**Index.html :-**

* Explains the concepts of BabyAES and it’s working highlighting all the mathematical principles involved.
* Has a navigation bar which takes you to encryption, decryption and home tabs.

**Encryption.html :-**

* Includes a field in which you can enter a plain-text for encryption and displays the encrypted cipher-text.
* Also explains how the encryption process was done step by step.

**Decryption.html :-**

* Includes a field in which you can enter a cipher-text for decryption and displays the decrypted plain-text.
* Also explains how the decryption process was done step by step.

**References:-**

|  |  |
| --- | --- |
| **[CJB12]** | **Christoforus Juan Benvenuto (2012). *Galois Field in Cryptography.* University of Washington.** |
| [MOV96] | Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography.* CRC Press. |
| [Sta16] | Stallings, W. (2016). *Cryptography and Network Security: Principles and Practice.* Pearson. |
| [NIST99] | National Institute of Standards and Technology. *AES Proposal: Rijndael.* 1999. (Online). <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>. |
| [MIT12] | Massachusetts Institute of Technology. *Introduction to Finite Fields and their Applications.* (Online). <http://people.csail.mit.edu/madhu/ST12/scribe/lect06.pdf> |