada fragmento proporciona algo de información significativa acerca del contenido del secreto. Bajo un esquema de compartición de secretos incondicionalmente seguro una persona que posea tres fragmentos debería tener $26^8 = 208$ billones de posibles combinaciones, mientras que una persona que posea cuatro fragmentos debería conocer el secreto. Algunos esquemas de compartición de secreto se dice que son seguros teóricamente a nivel de información mientras que otros no poseen esa seguridad incondicional a favor de una mejora de eficiencia mientras se mantiene suficiente seguridad para ser considerados seguros como otras primitivas criptográficas comunes. Por ejemplo, pueden permitir que secretos arbitrariamente largos se protejan por medio de fragmentos de 128 bits ya que esto genera 2^{128} posibles fragmentos que se considerarán suficientes para disuadir a cualquier adversario actual concebible.

Esquemas triviales de compartición de secretos

Existen varios esquemas de compartición de secretos (k, n) para k=n donde todos los fragmentos son necesarios para poder reconstruir el secreto:

1) El secreto se codifica como un número entero "s". Se da a cada participante "i" (salvo al último) un número entero aleatorio "r_i", se da al último participante el número $(s - r_1 - r_2 - \ldots - r_{n-1})$. El secreto es la suma de todos los fragmentos.

2) El secreto se codifica como un byte "s". Se da a cada participante "i" (salvo al último) un byte aleatorio "b_i", se da al último participante el byte $(s \text{ xor } b_1 \text{ xor } b_2 \text{ xor } \ldots \text{ xor } b_{n-1})$ El secreto es la suma módulo 2 ó operación xor de todos los fragmentos que poseen los participantes.

Protocolos criptográficos para el reparto-compartición de secretos

Los esquemas de reparto-compartición de secretos pueden considerarse protocolos criptográficos ideados para dividir un secreto en varias partes denominados fragmentos con el objetivo de conseguir un equilibrio entre disponibilidad (tolerancia a fallos) y confidencialidad.

Por ejemplo, se puede desear dividir un secreto en cinco partes y almacenar dichas partes en cinco lugares diferentes con los siguientes objetivos: si tres de las partes permanecen intactas se pueda reconstruir el secreto; si un atacante consigue acceso a sólo dos de estos lugares no pueda calcular, averiguar, deducir o inferir el secreto ni incluso nada de información sobre dicho secreto. Por ejemplo, se puede desear almacenar una contraseña poco utilizada de esta forma, por si se olvida o pierde e impidiendo que sea conocida por cualquiera no autorizado. Si se desea almacenar de forma fragmentada una contraseña en n=5 fragmentos, de modo que pueda reconstruirse sólo a partir de cualquiera de los k=3 fragmentos y además con (k-1)=2 no se proporcione información alguna sobre dicha clave o secreto.

