Homework 6: Contrast AES and DES

Mudit Vats
mpvats@syr.edu
5/27/2020

Table of Contents

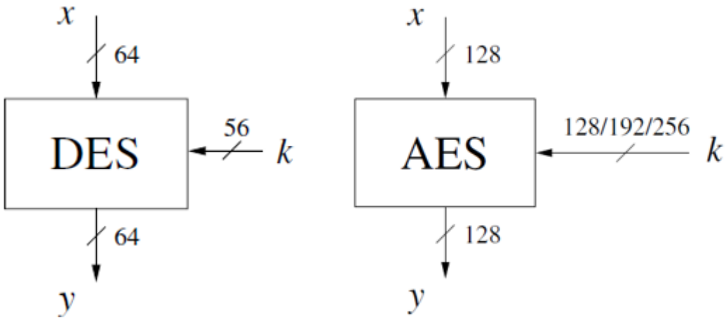
Overview

This lab report presents compares and contrasts DES and AES.

- First, use the small single box diagram for each (x+key in, y out) to discuss similarities and differences.
- Then, explain the full diagram of each algorithm (each step/layer from each round, including the transforms), again focusing on similarities and differences.

Small Box Diagram

Compare and contrast DES (left) and AES (right), focusing on the small diagram.



Similarities

- Both DES and AES are symmetric block ciphers. As such, the same key is used for both encryption and decryption. Additionally, since they are block ciphers, the input operates on an entire block of data versus stream ciphers which encrypt bits as they come in.
- Both DES and AES algorithms are completely open. Like Kerckhoffs's principle, the algorithms are open, the key should be protected. Both algos have been heavily studied and scrutinized.
- Both DES and AES use confusion (substitution) and diffusion.

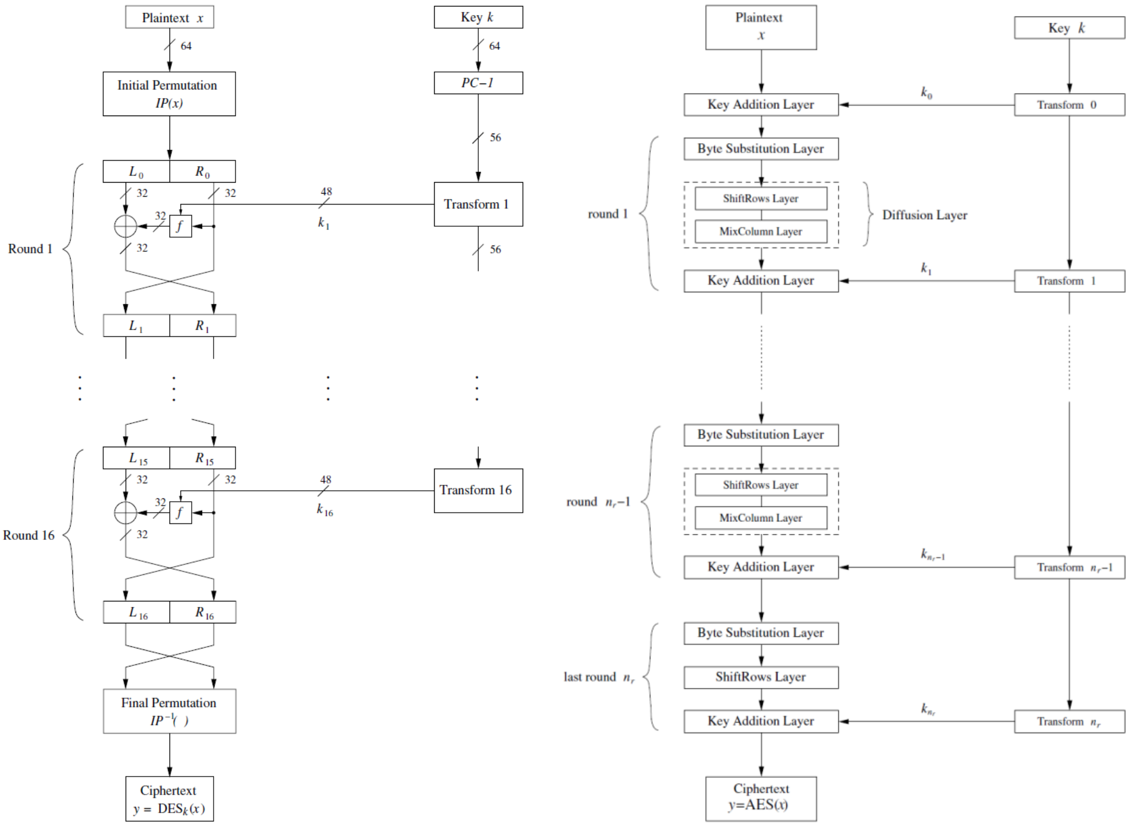
Differences

- DES was done as a top-secret endeavor by IBM/NSA. AES was borne from requests by NIST for a next generation cryptographic standard.
- DES operates on 64-bit blocks. AES operates on 128-bit blocks. This is the x input for both.
- DES uses a 56-bit key. AES can use 128, 192 and 256 bit keys (i.e. three key lengths). This is the k key input on the right side.
- DES outputs cipher text in 64-bit blocks, which is consistent with the 64-bit input. Likewise, AES outputs cipher text in 128-bit blocks, which is consistent with the 128-bit input. The difference is in the block size.
- DES is now considered inadequate for cryptographic uses due to key size. AES should be used and should stand the test of time even with quantum computing (as long as you use 256-bit key!).

