# APPLIED CRYPTOGRAPHY (CS6530), IIT MADRAS

**Total Time : 1 month** **Course Assignment**
**Max Marks :** 20 **5/3/2018**

## Designing and Implementing a Block Cipher Similar to AES

- There are thirty one different irreducible pentanomials in $GF(2^8)$ including the AES polynomial. These are listed at the end of this document.
- The aim of this course assignment is to design and implement a block cipher with an irreducible polynomial different from AES. The block cipher would encrypt in blocks of 128 bits with a 128 bit key. It would use the same keyschedule as that of AES. The target application for the cipher is for high-speed servers using the counter mode.
- The steps to be followed is as follows. For each step, submit relevant documents or answer relevant questions.

1. Pick a name for your cipher.
2. Add the last two digits of your's and your partner's roll number modulo 30. If this happens to be, say $i$, then pick the $i$-th irreducible polynomial from the list at the end of this document. You would be designing a cipher with this irreducible polynomial.
3. Write functions in C or x86 assembly as efficiently as possible for performing finite field operations in your chosen finite field.
4. Design the SBox using the same technique as that of the AES SBox, i.e. using field inversion. You would need to choose the affine transformation considering the desirable SBox properties (next question).
5. Write programs that would evaluate the following properties of your SBox and compare it with that of the AES SBox.
   - Balancedness property
   - Fixed Points
   - SAC
   - Non-linearity
   - Algebraic degree (optional)
6. Draw the linear approximation table of your SBox.
7. Draw the differential distribution table for your SBox.
8. Design the diffusion layer for your cipher. Find its branch number.
9. Design the cipher to have 10 rounds, similar to that of AES.
10. Show formally and with figures and code, the most deadly linear trail in your cipher.
11. Show formally and with figures and code, the most deadly differential trail in your cipher.
12. Implement your complete cipher as efficiently as possible. Some implementation options for high speed include **(1)** using T-tables (refer OpenSSL implementations as studied in class), **(2)** using bitslicing (refer to this paper: bitslice implementations of AES).
13. Evaluate your cipher with respect to AES to encrypt the file alice.txt.

- **Submission Deadlines**
  - Submission 1: Questions 1 to 7 to be submitted by 20nd March 2018
  - Submission 2: Questions 8 to 11 to be submitted by 10th April 2018
  - Submission 3: Questions 12 and 13 to be submitted by 18th April 2018
- **Submission Guidelines**
  - All submissions must be made by a group of at-most 2 students
  - Marks breakup : Submission 1: 25%; Submission 2: 25%; Submission 3: 30%; Presentation: 20%
  - Deadlines:
    - Only groups that have met all 3 submission deadlines will be able to make a presentation
    - Other groups will only be evaluated by their reports and code. Needless to say, these groups will be evaluated out of 80%.
  - More details about submissions will follow in a later email.

## Irreducible polynomials of degree 8 with binary coefficients

| | |
|---|---|
| 0 | 285 |
| 1 | 375 |
| 2 | 499 |
| 3 | 361 |
| 4 | 445 |
| 5 | 487 |
| 6 | 299 |
| 7 | 471 |
| 8 | 395 |
| 9 | 355 |
| 10 | 319 |
| 11 | 351 |
| 12 | 451 |
| 13 | 313 |
| 14 | 357 |
| 15 | 283 |
| 16 | 301 |
| 17 | 333 |
| 18 | 369 |
| 19 | 391 |
| 20 | 397 |
| 21 | 425 |
| 22 | 463 |
| 23 | 501 |
| 24 | 379 |
| 25 | 415 |
| 26 | 419 |
| 27 | 433 |
| 28 | 477 |
| 29 | 505 |

Notation: For instance 283 represents the AES poly: $256 + 16 + 8 + 2 + 1 = (x^8 + x^4 + x^3 + x + 1)$