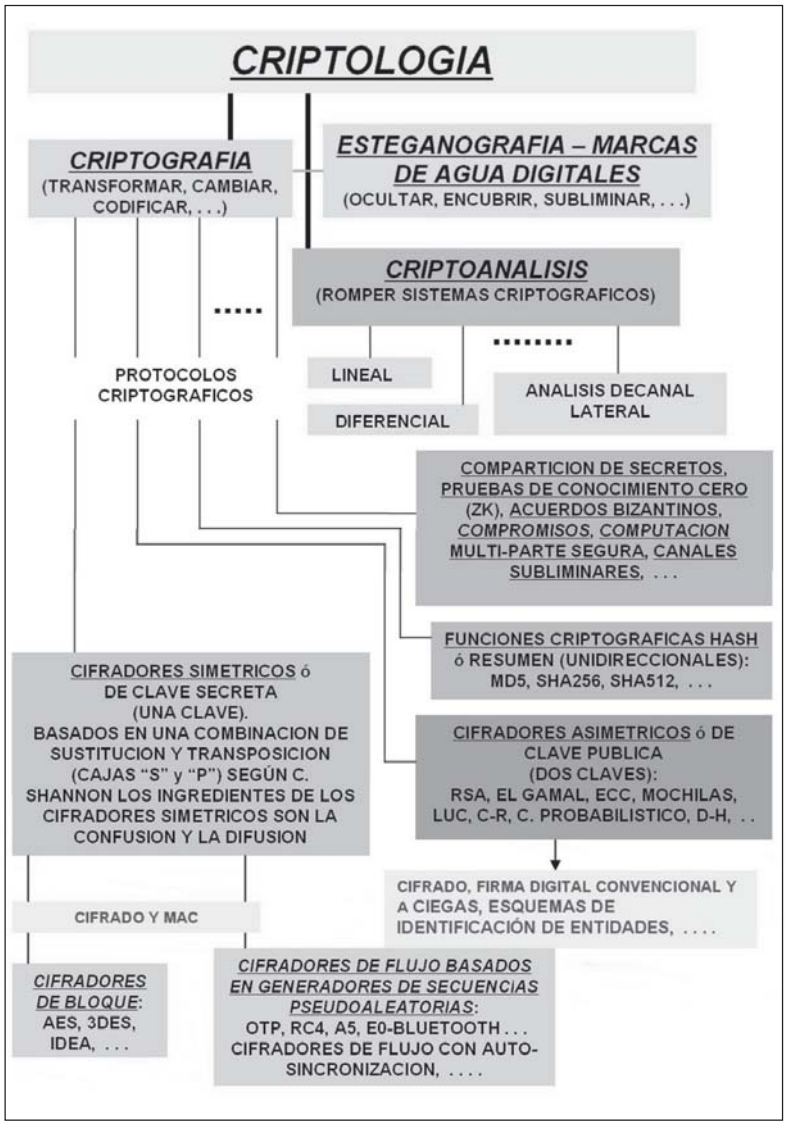

Figura 1. Esquema de clasificación de la Criptología, ciencia y tecnología que se ocupa del secreto, integridad, autenticación, no repudio, etc. de las comunicaciones.

El objetivo es conseguir un equilibrio entre las dos siguientes propiedades:
(a) Disponibilidad, incluso aunque algunos fragmentos se pierdan el secreto o contraseña se debe conservar.
(b) Confidencialidad, un adversario que obtenga acceso a un número de fragmentos menor que "k" no debe tener posibilidad de averiguar la contraseña ni poder inferir dato alguno.

El reparto-compartición de secretos no se puede realizar de una forma trivial almacenando los caracteres de la contraseña en diferentes lugares ya que no se cumplen los requisitos de que con cualquiera de los k=3 fragmentos es suficiente para reconstruir la clave o secreto y además se podría saber algo del secreto si un adversario consigue algunos fragmentos.

Para una definición más formal del mecanismo de reparto-compartición de secreto se identifican los siguientes parámetros:
(1) Número total de fragmentos deseado "n".
(2) Número mínimo de fragmentos a partir de los cuales es posible reconstruir el secreto "s".
(3) Un espacio de secretos S es decir un conjunto de posibles secretos a repartir.

Una instanciación con "n" y "k" específicos se denomina esquema de reparto-compartición de secreto (k, n). Existen tres funciones:
(a) Un repartidor, el propietario inicial del secreto.
(b) Los portadores de los fragmentos, son participantes que obtienen los fragmentos del repartidor.
(c) Un reconstructor, es una parte que reconstruye el secreto, en algunos casos puede ser el propio repartidor.

