**ANT BLOCK CIPHER (Design Document)**

**TEAM MEMBERS: Akshay Utture, Nikhil Maryala, Kshitij Tomar**

The cipher has 20 rounds, and each round is constructed as follows

**Each round is an SPN network and has 3 steps -**

1. Add round key (Randomness layer)
2. Substitution Box (Confusion layer)
3. Permutation layer (Diffusion layer)

**Explanation of each round**

1. Add round key (Randomness layer)

The 32 bit text is simply an ex-or with the 32 bit round key

1. Substitution Box (Variable S-box)

* Normally in a cipher like DES, cryptanalysis is possible because the S-box is known by all and fixed.
* But in this cipher, each variable S-box (labelled with ‘variable S-box’ in the digram above) has a choice of 4 S-boxes and only 1 will be chosen. Which S box will be chosen will be a function of the round key. To give this function good properties, this function itself will be an S-box function

The 4 S-boxes are given below (selected from Serpent S0,S1,S2,S3)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Input (x) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| S0(x) | 3 | 8 | F | 1 | A | 6 | 5 | B | E | D | 4 | 2 | 7 | 0 | 9 | C |
| S1(x) | F | C | 2 | 7 | 9 | 0 | 5 | A | 1 | B | E | 8 | 6 | D | 3 | 4 |
| S2(x) | 8 | 6 | 7 | 9 | 3 | C | A | F | D | 1 | E | 4 | 0 | B | 5 | 2 |
| S3(x) | 0 | F | B | 8 | C | 9 | 6 | 3 | D | 1 | 2 | 4 | A | 7 | 5 | E |

* The Round Key (K) of 32 bit is broken into eight 4-bit parts (K1,K2,...,K8). Each part is passed through an S-box (S5) to get the corresponding output as (B1,B2,...,B8) as given in the diagram below
* In one substitution level, we have to make a choice for the 8 ‘variable S-boxes’ (L1,L2,...,L8)
* The selection is done in the following way. The choice of L1 is decided by the first 2 bits of B1, choice of L2 is decided by the first 2 bits of L2, …… , choice of L8 is decided by the first 2 bits of B8

if the first 2 bits are: 00 - S-box is chosen to be S0(x)

01 - S-box is chosen to be S1(x)

10 - S-box is chosen to be S2(x)

11 - S-box is chosen to be S3(x)

S-Box for Round Key (S5)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Input (x) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| S5(x) | 1 | F | 8 | 3 | C | 0 | B | 6 | 2 | 5 | 4 | A | 9 | E | 7 | D |

1. Permutation Layer

A straight (32 x 32) permutation as in DES is used since it has good diffusion properties. The permutation is given in the table below

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Original Position | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| New Position | 16 | 7 | 20 | 21 | 29 | 12 | 18 | 17 | 1 | 15 | 23 | 26 | 5 | 18 | 31 | 10 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Original Position | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| New Position | 2 | 8 | 24 | 14 | 32 | 27 | 3 | 9 | 19 | 13 | 30 | 6 | 22 | 11 | 4 | 25 |

The reasons for some of the design decisions are given below

* 20 rounds is high enough to make any kind of cryptanalysis more difficult than brute force attack and it is small enough to do the encryption quickly
* The S-box was chosen to be a (4 x 4) because anything smaller than 4 x 4 does not have good non-linearity and is easier for cryptanalysis. Also, we wanted the S-box size to be small so that there are many S-boxes at each round. This increases the amount of uncertainty at each level for the attacker. i.e. 1 level can have 4^8 (8 variable S-boxes and 4 choices for each variable S-box) combination of S-boxes. If the S-box was 8 x 8, three would be 4^4 possible S-box combinations.
* The S-box mappings were taken from the Serpent cipher. These were used since they had good properties of SAC, balancedness and non-linearity.

The diagram for one full round is given below

