

Revolucionario Sistema Criptográfico Simétrico

Marcelo Abdala nos cuenta: Cuando comenzamos a desarrollarlo, no creíamos que lo podíamos hacer, hasta que lo hicimos. A partir de ahí nos dimos cuenta, que su correcta implementación en distintos ámbitos podría solucionar un tema, hoy en día muy cuestionado : ' LA SEGURIDAD E INTEGRIDAD DE LA INFORMACIÓN ' a partir de la criptografía 'en serio'.

Partiendo del hecho que la criptografía de llave pública es un complemento de la llave privada, porque no nos puede garantizar muchas cosas (certificación de las certificadoras, que quien nos envía una llave sea quien dice ser, etc..), y que las herramientas criptográficas que llegan al país no son las mejores...nos focalizamos en el estudio simétrico, descartando para su funcionamiento todo lo conocido hasta la fecha en la materia. Esto nos permitió esquivar las gigantescas formulaciones, con operaciones entre bits, potenciación de números primos, etc.. que se necesitan hoy para hacer creer que un método es seguro.

A partir de nuestro algoritmo, vemos que podrá ofrecerse de una vez por todas seguridad informática que incluya criptografía segura para proteger información sensible en las empresas, evitando los perjuicios que podría ocasionarle si cayera en manos de sus competidores o empleados desleales. Desde hace unos meses cuando empezamos a perfeccionarlo, nos dimos cuenta que la posibilidad de potenciarlo es permanente, lo que pretendo decir es que si las computadoras fuesen miles de veces superior a lo que son hoy en día, nuestro algoritmo se potenciaría paralelamente, manteniendo intactas sus características).

Si bien un archivo encriptado no impresiona si no se lo fundamenta científicamente, el único camino que tenemos x el momento de enunciar lo realizado, es el axiomático, a los efectos de no exponer el método, pero las pruebas realizadas por nosotros, y algunas empresas que se nos acercaron confirman lo expresado : Un código generado a partir de nuestra codificación no puede ser quebrado, ya que utilizamos para relacionar las burguesas estructuras matemáticas, un método no usual hasta la fecha.

Hoy en día existe mucha gente afirmando haber desarrollado algoritmos interesantes, pero siempre es importante remitirse a las pruebas y exámenes, y hasta ahora los únicos reprobados son los que nos examinaron, ya que ninguna de las pruebas a las que sometieron a nuestro código resultó exitosa (para ellos..), y en ningún momento pudieron descodificar un texto encriptado, inclusive dándoles el texto de origen, sumado a los diversos textos que nos mandaban para que les encriptemos.

Lo logrado no nos permite coincidir con las afirmaciones de la ciencia acerca de los ensayos de calidad, que dicen que el resultado de testear un cifrado puede ser de calidad alta pero inseguro, y nunca al revés porque indicaría su vulnerabilidad ante un ataque por criptoanálisis diferencial. (En nuestro caso no es aplicable - ver característica 9-)

Este desacuerdo se debe a que las herramientas de medición utilizadas actualmente, y sin duda, óptimas para otros sistemas criptográficos, no son ni remotamente las apropiadas para evaluar la esencia de nuestro desarrollo en particular.

Sintetizando, podemos enunciar que logramos el 'ALGORITMO SIMÉTRICO MAS POTENTE DE LA HISTORIA INCAPAZ DE SER QUEBRADO EN TIEMPO Y FORMA CON

CARACTERÍSTICAS TAN INÉDITAS COMO ASOMBROSAS' que lo convierten en único, y determinan que solo puede ser atacable por fuerza bruta.

También, y por lo que acabamos de mencionar, es que estamos en condiciones de afirmar que ninguna de las grandes potencias del mundo dispone hoy del Hardware suficiente para realizar dicho ataque (Esto incluye a la última supercomputadora que procesa cerca de 60 billones de cálculos/seg , y a la que está en desarrollo que procesará cerca de 500 billones.