En una ejecución concreta del reparto-compartición de secretos toman parte un repartidor, "n" portadores de fragmentos y un reconstructor. Existen dos sub-protocolos:
(i) Repartición-compartición, es un protocolo entre el repartidor y todos los "n" portadores de los fragmentos, normalmente es simple y sin interacción alguna. Las acciones que se realizan son:
(a) El repartidor posee un secreto "s" perteneciente al espacio S, por ejemplo una contraseña a repartir.
(b) El repartidor realiza unos cálculos locales que permiten obtener los fragmentos (s, . . ., s).
(c) El repartidor envía un fragmento a cada portador de fragmentos y cada portador guarda dichos fragmento(s).
(ii) Reconstrucción, es un protocolo entre el reconstructor y los "k" portadores de fragmentos, es simple y sin interacción alguna. Las acciones que se realizan son:
(a) Cada portador de fragmentos participante envía su fragmento al reconstructor.
(b) El reconstructor realiza ciertos cálculos locales (resolución de un sistema de "k" ecuaciones congruenciales) para reconstruir la contraseña o secreto deseado "s".

La figura 1 muestra un árbol de identificación de las áreas tecnológicas de la criptología donde se sitúa la compartición de secretos.

Esquema estilo Shamir para el reparto de secretos

Dos puntos definen de forma única una línea recta, tres puntos definen una parábola, cuatro definen una curva cúbica, etc. En general "n" pares de coordenadas (x_i, y_i) definen de forma única un polinomio de grado $(n-1)$. El repartidor de secretos codifica el secreto como la interceptación "y" de la curva y reparte a cada participante las coordenadas de un punto de esta curva. Cuando los participantes reúnen suficientes fragmentos pueden interpolar para encontrar la interceptación "y" y de este modo recuperar el secreto. No es muy práctico utilizar este esquema con polinomios convencionales; el secreto y los fragmentos generalmente son complejas divisiones que son difíciles de almacenar en un fichero convencional. Consecuentemente el polinomio se define normalmente sobre un campo finito Zp (de módulo p). El esquema estilo Shamir es eficiente en espacio, cada fragmento es del mismo tamaño que el secreto original debido a que las coordenadas "x" de cada fragmento pueden ser conocidas por todos los participantes. Este esquema también minimiza la necesidad de números aleatorios; para cada bit del secreto el repartidor debe generar "k" bits aleatorios donde "k" es el número umbral de personas participantes.

Consideremos un espacio de secretos S que debe ser un subconjunto de un campo finito F, por ejemplo un campo primo Zp. Además $|F| > n$. La técnica estilo Shamir consta de los siguientes pasos:
(1) El repartidor del secreto elige un polinomio aleatorio pol(x) de grado (k-1) sobre F con término constante "s". Selecciona los coeficientes $(a_1, \ldots, a_{k-1})$ de forma uniformemente aleatorios pertenecientes a F, es decir:
$pol(x) = (a_{k-1}x^{k-1} + \ldots + a_1 x + s) \bmod p$
donde "s" es el secreto.
(2) El repartidor del secreto fija un valor diferente no nulo x_i perteneciente a F para cada portador de fragmento y se le da el par: $s_i = (x_i, pol(x_i))$, donde cada fragmento es un punto del polinomio.
(3) Para recuperar el secreto "s" con "k" fragmentos s_i se forma un sistema de ecuaciones que permiten determinar "s". Consideremos un ejemplo de un esquema estilo Shamir: sea el secreto a compartir s=11, se construye un esquema umbral (k=3, n=5) en el que cualquiera grupo de tres de los cinco participantes puede reconstruir el secreto. Primero se genera un polinomio cuadrático (de grado k-1=2) con coeficientes de x^2 y de x aleatorios y como término independiente s=11, es decir:
$p(x) = (7x^2 + 8x + 11) \bmod 13$.

Se obtienen cinco fragmentos: (1, 0), (2, 3), (3, 7), (4, 12), (5, 5), de modo que con tres de ellos se puede recuperar "s".

