** V I T**

**U N I V E R S I T Y**

(Estd. u/s 3 of UGC Act 1956)

Vellore - 632 014, Tamil Nadu, India

School of Information Technology & Engineering

B.Tech – Information Technology

**ITE320 Network and Information Security**

***ASSIGNMENT***

**Last Date for Submission: 14th Oct, 2016.**

***Submission format:***

Name of the student: Reg No:

Name of the Program: Prog No:

1. Algorithms
2. Logic/design elements used in the algorithm
3. Cryptanalysis of Algorithm
   1. Strength of the algorithm
   2. Weakness of the algorithm
   3. Attacks possible
   4. Attacks impossible
   5. Benefits
   6. Drawbacks
   7. Computational power and other resources required
   8. Limitations of the system, Research issues and research gaps identified, features\properties\functionalities missing
4. Applications
5. Suggestions/proposal for Extension/Enhancement/Improvement/Modification of this Cryptosystem
6. Program: C/C++/Java code
7. Sample input and Output
8. References

(Both hard copy and soft copy)

5 minutes presentation of assignment work is on Oct 17th 2016 (includes demonstration of work and Question and Answer)

***Note:***

1. Each Student has to select any one of the following programs.

2. Read the input from key board.

3. Program selected by the student will be allotted to him/her on FCFS basis, if it is not already allotted. Last date for registration of program with faculty is 15th Aug 2016