- DES was primarily built for hardware implementations and, as such, software performance may not be as optimized. Per our course learnings, AES is efficient in software and hardware.

Full Diagram Comparison

Compare and contrast DES (left) and AES (right), focusing on the algorithm details.



Algorithm Overview

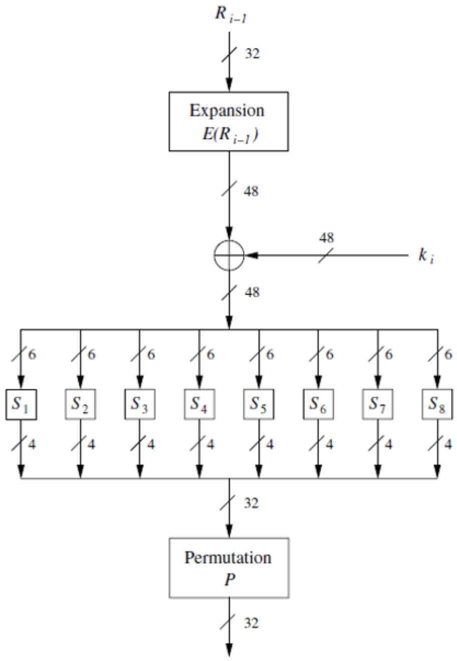
This section describes, in brief, the major functional units of DES and AES. The following sections then calls-out specific similarities and differences between the two algorithms.

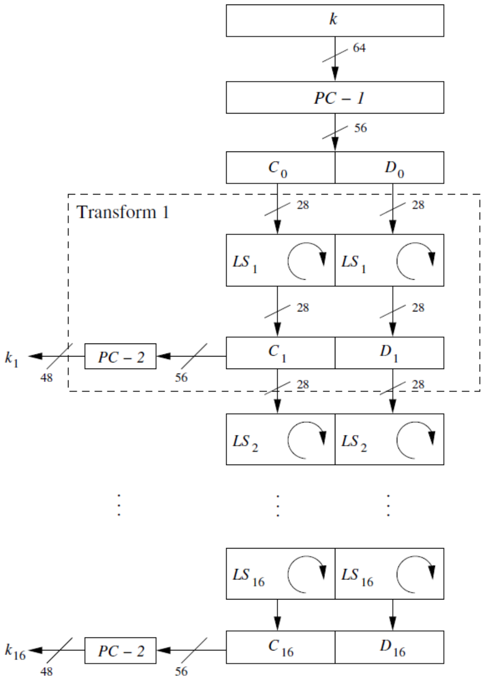
Data Encryption Standard (DES)

The follows bullets give a brief description of each functional unit.

- **Initial Permutation IP(x) and Final Permutation IP^{-1}(x).** These are bit permutations at the start and end of the algorithm. Per our class, they do not provide any increased security since one simply undoes the other.
- **Lx/Rx.** These are the left and right half of the bits used by algorithm. So, these are each 32-bit wide and are manipulated 32-bits at a time; i.e. left half gets XOR'd with the results of the f-function, then is used as the input to the next Rx half.

- **f-Function (below left).** This functional unit takes as input the Rx (right half), expands it to 48-bits, XOR's it with the key and then applies the S-boxes to it. That is, 48-bits go in, 32-bits come out. The S-box creates the confusion. Finally, a permutation is applied to create the diffusion of bits.





- As previously mentioned, the output of the f-Function is used to XOR with the Lx, left half.
- **Key Schedule (above right).** These are the steps to generate a new key (or subkey) based on the initial key (56-bits) and then subsequent keys. This consists of an initial expansion to add parity bits (64-bits), followed by a contraction and permutation (56-bits) and a division of Cx and Dx bits which are now 28-bits in size each. Shifts are performed and a final permutation to get the final 48-bit key, which as you may recall, is fed into the f-Function.
- This process would be considered a **Round** and the rounds are repeated 16 times for encryption and decryption.

Advanced Encryption Standard (AES)

The following bullets give a brief description of each functional unit.

- AES is built upon a **Layers** concept whereby each layer operates on the full 128-bit input and outputs 128-bits for the next layer. Unlike DES, where there are multiple units and several bit expansions, contractions and manipulations (i.e. like working on the left half at each round), AES operates on the same width of data throughout the layers.
- The next layer is the **Byte Substitution Layer** which applies the S-Boxes to each of the 16 bytes of input. Each S-Box is the same and, once applied, creates the confusion aspect of the algorithm.