CARACTERÍSTICAS :

1) Posee una estructura por demás de simple y elemental, que a primera vista produce una engañosa sensación de fragilidad (es una de sus fortalezas). La confección de los parámetros necesarios para su funcionamiento está sustentada en operaciones matemáticas, pero en el desarrollo del algoritmo se prescinde por completo de ellas. En esta etapa y como consecuencia de la forma en que se realizan las mencionadas combinaciones, es cuando se potencia la aleatoriedad propia del sistema, y por tal motivo no existe posibilidad alguna de decodificar el encriptado, ya que aún 'conociendo el método', sino se poseen los parámetros exactos, resulta imposible para cualquier mente humana y/o computadoras arribar a los puntos de partida correctos, a los cuales no se accede 'a través de ningún tipo de operación matemática'.

2) Su clave es Simétrica, y en el producto que hemos desarrollado, su tamaño finito de aplicación excede los 800 millones de caracteres, sin repetición de secuencia de valores.

3) Interactúan simultáneamente entre sí un mínimo de 5 claves.

4) No existe posibilidad de descubrir La clave en su transmisión, porque no es 'TRANSMITIDA' (cosa que no habitual en otros simétricos)

4) 'No efectúa operaciones entre Bits', no se trata de un PRNG (Pseudo Random Number Generator), ni tampoco de un Xorador de pad Largo (debido a que no trabajamos con bits), por lo cual todo Test estadístico conocido que se le efectúe, no es de utilidad para evaluarlo, considerando que los mismos no medirían correctamente la calidad del texto cifrado.

Verificamos esto tras las prácticas a las cuales fue sometido, por algunas empresas. (Test Universal de Maurer para medir el aumento de entropía informacional)

El resultado obtenido, aparentemente pobre y no aceptable por los principios en los que hasta hoy se basa la ciencia (y que de ahora en más , seguramente deberá revertir) criptográfica para determinar si un método es seguro y de alta calidad, sirvió para confirmar lo que por anticipado enunciamos que iba a arrojar :

'Pésimas propiedades estadísticas'.

Es decir, un diagnóstico totalmente equivocado producto de haberlo realizado con herramientas 'no adecuadas', tanto para evaluar su esencia, como para reflejar la potencia real del sistema.

5) Los números que representan los valores no surgen de ningún cálculo o sistema de ecuaciones (No se utilizan matrices, ni determinantes, ni residuos, ni potencias, ni otros sistemas poligráficos).

5) El mismo mensaje original, puede arrojar 380.000 mensajes cifrados diferentes con un determinado tamaño de clave, e incrementarse a más de 1.000.000, si la misma se extiende.

6) Un análisis rápido y superficial, puede sugerir existe alguna semejanza con la idea de la teoría de Shannon, pues la clave que logra desarrollar, es de suficiente tamaño y variación, pero difiere sustancialmente de la misma, tanto porque la confección de su estructura se realiza por caminos diametralmente opuestos, como porque a diferencia de lo que el postulaba, ésta puede reutilizarse entre 6 y 300 millones de veces sin necesidad de descartarla, ya que con cada implementación, la misma se autogenera de diferente manera.

7) La fortaleza mayor reside en la perfecta conjunción entre la esencia absolutamente original del método con la cual fue concebido y la extensión de la clave, que a diferencia de lo que sucede con otros algoritmos, no está sujeta a los 256 códigos de la tabla ASCII, sino que puede trabajar con miles de símbolos realmente diferentes.

8) Utiliza solo 10 dígitos en lugar de la vetusta tabla ASCII, para graficar el encriptado, pudiendo trabajar con menos.

9) ES UN método simétrico 'FUERTE' con alta redundancia de output (algo absolutamente inédito), pero fácil de entender, si leyeron el punto 7 y sobre todo el 8.

10) Garantiza en un 100 % la autenticidad, y la integridad de la información.

11) Mediante un ataque por fuerza bruta, demandaría cerca de 45.000 millones de años en analizarse entre el 10²⁰ e sus posibilidades, con una supercomputadora que procese cerca de 60 billones de calculos/seg.

12) En nuestro sistema no existe la aparición de frecuencias de repetición (Esto también lo hace diferente a cualquier otro sistema)

Si le interesa examinar mas a fondo el tema en cuestión, solo tienen que pedir lo que necesitan, y estamos a vuestra disposición para conversarlo

SICRIAL (Sistema Criptográfico Alógico) www.sicrial.com.ar (en construcción), Rosario, Argentina. Cuando lo esencial es invisible a los ojos.

Fecha artículo: 2002-05-12 03:07:08 - url artículo: <http://www.internautas.org/html/31.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org