

MdLock®

ALGORITMO PARA CIFRADO SIMETRICO DE FLUJO

*MDTechnology S.A.
28 de Julio del 2000*

El presente documento describe la novedosa solución criptográfica a los problemas de seguridad en el manejo de la información propuesta por MD Technology mediante su algoritmo MDLock®.

ANTECEDENTES

Desde hace siglos, la necesidad de proteger la información y la transmisión de esta a través de medios inseguros, ha tenido gran importancia para todos los países del mundo. Más aún, en las últimas décadas, debido al enorme desarrollo y utilización de la informática y las telecomunicaciones, la protección de la información se ha vuelto vital para el mundo empresarial y el ámbito personal. Una de las herramientas más utilizadas para proteger la información es la tecnología criptográfica, la cual permite cifrar los mensajes mediante una o varias claves para que estos no puedan ser interpretados a menos que se realice un proceso inverso o descifrado, el cual requiere volver a utilizar las claves. Existen en la actualidad algoritmos bastante seguros para realizar este proceso como DES y RSA. Sin embargo, al haber sido esta tecnología desarrollada en países que la consideran de importancia militar, los algoritmos están sujetos a leyes contra su libre exportación. Esto significa que estos países prohíben la exportación de tecnología que utilice estos algoritmos, o imponen restricciones que los debilitan que permiten aplicar técnicas de análisis criptográfico para descifrar la información sin poseer las claves. Esto ha dejado al resto de mundo expuesto a usar algoritmos débiles para resistir ataques de análisis criptográfico. Por esto M.D. TECHNOLOGY S.A. se propuso crear una solución superior incluso a los algoritmos utilizados dentro de países del primer mundo, que brindara a los usuarios de computadoras una tecnología para cifrar y descifrar información con el más alto nivel de seguridad. Tan alto que puede ser utilizado para las más complejas necesidades de seguridad nacional, pero tan eficiente que a la vez pueda ser aplicado con un mínimo de afectación en los tiempos de transmisión y almacenamiento de la información incluso en una computadora personal.

EL ALGORITMO MDLOCK

MDLOCK es un algoritmo para cifrado simétrico con un nivel de seguridad superior al de algoritmos como RC6 o DES. Este algoritmo utiliza un esquema diferente al manejo tradicional de paquetes de información a cifrar (56 bits, 64 bits, 128 bits, etc.). La tecnología se centra en el cifrado/descifrado mediante la generación de una cadena de

información única en el tiempo (en Inglés One Time Pad o también OTP) que se combina con el mensaje original. Sin importar si se utiliza la misma clave para cifrar un mismo mensaje, la OTP siempre será diferente. Por otro lado, al contrario de tecnologías de criptografía populares como PGP, las claves en el algoritmo MD Lock pueden ser muy pequeñas, y a pesar de ello proveer un nivel de seguridad más alto que el de algoritmos populares como DES. Lo más destacable de este algoritmo de cifrado es que gracias a la forma como se genera el OTP, puede ser utilizado tanto para el cifrado/descifrado de documentos estáticos como para el cifrado/descifrado de canales de comunicación que transmiten información en tiempo real con el mismo alto grado de seguridad.

MD Technology ha desarrollado una tecnología que permite superar las barreras teóricas y prácticas existentes para usar (inclusive en PCs, o chips, de pequeño tamaño y capacidad de procesamiento) de manera eficiente los únicos sistemas prácticamente invulnerables de cifrado conocidos, que en criptografía se denominan “generadores de OTPs”.

El Algoritmo MD Lock está compuesto de tres partes:

- a) Un Sistema de Codificación “Polimórfico” que genera la semilla o germen para la creación de una cadena de información única en el tiempo (OTP), a partir de un modelo matemático de codificación, el cual es también generado de por este Sistema de acuerdo al nivel de seguridad (complejidad del modelo) que le sea especificado.
- b) Un Algoritmo generador de una OTP de tamaño arbitrario, a partir una semilla de un tamaño variable que es producido por (a).
- c) Un algoritmo de cifrado y descifrado que se basa en los componentes (a) y (b).

A continuación se describe cada uno de estos componentes con más detalle

El Sistema de Encriptado Polimórfico.

El Sistema de Encriptado Polimórfico usa una tabla de substitución poli-alfabética, la cual asigna un subconjunto de símbolos de tamaño n a cada símbolo del alfabeto de entrada, para generar el alfabeto de salida. Obviamente, el alfabeto de salida es más grande que el alfabeto de entrada. A la tabla de substitución la denominamos el modelo matemático F y a través de este modelo matemático se definen las funciones de codificación C_F y decodificación D_F . Nótese que podemos considerar a C_F como una función de cifrado y a D_F como una función de descifrado, ambas usando el modelo matemático F como la clave en este proceso. Bajo este punto de vista denominamos a n el nivel de seguridad del modelo.

