JACOB S. SANTOS **10/21/24**
BSCOE 4-1 **Dr. Ariel Sison**

Assignment – Mix Column

Determine the MixColumn value of NB5 to NB8. Show your solutions.

Nb5 = (b5 * 02) XOR (b6 * 03) XOR (b7 * 01) XOR (b8 * 01)

= E(L(b5) + L(02)) XOR E(L(b6) + L(03)) XOR E(L(b7) + L(01)) XOR E(L(b8) + L(01))

= E(L(EB) + L(19)) XOR E(L(93) + L(01)) XOR E(L(C7) + L(00)) XOR E(L(20) + L(00))

= E(26 + 19) XOR E(7A + 01) XOR C7 XOR 20

= E(3F) XOR E(7B) XOR C7 XOR 20

= CD XOR AE XOR C7 XOR 20

= **84**

Nb6 = (b5 * 01) XOR (b6 * 02) XOR (b7 * 03) XOR (b8 * 01)

= E(L(b5) + L(01)) XOR E(L(b6) + L(02)) XOR E(L(b7) + L(03)) XOR E(L(b8) + L(01))

= E(L(EB) + L(00)) XOR E(L(93) + L(19)) XOR E(L(C7) + L(01)) XOR E(L(20) + L(00))

= EB XOR E(7A + 19) XOR E(FC + 01) XOR 20

= EB XOR E(93) XOR E(FD) XOR 20

= EB XOR 3D XOR 52 XOR 20

= **a4**

Nb7 = (b5 * 01) XOR (b6 * 01) XOR (b7 * 02) XOR (b8 * 03)

= E(L(b5) + L(01)) XOR E(L(b6) + L(01)) XOR E(L(b7) + L(02)) XOR E(L(b8) + L(03))

= E(L(EB) + L(00)) XOR E(L(93) + L(00)) XOR E(L(C7) + L(19)) XOR E(L(20) + L(01))

= EB XOR 93 XOR E(FC + 19) XOR E(7D + 01)

= EB XOR 93 XOR E(16) XOR E(7E)

= EB XOR 93 XOR 95 XOR 60

= **8D**

Nb8 = (b5 * 03) XOR (b6 * 01) XOR (b7 * 01) XOR (b8 * 02)

= E(L(b5) + L(03)) XOR E(L(b6) + L(01)) XOR E(L(b7) + L(01)) XOR E(L(b8) + L(02))

= E(L(EB) + L(01)) XOR E(L(93) + L(00)) XOR E(L(C7) + L(00)) XOR E(L(20) + L(19))

= E(26 + 01) XOR 93 XOR C7 XOR E(7D +19)

= E(27) XOR 93 XOR C7 XOR E(96)

= 26 XOR 93 XOR C7 XOR 40

= **32**