Esquema de reparto-compartición de secretos con dispersión de información

El valor secreto a repartir C se divide y utiliza como los coeficientes del polinomio es decir C se divide en k bloques $(a_0, \ldots, a_{k-1})$, y estos bloques se consideran los coeficientes de un polinomio. Los fragmentos se calculan como los puntos del polinomio. Dada una cierta información numérica secreta por ejemplo la contraseña (C = abcdefghij) que se desea repartir-compartir entre un colectivo de personas o entidades artificiales (por ejemplo empleando servidores) de forma que para averiguar su valor deben juntar sus fragmentos del secreto se procede de la manera siguiente:
(1) Se construye un polinomio de grado nueve:
$p(x) = (j + ix + hx^2 + gx^3 + fx^4 + ex^5 + dx^6 + cx^7 + bx^8 + ax^9) \bmod p$.
(2) Se determinar tantos valores como entidades se necesite para reconstruir el secreto en este caso diez puntos (p(x), x) permiten reconstruir el polinomio y sus coeficientes que permiten conocer el secreto a repartir. Examinemos un ejemplo, si se desea compartir entre cuatro entidades (k=4) el secreto C=11341, se fragmenta en cuatro trozos 11, 3, 4 y 1 y se colocan como coeficientes de un polinomio de grado (k-1), en este caso tres (igual al número de entidades que se precisan para recuperar el secreto menos uno). Es decir: $p(x) = (11 + 3x + 4x^2 + x^3) \bmod p$, donde p se elige por ejemplo 41. Entonces se determinan algunos puntos del polinomio p(x) por ejemplo: (1,19), (2,0), (3,1), (4,28), (5,5), (6,20), (7,38), (8, 24), (9,25), (10,6), (11,14), (12,14). Con cuatro de estos puntos se puede obtener el polinomio y por tanto determinar C.

Analicemos otro ejemplo, sea el secreto a compartir y repartir C = 791. Se desea que con tres fragmentos (k=3) se recupere C. Entonces planteamos un polinomio de grado (k-1), en este caso de grado dos sobre Z como por ejemplo:
$p(x) = (ax^2 + bx + c) \bmod 31$; donde los coeficientes a=1, b=9, c=7 son los trozos de C. Se calculan diversos puntos del polinomio como por ejemplo (2,29), (3,12), (4,28). De modo que con tres puntos cualesquiera se recuperan los coeficientes del polinomio y por tanto la clave C secreta a repartir-compartir.

Operaciones con secretos repartidos-compartidos. Compartición proactiva de secretos

A veces surge la necesidad de realizar determinados cálculos con secretos que han sido repartidos-compartidos y es peligroso poner el secreto junto. En particular esta necesidad surge en la criptografía de grupos. Consideremos el caso más simple que consiste en calcular com-

