ABSTRACT

Wireless Fidelity or WiFi technology is used as a Wireless Local Area Network or WLAN. One of the obstacles is the competence of the WLAN vulnerability to network security aspects. WPA-PSK is one of the methods of wireless security system that is already widely used and uses the RC4 algorithm. The weakness of the RC4 algorithm is the best known Bit Flipping Attack or BFA. BFA attack aimed to find part or all of the plaintext from the ciphertext without knowing the key.

In this final project proposed CRC-32 bits as a technique to assign a value to the plaintext prior to encryption. Addition of CRC-32 on the RC4 algorithm aims to strengthen the plaintext during the encryption process. Ciphertext encrypted form will then be sent to the recipient. Then in testing, the wireless media, the attacker did Bit Flipping Attack (BFA) by changing one bit of the ciphertext from 0 to 1 or 1 to 0, during the process of delivery. In the decryption process will be checking again whether the data received is damaged or not by reviving the keys and checking CRC values match or not.

From the results of tests performed on RC4, the addition of CRC in plaintext before encrypting managed to increase resistance to attack RC4 Bit Flipping Attack. The quality of the modified CRC RC4 is affected by the avalanche effect and the execution time of computing time. By using the same plaintext with different keys, as well as using different plaintext with the same key, each value of the avalanche effect produces equally good, ranging from 45% to 60% but there is a few result that give AE under 45 %, because of the different characters and key and seed that added. In RC4 with CRC-32, computation time for encryption / decryption become longer than RC4 without CRC-32 adding.

Keywords: *RC4, Bit Flipping Attack, CRC, Encryption, Decryption, Avalanche Effect.*