1. Blowfish Cryptosystem
2. Twofish cryptosystem
3. Threefish cryptosystem
4. IDEA cryptosystem
5. Elliptic Curve Cryptosystem
6. Key Exchange using Elliptic curve cryptography
7. Serpent Cryptosystem
8. CAST-256 Cryptosystem
9. CRYPTON Cryptosystem
10. DEAL Cryptosystem
11. DFC Cryptosystem
12. E2 Cryptosystem
13. FROG Cryptosystem
14. HPC Cryptosystem
15. LOKI97 Cryptosystem
16. MAGENTA Cryptosystem
17. MARS Cryptosystem
18. RC6 Cryptosystem
19. Rijndael (AES) Cryptosystem
20. SAFER+ Cryptosystem
21. Camellia Cryptosystem
22. RC2 Cryptosystem
23. RC4 Cryptosystem
24. RC5 Cryptosystem
25. [SEED](http://en.wikipedia.org/wiki/SEED) Cryptosystem
26. Skipjack Cryptosystem
27. TEA Cryptosystem
28. [XTEA](http://en.wikipedia.org/wiki/XTEA) Cryptosystem
29. [3-Way](http://en.wikipedia.org/wiki/3-Way) Cryptosystem
30. [Akelarre](http://en.wikipedia.org/wiki/Akelarre_%28cipher%29) Cryptosystem
31. [Anubis](http://en.wikipedia.org/wiki/Anubis_%28cipher%29) Cryptosystem
32. [ARIA](http://en.wikipedia.org/wiki/ARIA_%28cipher%29) Cryptosystem
33. [BaseKing](http://en.wikipedia.org/wiki/BaseKing) Cryptosystem
34. [BassOmatic](http://en.wikipedia.org/wiki/BassOmatic) Cryptosystem
35. [BATON](http://en.wikipedia.org/wiki/BATON) Cryptosystem
36. [BEAR and LION](http://en.wikipedia.org/wiki/BEAR_and_LION_ciphers) Cryptosystem
37. [Chiasmus](http://en.wikipedia.org/wiki/Chiasmus_%28cipher%29) Cryptosystem
38. [CIKS-1](http://en.wikipedia.org/wiki/CIKS-1) Cryptosystem
39. [CIPHERUNICORN-A](http://en.wikipedia.org/wiki/CIPHERUNICORN-A) Cryptosystem
40. [CIPHERUNICORN-E](http://en.wikipedia.org/wiki/CIPHERUNICORN-E) Cryptosystem
41. [CLEFIA](http://en.wikipedia.org/wiki/CLEFIA) Cryptosystem
42. [CMEA](http://en.wikipedia.org/wiki/Cellular_Message_Encryption_Algorithm) Cryptosystem
43. [Cobra](http://en.wikipedia.org/wiki/Cobra_ciphers) Cryptosystem
44. [COCONUT98](http://en.wikipedia.org/wiki/COCONUT98) Cryptosystem
45. [Crab](http://en.wikipedia.org/wiki/Crab_%28cipher%29) Cryptosystem
46. [Cryptomeria/C2](http://en.wikipedia.org/wiki/Cryptomeria_cipher) Cryptosystem
47. [CRYPTON](http://en.wikipedia.org/wiki/CRYPTON) Cryptosystem
48. [CS-Cipher](http://en.wikipedia.org/wiki/CS-Cipher) Cryptosystem
49. [DEAL](http://en.wikipedia.org/wiki/DEAL) Cryptosystem
50. DFC Cryptosystem
51. [E2](http://en.wikipedia.org/wiki/E2_%28cipher%29) Cryptosystem
52. [FEAL](http://en.wikipedia.org/wiki/FEAL) Cryptosystem
53. [FEA-M](http://en.wikipedia.org/wiki/FEA-M) Cryptosystem
54. [FROG](http://en.wikipedia.org/wiki/FROG) Cryptosystem
55. [GOST](http://en.wikipedia.org/wiki/GOST_%28block_cipher%29) Cryptosystem
56. [Grand Cru](http://en.wikipedia.org/wiki/Grand_Cru_%28cipher%29) Cryptosystem
57. [Hasty Pudding cipher](http://en.wikipedia.org/wiki/Hasty_Pudding_cipher) Cryptosystem
58. [Hierocrypt](http://en.wikipedia.org/wiki/Hierocrypt) Cryptosystem
59. [ICE](http://en.wikipedia.org/wiki/ICE_%28cipher%29) Cryptosystem
60. [IDEA NXT](http://en.wikipedia.org/wiki/Idea_NXT) Cryptosystem
61. [Iraqi](http://en.wikipedia.org/wiki/Iraqi_block_cipher) Cryptosystem
62. [KASUMI](http://en.wikipedia.org/wiki/KASUMI) Cryptosystem
63. [KeeLoq](http://en.wikipedia.org/wiki/KeeLoq) Cryptosystem
64. [KHAZAD](http://en.wikipedia.org/wiki/KHAZAD) Cryptosystem
65. [Khufu and Khafre](http://en.wikipedia.org/wiki/Khufu_and_Khafre) Cryptosystem
66. [KN-Cipher](http://en.wikipedia.org/wiki/KN-Cipher) Cryptosystem
67. [Ladder-DES](http://en.wikipedia.org/wiki/Ladder-DES) Cryptosystem
68. [Libelle](http://en.wikipedia.org/wiki/Libelle_%28cipher%29) Cryptosystem
69. LOKI ([97](http://en.wikipedia.org/wiki/LOKI97), [89/91](http://en.wikipedia.org/wiki/LOKI)) Cryptosystem
70. [Lucifer](http://en.wikipedia.org/wiki/Lucifer_%28cipher%29) Cryptosystem
