**Some Clues about how to proceed with the block cipher assignment**

1. **Decide on the structure of the cipher.**

We have multiple options :

1. SPN (like AES)
2. Feistel (like DES)
3. Generalized Feistel (like CLEFIA)

<http://www.sony.net/Products/cryptography/clefia/?j-short=clefia>

1. Unbalanced Feistel

<https://www.schneier.com/academic/paperfiles/paper-unbalanced-feistel.pdf>

1. Hybrid (Feistel with SP networks – like CLEFIA
2. Hash based cipher

https://en.wikipedia.org/wiki/SHACAL

**2. Decide on the s-box type and size.**

(1) Do you want a compression s-box, straight s-box, or expansion s-box

(2) What is the size of your s-box (m x n mapping, eg. 4X4, 8x8, 16x16, 16x8, etc.)

(3) Do you want 1 s-box mappings in your cipher (like AES) or multiple s-box mapping (like

DES)

**3. Choose the s-boxes. You have multiple options for this.**

(1) Choose n random non-linear functions that are balanced and make them satisfy SAC. Check their non-linearity. Repeat this until you find the right set of functions.

(2) Like AES, create a finite field and use the inverse of an element for the s-box mapping

(4) Look up this paper which lists all possible 4x4 mappings and choose one that has good

features (<https://eprint.iacr.org/2011/218.pdf>)

**4. S-box analysis**

(1) Find the non-linearity, SAC, and balancedness

 (2) Find the DDT and LDT tables for the s-boxes

(3) For Algebraic degree, you need to represent each output bit of the s-box in terms of the input bits. The non-linear equations should have a high degree. If you use first principles to design the s-box, then this should be trivial. If you decide to adopt another s-box, you would need to use a tool like Mathematica, pari, or Sage for this purpose. (This answer is optional. But doing it will definitely boost your marks.)

**5. Key addition**

(1) You don’t need to come up with a key expansion algorithm. You can assume that each round has a round key as input.

(2) Typically, keys will be ex-ored in every round. But you can also try modular additions of the key. For example mod 32, mod 8, etc.

**6. Choose the diffusion layer for the round**

(1) Do you really need one. Depending on your answer to question 1, a diffusion layer may not be

required.

(2) There are multiple options to choose a diffusion layer.   
 Examples are

(a) Some permutations (like DES)

(b) MDS matrix (like AES)

(c) some diffusion operations like circular shifts, integer additions, linear maps, etc.

(3) Find the branch number for the design

**6. Linear and Differential trails**

(1) Compute the linear and differential trail for the cipher. You would need to write a program that

probes every possible trail and finds the trail that has the maximum bias / difference probability.

This answers question 12 in the assignment.

(2) Use this to decide on the number of rounds for your cipher. The number of rounds should be

such that the best differential trail (or linear trail) should have a probability (or bias) lesser than

that of a brute force.

**7. Implementation aspects**

Use smart techniques to implement the cipher efficiently. You could use larger tables for instance. Choose operations for sbox and diffusion layer which are easy to implement: for instance see composite fields of AES

**Points to remember:**

1. **Think differently. The more novel your idea is, the more you score!**
2. **In every design step consider all aspects (ie. Its implication on security. 2. What are its implementation costs).**
3. **As far as possible, discussions and queries about the assignment should be made public (through google groups).**