binaciones lineales de secretos compartidos. Es equivalente a poder calcular sumas y multiplicaciones escalares, multiplicaciones por un valor que no esté oculto como el secreto compartido pero conocido para todos los participantes. Supongamos que dos secretos s y s' se comparten utilizando los polinomios pol(x) y pol'(x). Los secretos son s = pol(0) y s' = pol'(0) y los fragmentos de un participante con valor fijo x_i son: $y_i = pol(x_i)$, $y'_i = pol'(x_i)$. Ahora consideremos la suma de polinomios $pol''(x_i) = pol(x_i) + pol'(x_i)$ que también es un polinomio de grado al menos (k-1). Se tiene que:
pol''(0) = pol(0) + pol'(0) = s + s'.
Por tanto este polinomio pol''(x) puede utilizarse para repartir-compartir la suma de secretos. Además:
$pol''(x_i) = pol(x_i) + pol'(x_i) = y_i + y'_i$.
Por tanto los fragmentos de este polinomio pol''(x) son las sumas de los fragmentos de los polinomios originales. Esta última operación la puede realizar de forma local cada portador de fragmento sumando sus dos fragmentos. De este modo ahora poseen los fragmentos de la suma s + s' y de los dos secretos originales. De forma análoga se puede obtener los fragmentos de un valor secreto ks (donde k pertenece al conjunto F) es un valor conocido y "s" es un secreto compartido si cada portador de fragmento multiplica localmente su fragmento por el valor "k". Si el esquema de reparto-compartición de secreto es homomórfico (caso de los métodos considerados, estilo Shamir y de dispersión de información) entonces si $(d_1, d_2, \ldots, d_n)$ es una asignación de fragmentos para determinar el secreto D y $(d'_1, d'_2, \ldots, d'_n)$ representa una asignación de fragmentos para el secreto 0, entonces los fragmentos $(d_1+d'_1, d_2+d'_2, \ldots, d_n+d'_n)$ es también una asignación para el secreto D. Dicho esquema permitirá que muchas partes renueven pro-activamente sus fragmentos sin cambiar el secreto D. La ventaja es que limita la cantidad de daño si las partes se ven comprometidas. Si los portadores de los fragmentos almacenan sus fragmentos en servidores de computación no seguros, un atacante puede acceder de forma no autorizada y robar algunos fragmentos. Si no es práctico cambiar el secreto, los fragmentos no comprometidos (estilo Shamir) se pueden renovar. El repartidor genera un nuevo polinomio aleatorio con término constante igual a cero y calcula para cada participante restante un nuevo par ordenado donde las coordenadas "x" de los nuevos y antiguos pares coinciden. Cada participante suma la vieja y nueva coordenada "y" y guarda el resultado como la nueva coordenada "y" del secreto. Todos los fragmentos no actualizados que acumuló el atacante se hacen inservibles. Un atacante sólo puede recuperar el secreto si puede encontrar suficientes fragmentos no actualizados para alcanzar el valor umbral. Esta situación no debería suceder debido a que los participantes borraron sus fragmentos antiguos. Así mismo, un atacante no puede recuperar nada de información acerca del secreto original a partir de los ficheros actualizados debido a que contienen sólo información aleatoria. El repartidor puede cambiar el valor umbral mientras distribuye las actualizaciones pero debe siempre permanecer vigilante de que los participantes guarden los fragmentos expirados.

Comparticion de secretos verificable

Un participante puede mentir acerca de su propio fragmento para obtener acceso a otros fragmentos del secreto. Un esquema de compartición de secretos verificable (VSS Verifiable Secret Sharing) permite a los participantes estar seguro de que ningún otro participante mienta sobre los contenidos de sus fragmentos hasta una probabilidad de error razonable. Dichos esquemas no pueden calcularse de forma convencional, los participantes deben colectivamente sumar y multiplicar números sin que ningún individuo sepa lo que esta exactamente sumando y multiplicando. Tal Rabin y Michael Ben-Or desarrollaron un sistema de computación multi-parte MPC (MultiParty Computing) que permite a los participantes detectar falta de honestidad en la parte del repartidor o por parte de hasta un tercio del número umbral de participantes, incluso aunque dichos participantes los coordina un atacante adaptativo que puede cambiar las estrategias en tiempo real dependiendo de que información se ha revelado.

Aplicaciones de la comparticion de secretos

Un esquema de compartición de secretos puede proteger un secreto guardado sobre múltiples servidores y permanecer recuperable a pesar de que varios de dichos servidores se averíen. El repartidor del secreto puede tratar a él mismo como varios participantes distintos, distribuyendo los fragmentos de secreto sobre él. Cada fragmento puede almacenarse en un servidor diferente pero el repartidor puede recuperar el secreto incluso aunque varios servidores se averíen. Los posibles atacantes que accedan de forma no autorizada a un servidor no podrán conocer el secreto. Un repartidor de secreto puede enviar "k" fragmentos a un único receptor, todos ellos necesarios para poder recuperar el secreto original, un posible atacante debería interceptar todos los "k" fragmentos para poder recuperar el secreto, tarea que puede ser más difícil que interceptar un único fichero.

