Vincent Fiore

Cryptography Assignment 6

6.2. In this scenario, the attacker would have the values of C and the value of A when B||C or B when A||C. If the sender then authenticates A||D, he will then have the value of B||D since he has all parts of the equation. IE: He has figured out A, B, C, D and all of the values they result to when combined.

6.3. This statement is mathematically true because the attacker is able to figure out all of the information that results from this longer equation. Since he has *M(a)* and *M(b),* and *b || (M(b) xor M(a) xor b)* equals *M(a||b),* it is clear that *(M(b) xor M(a) xor b)* equals simply *a*. Since he already has the product of *M(a||b),* he will have the MAC of this full equation that he never intercepted.

6.6. The resulting MAC is

BE 48 C6 59 EE 04 1E DC 12 AF 8D 47 96 07 76 18 99 02 E0 11 B1 C6 A5 40 56 A5 B1 0D 96 18 FA 4A