Tutorial 2 Solutions

**School of Digital Media and Infocomm Technology ST2504 Applied Cryptography**

1. DES uses **Feistel** scheme as the basis of the cipher design.

1. Complete the following table

|  |  |  |
| --- | --- | --- |
|  | Data block (bit) | Key size (bit) |
| Lucifer cipher (IBM) | **64** | **128** |
| DES | **64** | **56** |

1. Explain with the aid of a diagram the working principle of Feistel Scheme.

* **The diagram above shows 1 round of Fiestal transformation.**
* **In each Fiestal round, half of the input data block (Li) is XOR-ed with the product of F-function (f) which got its inputs from a round key (Ki + 1) and the other half of the data from the previous round (Ri).**
* **Each half of the input data (Li and Ri) will swap location after each round. Hence Li+1 = Ri and Ri + 1 = XOR Li.**

1. List the key operations performed by the DES round function.

**It expands the round function from 32 bits to 48 bits using Expansion P-box function.**

**Afterwards, XOR with 48-bits subkey K.**

**Passes through 8 S-boxes to get 32-bit result.**

**Finally, permutes using 32-bit [P] function.**

1. Based on question 2, explain why the Round function need NOT be reversible. (Note: a cipher must be able to encrypt and decrypt messages.)

**Since XOR is its own inverse (a XOR b XOR b = a for any a,b) and the half-block that is used as input to the F-function is unchanged in each round.**

**Reversing a Fiestel round is possible by using the same F-function again with the same inputs and XOR the result into the ciphertext to cancel out the previous XOR.**

1. Describe how a DES cipher generates sub-keys (from the secret key)

**The DES cipher will first generate 16 subkeys where it will use Permutation-Choice 1 (PC-1) for initial permutation. Only 56-bits were used as the other 8-bits will be parity bits, hence, the key generally should only have 56-bits and not 64-bits. The resulted 56-bits intermediate subkey is split into 2 x 28-bits halves. It will then do a left-shift, which moves each bit one place to the left, except for the first bit which goes to the end of the block. Afterwards, it will refine the 16 subkeys by left rotating each halves separately. Finally, use PC-2 for permutation and select 48 bits from 56 bits, and we will have our resultant sub-keys.**

\*\*\*The purpose of parity bits is for error checking.\*\*\*

1. Why is DES broken?

**The DES is broken due to the design of the encryption process. The S-boxes used were designed under classified conditions and led people to think that it is a “trapdoor” for National Security Agency (NSA). Furthermore, the 56-bit key that DES uses is too short; thus, it is vulnerable to brute-force search of the whole-key space in our current time. If, it is during the early stages of using this encryption method, it will still be hard to brute force it. However, due to the advancement of internet and technologies, exploiters are able to brute force it within 22 hours, compromising its security.**

ACG/ST2504 1 Apr 2018