Otro ejemplo de utilización de la tecnología de compartición de secretos esta a la hora de distribuir una fórmula secreta entre un grupo relevante de empleados de la organización. A la hora de poder disparar un

GENERACION DEL PAR DE CLAVES PUBLICA-PRIVADA DE LA ENTIDAD A (e, d)

1) ENTIDAD A ELIGE DOS NUMEROS PRIMOS p, q QUE LOS MANTIENE EN SECRETO.
2) ENTIDAD A CALCULA EL MODULO PUBLICO
m = (p . q)
3) ENTIDAD A ELIGE UN VALOR ALEATORIO "e" TAL QUE 0 < e < m ES SU CLAVE PUBLICA
4) ENTIDAD A CALCULA EL MODULO SECRETO
k = (p-1)(q-1)
5) ENTIDAD A CALCULA SU CLAVE PRIVADA DE DESCIFRADO
d = e mod k
6) ENTIDAD A ENVIA A ENTIDAD B LOS VALORES (m, e).

OPERACIONES DE CIFRADO Y DESCIFRADO

1) ENTIDAD B CODIFICA SU MENSAJE COMO UN NUMERO
x TAL QUE 0 <= x < m
2) ENTIDAD B CIFRA EL MENSAJE "X" CALCULANDO
y = T(x) mod m
Y ENVIA EL CRIPTOGRAMA "y"A LA ENTIDAD A.
3) LA ENTIDAD A DESCIFRA EL CRIPTOGRAMA "y" CALCULANDO
z = T(y) mod m
4) LA ENTIDA A OBTIENE z = x

Figura 2. Especificación de un sistema criptográfico estilo RSA basado en polinomios de Chebyshev.

misil balístico intercontinental con múltiples cabezas nucleares se puede utilizar la tecnología de compartición de secretos y dividir la clave de disparo entre un colectivo numeroso de personas de muy elevada responsabilidad.

Limitaciones de los esquemas de compartición de secretos incondicionalmente seguros

1) Cada fragmento del secreto debe ser al menos tan grande como el propio secreto. Este resultado se basa en la teoría de la información. Dados (k-1) fragmentos no se debe poder determinar información alguna acerca del secreto. Por tanto, el fragmento final debe contener tanta información como el propio secreto.

2) Todos los esquemas de compartición de secretos utilizan bits aleatorios. Para distribuir un secreto de un bit entre un colectivo umbral de "k" participantes se necesitan k-1 bits aleatorios. El fragmento final contiene tanta información como el secreto, pero los otros k-1 fragmentos aún proporcionan información relevante de forma individual. Esta información no puede ser el secreto de modo que debe ser aleatoria.

Desarrollo de un mecanismo de acuerdo de claves secretas entre dos entidades finales estilo D-H basado en polinomios de Chebyshev

Para intercambiar un secreto entre dos entidades que se comunican a través de una red sin transportar por dicha red información sensible, se desarrolla un mecanismo estilo D-H (Diffie-Hellman) basado en la utilización de polinomios de Chebyshev. Los polinomios de Chebyshev de primera clase se caracterizan por la siguiente especificación de recurrencia:

$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$, donde:
$T_0(x) = 1$;
$T_1(x) = x$;
$T_2(x) = (2x^2 - 1)$;
$T_3(x) = (4x^3 - 3x)$;
$T_6(x) = (32x^6 - 48x^4 + 18x^2 - 1)$.

Así mismo, se verifica la propiedad conmutativa:

$T_m(T_n(x)) = T_{m.n}(x) = T_n(T_m(x))$.

Dicho mecanismo se describe de la siguiente forma:

1) La entidad emisora A crea dos números enteros positivos y primos "p" y "g" tal que g < p ("g" es menor que "p"); por ejemplo p=89, g=7.

2) La entidad emisora A elige un número entero secreto "m" tal que 0<m<p (está comprendido entre cero y "p"); por ejemplo m=2.

