E4.44 Network Security : Problem Sheet 1

1. How many DES keys on average encrypt a particular plaintext block to a particular ciphertext block?

2. Why can't the initial permutation in DES have any security value?

3. If the DES mangler function were to transform all 32-bit inputs into the all zero stream regardless of input and stage key what function would DES encryption perform?

4. What value do the 8 parity bits in DES have?

5. A bank which manages 100,000 accounts has correspondent relationships with other banks of comparable size in numbers of accounts managed. For same day value payments messages it allows payments of between £10,000 and £1,000,000 in multiples of £1,000 to be transmitted and appends a 16-bit MAC to each payment message which is created using a key shared with the correspondent bank. If the payment message contains the home account number, the payment figure and the destination account number, how many possible payment messages to a specified correspondent bank will have the same MAC? If the payment clerk is able to run dummy messages through his system to check that a MAC is created, how many messages would he try before he is likely to find two with the same MAC for a specified destination bank?

6. In IDEA addition is performed modulo 2^{16} whilst multiplication is performed modulo $2^{16} + 1$. Given that 16-bit numbers are used in the operations why is multiplication modulo 2^{16} not used in IDEA? When an IDEA key is used in a multiplication what value is zero understood to represent and why?

7. In an IDEA Odd Round, keys K_b and K_c used in addition operations mod 2^{16} are 9EC3 and AFD4 respectively. What values should be used for these keys in the equivalent round for decryption?

8. If keys K_e and K_f are used in an IDEA Even Round what values should these keys take in the equivalent round for decryption?

9. If a brute force attack (i.e. an exhaustive key search) is employed on a 64-bit block encrypted by DES and a second block encrypted by IDEA how much more computing power would be required to break IDEA as against breaking DES?

10. A weak key in DES is its own inverse (two keys are inverses of each other if encryption under one is equivalent to decryption under the other). What pseudo random block stream is generated in an Output Feedback Mode system using a weak key?

11. In a section of ciphertext prepared by the Cipher Block Chaining method it is required to change the tenth 64-bit block of plaintext to yield 8 all zero octets. How should the ciphertext be manipulated to achieve this result? What other effect would the change have?

12. The Cipher Block Chaining method is used to form a MAC for a message stream using the CBC residue. The MAC is appended to the message and is then encrypted using the same key as employed to generate the MAC. Explain how you could obtain at least one plaintext/ciphertext pair of blocks as a result.

13. In ciphertext produced by the 8-bit Cipher Feedback Mode explain how synchronization is restored following the removal or addition of bytes in the ciphertext. What would be the effect of a similar manipulation of ciphertext produced by the Cipher Block Chaining method?