- The next layer is the **Diffusion Layer**. It consists of two sub-units which are the ShiftRows Layer and the MixColumn Layer.
    - The **ShiftRows Layer** simply organizes the bytes into a matrix (bytes ordered column-wise down), and applies shifting rules for each row: row 1 no shift, row 2 left shift one position, row 3 left shift two positions and row 4 left shift three positions. This is actually a rotate as the byte on the left would move to the right and shifted, depending on the shift rule.
    - The **MixColumn Layer** applies Galois mathematics to move columns around. We didn't go into the details due to the mathematics, but both MixColumn and ShiftRows together help with the diffusion aspect of the algorithm.
- **Key Addition Layer** is where the key (or subkey) is applied to the input bits. In this layer, the input is XOR'd with the key. As the last step in a round, this layer takes the output of the Diffusion Layer and XOR's with the key.

Architecture Comparison

- **DIFFERENCE** DES based on Fiestel cipher. AES is based on Layers where each layer manipulates all bits of data at each layer.
- **SIMILAR** Both DES and AES follow a key schedule.
- **DIFFERENCE** DES is more complex in a way such that there are several units such as the f-Function, Lx/Rx and swapping halves (32-bits), bit translations from smaller to larger and larger to smaller. AES works on all bits of data at each layer (128-bit), less complex from bit manipulation perspective.
- **DIFFERENCE** DES operates on half the data at a time: 32-bit halves, one half at a time. AES operates on the full block size of 128-bit; i.e. all the bits.
- **SIMILAR** DES uses Initial Permutation IP(x) and Final Permutation IP^{-1} as its first and last step (even though they cancel each other out). AES uses Key Whitening (not to be confused with "teeth whitening"; sorry, I couldn't resist!) which is an initial XOR of the Plaintext with the Key Addition Layer (k0) and the final XOR with the Key Addition Layer K_{nr}, which adds to the complexity.
- **SIMILAR** DES and AES accomplish decryption by reversing the encryption order. AES, however, inverts each layer's functionality. Both decryptions start with the last encryption key and perform the rounds in reverse so that each stage undoes what the analogous encryption round did; so round 1 in decryption undoes what round 16 did for encryption.
- **DIFFERENCE** DES has 16 rounds for encryption and decryption. AES varies depending on key size: 128-bit goes 10 rounds, 192-bit goes 12 rounds, 256-bit goes 14 rounds.
- **DIFFERENCE** DES operates on each bit individually. AES works on 8-bit byte chunks, basically at byte-level versus the bit-level. Like AES, DES is still a block cipher, but there is a bit-level versus byte-level difference on data manipulation.

Key Schedule Comparison

- **SIMILAR** Both DES and AES have a key schedule that computes the round keys.
- **DIFFERENCE/SIMILAR** DES is based on Fiestel cipher where encryption and decryption are very similar simply using the reversal of the key schedule. There

is also inversion of layers in AES and some minor differences in layers (Key Addition Layer and MixColumn Layer encrypt/decrypt for last/first stages), but generally speaking, decryption process is same as encryption.

- **DIFFERENCE** DES based shifting and permuting values at each subkey generation. AES relying on Galois math to compute / transform each subkey value.

S-Box Comparison

- **SIMILAR** Both DES and AES use S-boxes for substitution.
- **DIFFERENCE** AES S-boxes are the same. DES S-boxes are different.
- **DIFFERENCE** AES S-box are same size bits in and same size bits out. DES has 6 bits going in, 4 bits going out.
- **DIFFERENCE** DES s-boxes origins are were designed in a clandestine manner such that the reason for their design wasn't given. There values were secretly chosen to prevent differential cryptanalysis attacks. AES s-boxes are based on Galois arithmetic (mathematical backing) and can be changed as long as the Galois properties hold (of course encryption and decryption would need to use the same S-box values).
- **SIMILAR** Both DES and AES prevent differential cryptanalysis attacks by "confusing" the data via the S-Boxes.
- **DIFFERENCE** DES has 48-bits going into the S-Boxes and 32-bits coming out. AES has 128-bits going into the S-Boxes and 128-bits coming out. As stated previously, AES works on all bits at each layer.
- **DIFFERENCE** S-Box lookup in DES is more complex such that the first + last bit are the row and the middle bits are column. This also results in a 6 bit input translating to a 4 bit output. With AES, the lookup is much simpler in that the two nibbles of the 8-bit byte are used as row and column looks to get an 8-bit (or byte) value.

Diffusion Comparison

- **SIMILAR** Both DES and AES use diffusion to 1) prevent any correlation between plain text bits (input) and cipher text (output) and 2) single bit changes result in >=50% output bit changes.
- **DIFFERENCE** DES uses Expansion E-Box and Permutation P-boxes to achieve diffusion. AES uses, the Diffusion Layer which consist of the ShiftRows Layer and MixColumn Layer.
- **SIMILAR** Both AES and DES use S-boxes for confusion.

References

Primary references for this document are listed below.

- Professor Weissman’s asynchronous class slides: CIS628_Live6_2_2_2_2_2.pptx (DES) and CIS628_Live7and8_2.pptx (AES).
- Professor Weissman’s asynchronous class lectures.
- Course textbook: Understanding Cryptography, Christof Paar and Jan Pelzl.