3) La entidad emisora A calcula:
$a = T_m(g) \bmod p$
En este caso:
$a = T_2(7) = 2 \cdot (7^2) - 1 \bmod 89 = 97 \bmod 89 = 8$

4) La entidad emisora A envía a la entidad receptora B: (p, g, a) en este caso (p=89, g=7, a=8).

5) La entidad receptora B elige un número entero secreto "n" comprendido entre cero y "p" (0<n<p), por ejemplo n=3.

6) La entidad receptora B calcula:
$b = T_n(g) \bmod p$.
En este caso:
$b = T_3(7) = 4.(7^3) - (3 \cdot 79 \bmod 89) = 1351 \bmod 89 = 16$.

7) La entidad receptora B envía a la entidad emisora A el valor "b", en este caso b = 16.

8) La entidad emisora A calcula la clave secreta compartida:
$k = c = T_m(b) \bmod p$, en este caso:
$c = T_2(16) = 2 \cdot (16^2) - 1 \bmod 89 = 511 \bmod 89 = 66$.

9) La entidad receptora B calcula la clave secreta $k = d = T_n(a) \bmod p$, en este caso:
$d = T_3(8) = 4.(8^3) - 3 \cdot 8 \bmod 89 = 2024 \bmod 89 = 66$.

El número entero "c" de la entidad A y el número entero "d" de la entidad B constituye la clave secreta compartida ya que ambos han calculado $T_{m.n}(g) \bmod p$. Las entidades correspondientes A y B han generado la misma clave secreta k = 66 que también es:
$T_6(7) \bmod 8 = 3650401 \bmod 89 = 66$.

Dado el polinomio de Chebyshev $T_n(x) \bmod 11$; si x=3, para n=0, 1, 2, . . ., 23 los resultados son:
1, 3, 6, 0, 5, 8, 10, 8, 5, 0, 6, 3, 1, 3, 6, 0, 5, 8, 10, 8, 5, 0, 6, 3; donde se observa como período el valor 12.

Si x=0 se obtienen los valores:
1, 0, 10, 0, 1, 0, 10, 0, 1, 0, 10, 0 cuyo período es 4.

Para x=1 los valores son:
1, 1, 1, 1, 1, 1, 1, 1 con período 1.

Para x=2 los valores son:
1, 2, 7, 4, 9, 10, 9, 4, 7, 2, 1, 2 cuyo período es 10, etc.

La figura 2 muestra un criptosistema estilo RSA basado en polinomios de Chebyshev.

Consideraciones finales

Los protocolos criptográficos permiten establecer determinadas interacciones entre una o más entidades con objeto de llevar a cabo un cierto objetivo. De hecho, el cifrado y la firma digital pueden verse como un caso especial de protocolos criptográficos, ejemplos de protocolos criptográficos son la gestión de claves, la autenticación de usuario, etc. Podemos preguntarnos ¿por qué necesitamos la criptografía?, la respuesta aparece al considerar las siguientes cuestiones:

(i) Si la confidencialidad y la precisión de la información tienen valor, entonces debería protegerse con un nivel adecuado.

(ii) Si la revelación no autorizada o la alteración de la información puede dar lugar a un impacto negativo en la organización, empresa o unidad de negocio entonces debería aplicarse la criptografía como posible salvaguarda ó contramedida.

Las personas piensan en cosas distintas cuando se habla de criptografía, los niños juegan con cifradores de juguete y con lenguajes secretos. Sin embargo, estos artilugios infantiles poco tienen que ver con la seguridad real y el cifrado robusto. El cifrado robusto (con algoritmos estándar como AES, IDEA, 3DES, RSA, etc. y otros no estándar para entornos de propósito especial, por ejemplo basados en cifrado de flujo) es la clase de cifrado que se puede utilizar para proteger la información de valor real contra delincuentes organizados, empresas multinacionales, gobiernos, etc.. El cifrado robusto se utilizó en un principio para cuestiones militares y diplomáticas, sin embargo en la sociedad de la información y del conocimiento actual se ha convertido en uno de los pilares centrales para mantener la privacidad, confidencialidad, integridad, autenticación, para la identificación de todo tipo de entidades, etc.