Las salidas de la función polimorfo son bastante difíciles de predecir. El único ataque factible sería un estudio estadístico de las frecuencias de aparición de cada símbolo de A y B (alfabetos de entrada y salida). Sin embargo, sería imposible recabar información suficiente para efectuar este ataque, debido por un lado a que esta función se aplica sobre las contraseñas (o la salida de alguna función hash sobre ellas) para obtener la semilla del generador de la OTP. Esto impediría tener un perfil estadístico viable tanto de los símbolos de A como de los de B . En consecuencia, podemos decir que la función polimorfo no presenta en principio ninguna posibilidad práctica de ser atacada con éxito, siempre y cuando se desconozca por completo el modelo matemático. Aún en caso de disponer de la

contraseña, parte del mensaje original, y una parte sustancial del modelo matemático, la calidad de la función generadora de la OTP es lo suficientemente buena como para que las posibilidades de descifrar un mensaje sean prácticamente nulas.

Algoritmo Generador de la OTP.

La función generadora de la OTP que se propone para el algoritmo MD Lock produce una secuencia de bytes de longitud arbitraria a partir de una cadena inicial – semilla o germen– de bytes de longitud múltiplo de 20. La secuencia es generada en bloques de tamaño menor al de la semilla pero que no siguen un patrón identificable de generación. Debido a que la secuencia puede ser infinitamente grande, el algoritmo es susceptible de ser utilizado en aplicaciones de telecomunicaciones. La función generadora del OTP tiene las siguientes fortalezas:

- a) Cada valor de la semilla genera un bloque cuya longitud es un fragmento de la propia semilla, por lo que en principio nunca podemos recuperar toda la semilla a partir de un fragmento de la secuencia.
- b) El procedimiento de generación de la semilla para el siguiente paso es bastante independiente del proceso de generación del bloque correspondiente de la OTP, por lo que sería bastante difícil combinar las posibles evidencias obtenidas a lo largo de diferentes bloques de OTP para recuperar la semilla inicial correspondiente. El mejor ataque que parece poder llevarse a cabo para recuperar un byte de una semilla de 160 bits, a partir de un fragmento de la OTP, tendría una complejidad que estaría por encima 2^{100} pasos, y los astronómicos requerimientos de memoria harían del todo inviable dicho ataque. Recordemos que la longitud de la semilla es arbitraria, y la complejidad de romper un fragmento de la OTP aumenta con el tamaño de la semilla. Para una semilla de 1600 bits, la complejidad aumenta a un valor mayor de 2^{900} por byte, lo cual no es alcanzado de manera eficiente por ninguno de los algoritmos conocidos de criptografía simétrica existentes hasta el momento.

Algoritmo para el Cifrado/Descifrado

Estos algoritmos son muy simples y consisten en utilizar los algoritmos descritos anteriormente para generar primero la semilla y luego la OTP para con esta hacer una operación de XOR y cifrar/descifrar el mensaje

BENEFICIOS DE LA TECNOLOGIA

A continuación se resumen algunas de las características que hacen a MDLock el mejor algoritmo de criptografía simétrica

- MDLOCK presenta un nivel de seguridad muy alto que le permite ser utilizado inclusive en aplicaciones de seguridad nacional.

- MDLOCK es un algoritmo muy eficiente que no produce un efecto significativo en el procesamiento de la información, ya sea que esta se almacene en un disco o que sea transmitida a través de una red. Esto permite utilizar el algoritmo en componentes de reducido tamaño y poder de procesamiento.
- MDLOCK presenta la capacidad de controlar la seguridad basándose en dos componentes que deben ser conocidos por las partes: la palabra secreta y el modelo matemático. El modelo matemático puede ser utilizado con diferentes palabras secretas.
- MDLOCK ha sido desarrollado fuera de países con restricciones de exportación. El algoritmo con toda su fortaleza y seguridad se encuentra disponible para todo el mundo
- MDLOCK le permite a los usuarios generar sus propios modelos matemáticos y utilizar las palabras secretas del tamaño que sea necesario, lo que garantiza el nivel de seguridad del cifrado y la invulnerabilidad ante un análisis criptográfico realizado por alguien más (incluso por MD Technology).

La aplicación del algoritmo MD Lock en los negocios o en cualquier campo de la actividad institucional o individual repercute positivamente en mejorar la seguridad y eficiencia de la gestión de la información sensible. El disponer de un sistema criptográfico para proteger documentos privados y/o su transmisión a través de medios inseguros, permite ahorrar tiempo invertido en reuniones personales o en la entrega persona a persona de la información. Además permite proteger la inversión muchas veces intangible de los secretos corporativos. Por otro lado permite establecer canales de comunicación seguros de acuerdo a niveles de jerarquía dentro de la misma organización y la posibilidad de establecer canales de comunicación seguros con los clientes para poder realizar transacciones a nivel mundial logrando la expansión y la globalización del negocio. Desde el punto de vista del derecho ciudadano a la privacidad de su información personal, el algoritmo M.D. Lock y cualquier aplicación basada en el algoritmo otorga a los individuos una herramienta para proteger ese derecho de manera efectiva. MDLock es la solución que nos permite verdaderamente mantener la privacidad sobre la información que consideramos valiosa para la seguridad y el desarrollo individual, empresarial y regional.