Miramontes Sarabia Luis Enrique

Agosto 26, 2019

Advanced Encryption Standard

La criptografía es una de las técnicas más populares para asegurar datos usando dos procesos, cifrado y descifrado. Para operar la criptografía se basa en cálculos matemáticos, algunas sustituciones y permutaciones con y sin llave. La criptografía moderna sigue los principios de confidencialidad, integridad, no repudio y autenticación. Uno de estos algoritmos es AES, algoritmo de cifrado por bloque publicado por el NIST y diseñado para reemplazar DES. Se seleccionó por medio de un concurso compitiendo contra otros cinco algoritmos, diseñado por dos belgas, Joan Daeman y Vincent Rijmen, su nombre original era Rijndel.

Se usaron tres criterios importantes para evaluar algoritmos en este concurso: Seguridad, uno de los aspectos cruciales en el concurso, se probó este rubro usando ataques teóricos y prácticos; Costo, se evaluó el costo de implementación e impacto en la eficiencia cuando se aplica a una gran variedad de dispositivos; Características de implementación, se mantuvo en mente la flexibilidad del algoritmo para implementaciones de hardware y software.

La estructura básica del algoritmo está basada en un método iterativo y no de tipo Feistel, se basa en redes de sustitución y permutación. Es capaz de manejar 128 bits de texto plano por bloque y con llaves de 129, 192 y 256 bits, que determinarán el número de rondas que usará el cipher, siendo 10, 12 y 14 respectivamente.

El proceso de cifrado se basa en el número de rondas, cada ronda contiene cuatro subprocesos: Sustitución de bytes: Esta etapa depende de una S-box no lineal, de acuerdo a los principios de difusión y confusión de Shannon este proceso brinda mucha más seguridad; Intercambio de filas, el siguiente paso consiste en hacer desplazamientos a nivel byte hacia la izquierda en las filas, la primera fila no se moverá, la segunda sólo un espacio, y así sucesivamente; Mezcla de columnas, otro paso crucial es la mezcla de columnas, se multiplica la matriz obtenida con los pasos anteriores con una matriz establecida; Round Key, el paso más vital en el cifrado, se estructuran las matrices de la llave y plaintext para que compartan una relación y la salida depende de estas dos, también se combina la subllave usando un XOR con la matriz obtenida.

Miramontes Sarabia Luis Enrique

Para el descifrado se usan las operaciones inversas de las aplicadas cuando se realizó el cifrado, es similar a éste ya que simplemente se usa el orden inverso de las operaciones.

Como conclusión AES es el estándar definido actualmente por la NIST, tiene un gran nivel de seguridad y sus aplicaciones son muchas gracias a la gran flexibilidad que el algoritmo tiene. Lo usamos muchas veces durante nuestra vida cotidiana, ya que se usa para cifrar mensajes, conexiones de internet, routers y muchas otras herramientas que necesitamos día a día. Cuando lo comparamos contra DES, AES muestra un nivel muy superior de seguridad, desde teniendo una clave mucho más larga de hasta 256 bits, en comparación a los 56 bits que tenía DES, que si recordamos el artículo leído anteriormente, era una de sus debilidades más importantes. Además que AES es mucho más rápido que DES, aunque no más rápido que Twofish, que fue otro candidato del concurso de selección. Esto me da curiosidad, ¿cuál es la razón de no elegir a Twofish aun siendo más rápido y también seguro?