En la sociedad de la información y del conocimiento donde nos movemos el significado tecnológico de la criptografía es para la supervivencia global de millones de individuos. La criptografía se ha convertido en una herramienta de primer orden para asegurar la confianza, privacidad, anonimato, control de acceso, pagos de forma electrónica, seguridad corporativa, votación electrónica, mantenimiento de historiales y control de constantes vitales en hospitales, etc. Las cuestiones de seguridad de los sistemas de información son clave hoy en día y se esta observando una unión cada vez más estrecha de esfuerzos por parte de un creciente número de disciplinas de conocimiento, por ejemplo tecnológicas, organizativas, administrativas, legales, etc. con objeto de abordar esta área actualmente de interés creciente.

Actualmente, la criptografía es la clave para construir bloques de soluciones de seguridad (en móviles con tarjeta inteligente SIM, en cajeros automáticos, en sistemas informáticos de entidades financieras, en sistemas de computación de hospitales, etc.).

La criptografía débil tira abajo a la seguridad debido a:

(i) Confiar en una mala o defectuosa configuración por parte de empleados cómodos.

(ii) Controles de exportación que reducen el tamaño de claves, etc.

(iii) La potencia de computación cada día es mayor.

(iv) Los progresos en criptoanálisis incluyendo errores en pruebas.

En algunos casos la criptografía que es ineficiente o difícil de configurar se inhabilita o se salta. Con la criptografía no significa que se tenga seguridad ya que:

(i) Los requisitos o especificaciones pueden ser incorrectas.

(ii) Puede haber errores en la implementación.

(iii) Errores en el protocolo criptográfico.

ESQUEMA UMBRAL DE COMPARTICIÓN DEL SECRETO "s" CON DISPERSIÓN DE INFORMACIÓN (k=3, n=5) SOBRE Z_{13}.

Sea el secreto s = 7811

Método: Se crea un polinomio de grado (k-1) donde sus coeficientes son "k" trozos del secreto (en este caso 7, 8, 11)

$$p(x) = (7x^2+8x+11) \bmod 13$$

Posibles fragmentos del secreto a compartir son los puntos:

(1. 0), (2, 3), (3, 7), (4, 12), (5, 5), . . .

Con "k" fragmentos se puede recuperar "s".
Con (k-1) fragmentos imposible averiguar "s".

Figura 3.- Desarrollo de un Esquema umbral de compartición de secreto con dispersión de información (k=3, n=5) sobre Z_{13}

Por tanto, se necesita una gestión de la seguridad (que engloba las tres funcionalidades de prevención, detección y respuesta) y nunca olvidar a la ingeniería social donde el componente humano puede tirar abajo la criptografía más robusta revelando claves, etc..

La figura 3 muestra un desarrollo de un esquema de compartición del secreto s = 7811 con dispersión de información del tipo (k=3, n=5) sobre Z_{13}. o

Bibliografía

- Areitio, J. "Análisis y desarrollo de cripto-sistemas probabilísticos". Revista Española de Electrónica. nº 586. Septiembre 2003.
- Areitio, J. "Diseño, síntesis y monitorización de cripto-sistemas simétricos ". Revista Española de Electrónica. nº 595. Junio 2004.
- Buchmann, J. "Introduction to Cryptography. Undergraduate Texts in Mathematics". 2nd Edition. Springer Verlag. 2994.
- Katzenbeisser, S. "User's Guide to Cryptography and Standards". Artech House Publishers. 2004.
- Smart, N. "Cryptography: An Introduction". McGraw-Hill. NY. 2003.
- Spillmann, R.J. "Classical and Contemporary Cryptology". Pearson Education. 2004.