ABSTRACT

Security and confidentiality of data is an important aspect in data communications, especially in wireless network lan. Nearly many people now knows what is wireless lan. Many people know communication on the wireless lan uses radio waves, so many people want to explore their knowledge to attack the system. One way to maintain the security and confidentiality of the data is encoded using a technique called cryptography. Therefore, in this final project to create applications like wireless lan where there are senders and receivers.

Application systems on tihis Final Project include standardization wireless lan of WEP, WPA, WPA2. WEP uses the RC4 algorithm to standardize 64-bit, WPA uses 128 bit RC4 standardization, and to WPA2 uses AES algorithm 256 bit CBC mode standardization. In this aplication, authors make variance of key length to 256 bits and 1024 bits in WEP and WPA protocols to increase the level of WEP and WPA security, because it is based on the concept if the longer of the key sizes its make the encryption and decryption process time and brute force time will take the long time.

From the results of performance of the time of encryption and decryption process show the length key will be take the long time to proces, based on to brute force calculation show if the length key will be influence to time process of brute force, as well as the calculation of IV, if the length of IV its show the repetition of calculation IV will be take the long time. So WPA is very strong than WEP, but althougt the WPA uses 48 bits IV its important to repetition calculation. So WPA2 that uses AES is more secure than WEP and WPA althought uses 16 bits IV, its because the scheduling of AES is very difficult, so it make the cryptanalis dificult to attack the system.

Key Words : WEP, WPA, WPA2, AES, RC4, CBC, IV