Cryptography: Reading #1

Due on June 2, 2025 at 10:00pm

Instructor: *Elena Machkasova*

Ellis Weglewski

Prompt 1

Question:
What is the main advantage of a Feistel cipher? Clearly explain, refer to the formula on p.59.

Answer:
A Feistel network (which is the heart of a Feistel cipher) is an elegant way of ecnrypting and decrypting blocks of bits. First, the plaintext block input of 64 bits is permuted and then split in half. The right half is fed through a function that handles confusion and diffusion (properties theoretically required for cryptographic integrity). The output of the confusion/diffusion function is then XOR'd with the left half of the input and their respective positions (left/right) are swapped. This operation is repeated 15 more times and then a final permutation is applied at the end. The entire operation has the unique advantage of a sort of backwards-compatibility where the decryption operation is essentially the same as the encryption operation, just with a reversed key-schedule.

Prompt 2

Question:
What is the purpose of the initial permutation?
Answer:
The exact reasoning for the initial permutation is not known though it is speculated that it was to make data fetches via the 8 bit buses used at the time more efficient.

Prompt 3

Question:
What is the role of the S-Boxes?
Answer:
The S-Box tables are part of the function that procedes the XOR and subsquent left/right swap in the actual Feistel network. The function is supposed to provide confusion and diffusion for cryptographic strength and the S-Boxes provide the confusion component through being non-linear. Preceding the S-Box in the diffusion/confusion function, there is an element called the E-Box which handles the diffusion component. I think that it is hard to properly understand the role of the S-Boxes without also understanding the functionality/role of the E-Box. The E-Box takes an 8 element 32 bit input and maps it to a 8 element 48 bit output by diffusing some of the input bits across multiple elements so that each element has 6 bits instead of 4. This output is then XOR'd with the round key and fed into the S-Boxes. The S-Boxes take this 48 bit output as input and map it back to a 32 bit output by using each element's bit composition as lookup info for the corresponding S-Box table where an 4 bit designation is waiting. The output of the S-Boxes is then permuted and fed into the left/right XOR part of the Feistel network and subsequently swapped with the left half. Essentially, the S-Box(es) are the second part of a larger function that is meant to confuse and mislead an attacker by removing possibility of cryptoanalysis via a linear system of equations because, as mentioned before, they are non-linear.

Prompt 4

Question:
Why is triple DES considered secure?

Problem 4 continued on next page. . .

Answer:
Triple DES (and any 3x applied block cipher for that matter) is cryptographically secure because, in theory, and attacker would have to compute two encryptions or two decryptions in a row in order to break it. In regards to triple DES, this would force an attacker to perform 2^{112} key tests which is infeasible with current hardware/technology. Triple DES also has the nice advantage of being able to work with legacy implementations because if the key is the same for each round, it works like a single DES encryption.

Prompt 5

Question:
Ask at least one question about DES; More are welcome
Answer(s):
Was DES the first known use of S-Boxes in cryptography?