Carl Cortez

CIS 628

Contrast AES and DES

Lab 6

Task 1) First, use the small single box diagram (plaintext and key in, ciphertext out) for each to discuss similarities and differences.

For the DES cipher, we can encrypt blocks of 64 bits using a key of 56 bits. Each block of plaintext encryption is handled in 16 similar rounds. DES is considered a Feistal cipher because its encryption and decryption are almost identical. With DES, we hit rounds of Expansion, XOR operations, Substitution (S-Box), and Permutation. DES is older than AES and shows it by having well known vulnerabilities. DES uses S-boxes that are roughly put together at random just to fulfill certain properties.

AES in comparison is byte oriented and can have a key of 128, 192, and 256 bits. We have a variety of rounds that can occur depending on the key length. Instead of a Feistal cipher, AES is based on using substitution and permutation. Since AES is younger (potentially more tech savvy), it's more secure than the DES cipher. Our AES rounds use Byte Substitution, Shift Row, Mix Column, and Key Addition. AES uses S-boxes that have a strong algebraic structure.

Both AES and DES serve their purposes as symmetric block ciphers. Both use a single key for encoding and decoding their data respectively. Both the encrypted DES blocks and AES key sizes are divisible by 64. If I think of any additional similarities, I will add them to this section.

Task 2) Explain the full diagram of each algorithm (each step/layer from each round, including the transforms), again focusing on similarities and differences.

For DES, we have our 64 bit plaintext go through an initial permutation to rearrange the bits. DES continues to split our input into a left and right portion. Each portion goes through 16 similar rounds. As mentioned above, each round consists of Expansion, XOR operations, Substitution (S-Box), and Permutation. Expansion takes the right portion and expands it to a 48 bit right half. XOR takes the new 48 bit right half and XORs with a 48 bit subkey; giving us a 48 bit output (again). S-box takes us from a 48 bit output to 32 bits. Permutation is done on the 32 bits to produce a 32 bit permuted output. After the rounds have completed, the 64 bit ciphertext is complete.

AES takes 2x DES' plaintext bits (at the least) along with a key to form a block. We do not have a left and right portion to deal with during AES. The number of rounds varies in accordance to the plaintext instead of a flat 16 for DES. Byte Substitution starts our round off and is done with an S box to the entire block. Rows are shifted during the round since our block is in a matrix format. Columns are respectively shuffled from right to left. Key Addition performs an XOR on the block and key. We're given ciphertext which is the same length as the plaintext.