Integridad de Mensajes

Nos centramos en adversarios activos que pueden modificar un mensaje en ruta. La integridad del mensaje asegura que un mensaje transmitido por el emisor es original y no ha sido modificado por un tercero antes de ser recibido. La integridad del mensaje no asume el secreto, la integridad puede ser necesaria también para mensajes en texto plano. La integridad del mensaje requiere que el emisor tenga una clave secreta desconocida para el adversario.

Message Autentication Codes (MAC)

Par de algoritmos para firma y verificación, ambos son probabilísticos. El algoritmo de firma devuelve un tag cuando recibe una clave y un mensaje. El algoritmo de verifiación devuelve una decisión binaria (aceptar o rechazar) cuando recibe una clave, un mensaje y un tag. Los tags deben ser cortos en comparación con el mensaje para minimizar el tamaño de la transmisión.

$V(k,m,t) = accept -> IF -> S(K,M) = t$

Seguridad MAC

- Para sistemas MAC deterministico, la seguridad MAC es equivalente a que S sea impredecible o indistinguible de un numero aleatorio
- Para sistemas MAC randomizados, la seguridad implica que el adversario es incapaz de producir un mensaje y un tag validos aun sabiendo estos.

Numeros pseudoaleatorios (PRF) como sistemas MAC