



TECNOLÓGICO
NACIONAL DE MÉXICO



INSTITUTO TECNOLÓGICO DE CANCÚN

**INGENIERÍA EN
SISTEMAS COMPUTACIONALES**

FUNDAMENTOS DE TELECOMUNICACIONES

**NOMBRE DEL ALUMNO:
CHAN BURGOS JOSE REYES**

**HORARIO
LUNES A JUEVES
5:00 PM – 6:00 PM**

**PROFESOR
ING. ISMAEL JIMENEZ SANCHEZ**



TECNOLÓGICO
NACIONAL DE MÉXICO



MITM (Ataques Man-In-The-Middle.)

El término Man-In-The-Middle (hombre en el medio en inglés) denota un ataque de encriptación en una red de ordenadores. Es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas y procurar que ninguna de las víctimas conozca que el enlace entre ellos ha sido violado. El ataque MitM es particularmente significativo en el protocolo original de intercambio de claves de Diffie-Hellman, cuando este se emplea sin autenticación.

En un ataque de MITM, el atacante tiene control total de la información entre dos o más socios de enlace. Esto permite al atacante leer, influir y manipular la información. El atacante está reflejando la identidad del primero y del segundo interlocutor de comunicación, de modo que puede participar en el canal de comunicación. La información entre los dos hosts está cifrada, pero es descifrada por el atacante y transmitida (ver también servidor proxy).

