Tutorial 2: Modern Symmetric Ciphers ~ DES

1. Derive by hand and write down all sixteen DES subkeys for the following keys:
   - The Key: A9 BF 4C 33 9E FB 29 C3
   - Weak Key 1F 1F1F 1F 0E 0E 0E 0E
   - Possibly Weak 1F 1F 01 01 0E 0E 01 01

2. Are weak keys also semi weak? (i.e. do they have the properties necessary for them to classify as semi weak) Are semi-weak keys also "possibly weak"?

3. Given the requirement of finding the key and plaintext of an ordinary DES ciphertext block in 1 week by an exhaustive search, calculate what computational resources would be required?

4. Using the same resources as in question 3, how long would it take to find the key and plaintext for a triple-DES ciphertext block?

5. The DES S-Box lookup tables define two of the six input bits (b_1 and b_6) as the row number and the remaining four as the column number. This row/column arrangement is not really necessary for implementation and each S-box could simply be a list of 64 values (like the permutation tables) which map the 6 input bits. Write down such a table for s-box 1.

6. Write a MATLAB program which implements the DES enciphering and deciphering functions. Perform some time encryption operations and calculate the throughput of your implementation in bytes/second. (For the energetic!)

7. Search the web and find out about
   - Linear Cryptanalysis
   - Differential Cryptanalysis

8. What is a closed cipher? What is a pure cipher? Prove that all closed cipher functions are always pure functions as well.

9. Describe in enough detail for an implementation, how one might demonstrate in an experimental fashion (i.e. not by mathematical proof) that the DES encryption and decryption functions are not closed. The experimental method needs not be practical – assume that there is no restriction on processing power or memory.

10. In a shop you find a secure email package with the following printed in the box:
    "This software contains the very latest and most powerful encryption algorithm available – with 256 bit keys, it would take supercomputers the age of the universe to break your encrypted messages."
    Write a critical review of this product.

11. Look at the diagram of one round of DES. It has a key size of 56 bits and a block size of 64 bits. With reference to the blocks in the figure, explain briefly how DES achieves the goals of confusion and in particular diffusion effectively.

12. Answer the following Questions
    a. Explain and give a mathematical definition of the term “closed cipher”. *[2 marks]*
    b. A cryptographer proposes to improve the security of a cipher by using the cipher twice in succession, with two different keys (double encryption). Explain, with the aid of rudimentary equations, why it is advisable to know whether or not the cipher is closed, and what the implication is for the proposed scheme. *[5 marks]*
    c. Give a clear explanation of the meet-in-the-middle attack. What kind of cryptosystem is it applied to and how it is implemented? Describe a scheme that can be used to circumvent the meet-in-the-middle attack. *[5 marks]*

[June 2001]