Zak Rowland
CST 466
Assignment 4: Block Cipher and DES

2. In general, in a block cipher, we replace N bits from the plaintext with N bits of ciphertext. What defines an ideal block cipher?

   The relationship between the input blocks and the output block is completely random in an ideal block cipher. Since it must be invertible for decryption, the mapping has to be one-to-one.

3. Whereas it is true that the relationship between the input and the output is completely random for an ideal block cipher, it must nevertheless be invertible for decryption to work. That implies that the mapping between the input blocks and the output blocks must be one-to-one. If we had to express this mapping in the form of a table lookup, what will be the size of the table?

   The size of the table will be N x N, where N is the number of bits in a block.

4. What would be the encryption key for an ideal block cipher?

   The encryption key for an ideal block cipher is $N \times 2^N$, where N is the number of bits in a block.

5. What makes ideal block ciphers impractical?

   Ideal block ciphers are impractical because the keys become exponentially large as block size increases. This creates issues with transmission, storage, and processing of the keys because there is just so much data.

6. What do we mean by a "Feistel Structure for Block Ciphers"?

   A Feistel Structure for block ciphers means the system uses the same basic algorithm for both encryption and decryption. The input block to each round is divided into two halves, left (L) and right (R). In each round, R goes through unchanged, but L goes through an operation that depends on R and the encryption key. This operation carried out on the left half (L) is referred to as the Feistel Function.

Zak Rowland
CST 466
Assignment 4: Block Cipher and DES

7. Are there any constraints on the Feistel function F in a Feistel structure?

   The output of each round during decryption is the input to the corresponding round during encryption, except for the left and right switch between the two halves. This property must hold true regardless of the choice of the Feistel function F.

8. Explain the concepts of diffusion and confusion as used in DES.

   Diffusion means that each plaintext bit must affect as many ciphertext bits as possible. Confusion means that the relationship between the encryption key and the ciphertext must be as complex as possible. For confusion, each bit of the key must affect as many bits as possible in the output ciphertext block.

10. How does the permutation/expansion step in DES enhance diffusion? This is the step in which we expand by permutation and repetition the 32-bit half-block into a 48-bit half-block

    The expansion step in DES enhances diffusion because there are more ciphertext bits than plaintext bits. This means "fake" data is added to the plaintext during encryption, making attacks more difficult and the ciphertext more secure.

11. DES encryption was broken in 1999. Why do you think that happened?

    DES was adopted by NIST in 1977. Computer processing power was increasingly exponentially at the time, so the difference between computers in the early '80s and late '90s is massive. The encryption was broken to prove it was insecure against modern computers, and so that a more advanced encryption standard could take its place; like the one suitably named Advanced Encryption Standard.

12. Since DES was cracked, does that make this an unimportant cipher?

When an encryption method is cracked, it isn't immediately useless for everything. It should no longer be used for storing or transmitting sensitive information like passwords, but it could still be used for things like checking data integrity after transmitting a file. There are also things to learn from cracked encryption standards, and this knowledge can be applied to developing an even better solution.