71. [M6](http://en.wikipedia.org/wiki/M6_%28cipher%29) & M8 Cryptosystem
72. [MacGuffin](http://en.wikipedia.org/wiki/MacGuffin_%28cipher%29) Cryptosystem
73. [Madryga](http://en.wikipedia.org/wiki/Madryga) Cryptosystem
74. [MAGENTA](http://en.wikipedia.org/wiki/MAGENTA) Cryptosystem
75. [MARS](http://en.wikipedia.org/wiki/MARS_%28cryptography%29) Cryptosystem
76. [Mercy](http://en.wikipedia.org/wiki/Mercy_%28cipher%29) Cryptosystem
77. [MESH](http://en.wikipedia.org/wiki/MESH_%28cipher%29) Cryptosystem
78. [MISTY1](http://en.wikipedia.org/wiki/MISTY1) Cryptosystem
79. [MMB](http://en.wikipedia.org/wiki/MMB) Cryptosystem
80. [MULTI2](http://en.wikipedia.org/wiki/MULTI2) Cryptosystem
81. [MultiSwap](http://en.wikipedia.org/wiki/MultiSwap) Cryptosystem
82. [New Data Seal](http://en.wikipedia.org/wiki/New_Data_Seal) Cryptosystem
83. [Nimbus](http://en.wikipedia.org/wiki/Nimbus_%28cipher%29) Cryptosystem
84. [NOEKEON](http://en.wikipedia.org/wiki/NOEKEON) Cryptosystem
85. [NUSH](http://en.wikipedia.org/wiki/NUSH) Cryptosystem
86. [PRESENT](http://en.wikipedia.org/wiki/PRESENT_%28cipher%29) Cryptosystem
87. [Q](http://en.wikipedia.org/wiki/Q_%28cipher%29) Cryptosystem
88. [REDOC](http://en.wikipedia.org/wiki/REDOC) Cryptosystem
89. [Red Pike](http://en.wikipedia.org/wiki/Red_Pike_%28cipher%29) Cryptosystem
90. [S-1](http://en.wikipedia.org/wiki/S-1_block_cipher) Cryptosystem
91. [SAFER](http://en.wikipedia.org/wiki/SAFER) Cryptosystem
92. [SAVILLE](http://en.wikipedia.org/wiki/SAVILLE) Cryptosystem
93. [SC2000](http://en.wikipedia.org/wiki/SC2000) Cryptosystem
94. [SHACAL](http://en.wikipedia.org/wiki/SHACAL) Cryptosystem
95. [SHARK](http://en.wikipedia.org/wiki/SHARK) Cryptosystem
96. [Simon](http://en.wikipedia.org/wiki/Simon_%28cipher%29) Cryptosystem
97. [SMS4](http://en.wikipedia.org/wiki/SMS4) Cryptosystem
98. [Speck](http://en.wikipedia.org/wiki/Speck_%28cipher%29) Cryptosystem
99. [Spectr-H64](http://en.wikipedia.org/wiki/Spectr-H64) Cryptosystem
100. [Square](http://en.wikipedia.org/wiki/Square_%28cipher%29) Cryptosystem
101. [SXAL/MBAL](http://en.wikipedia.org/wiki/SXAL/MBAL) Cryptosystem
102. [Treyfer](http://en.wikipedia.org/wiki/Treyfer) Cryptosystem
103. [UES](http://en.wikipedia.org/wiki/UES_%28cipher%29) Cryptosystem
104. [Xenon](http://en.wikipedia.org/wiki/Xenon_%28cipher%29) Cryptosystem
105. [xmx](http://en.wikipedia.org/wiki/Xmx) Cryptosystem
106. [XXTEA](http://en.wikipedia.org/wiki/XXTEA) Cryptosystem
107. [Zodiac](http://en.wikipedia.org/wiki/Zodiac_%28cipher%29) Cryptosystem
108. Cramer Shoup Cryptosystem
109. Mc Eliece Cryptosystem
110. ElGamal Cryptosystem
111. Paillier Cryptosystem
112. YAK Key agreement protocol
113. NTRUEncrypt Cryptosystem
114. Merkle Hellman Knapsack Cryptosystem
115. Digital Signature Algorithm
116. Benaloh cryptosystem
117. [Blum–Goldwasser cryptosystem](http://en.wikipedia.org/wiki/Blum%E2%80%93Goldwasser_cryptosystem)
118. [Boneh–Franklin](http://en.wikipedia.org/wiki/Boneh%E2%80%93Franklin_scheme) Cryptosystem
119. Damgard Jurik Cryptosystem
120. Naccache–Stern cryptosystem
121. [Naccache–Stern knapsack cryptosystem](http://en.wikipedia.org/wiki/Naccache%E2%80%93Stern_knapsack_cryptosystem)
122. [Niederreiter cryptosystem](http://en.wikipedia.org/wiki/Niederreiter_cryptosystem)
123. Okamoto–Uchiyama cryptosystem
124. [Sakai–Kasahara scheme](http://en.wikipedia.org/wiki/Sakai%E2%80%93Kasahara_scheme)
125. [Schmidt-Samoa cryptosystem](http://en.wikipedia.org/wiki/Schmidt-Samoa_cryptosystem)
126. [Goldwasser–Micali cryptosystem](http://en.wikipedia.org/wiki/Goldwasser%E2%80%93Micali_cryptosystem)
127. Rabin Cryptosystem
128. GGH Cryptosystem
129. CEILIDH Cryptosystem
130. Massey-Omura cryptosystem