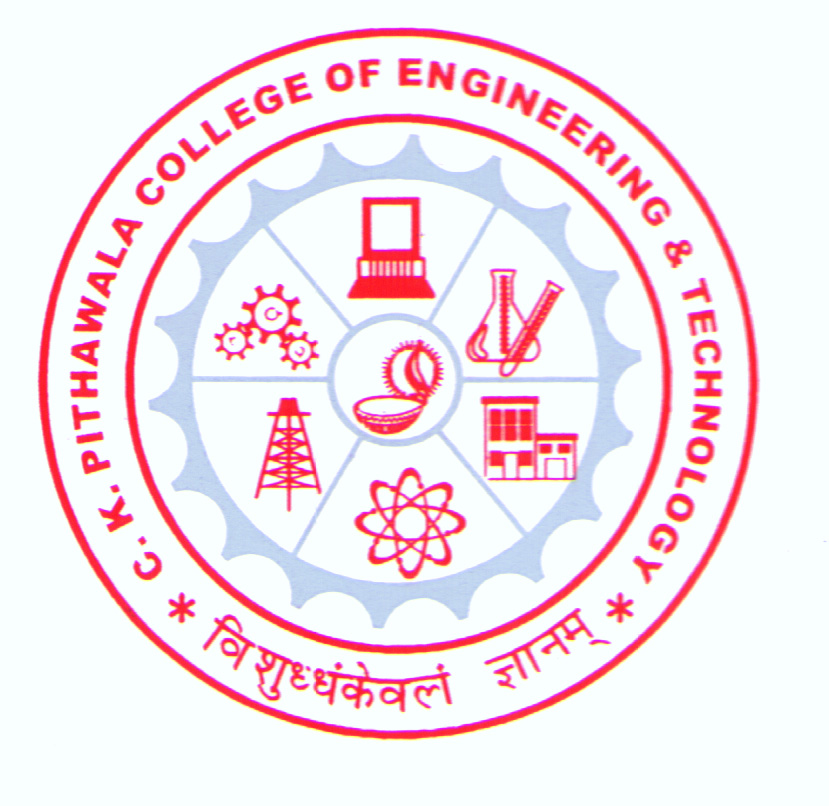
aDVANCED ENCRYPTION STANDARD

The Advanced Encryption Standard is an encryption standard adopted by the U.S. Government.

**Rijndael**



**C.K.PITHAWALLA COLLEGE OF ENGG. & TECHNOLOGY,**

**SURAT – 395 009. (GUJARAT, INDIA)**

**DEPARTMENT OF COMPUTER ENGINEERING**

**A Seminar Report On:**

Advanced Encryption Standard

Prepared By : Jalpan Randeri (8145)

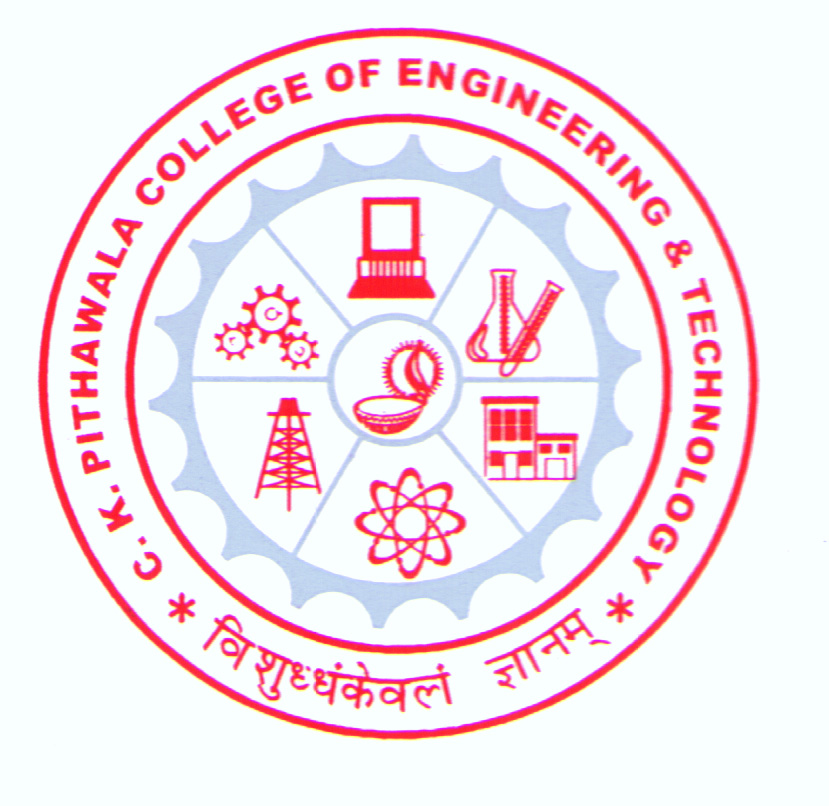
Vivek Champaneria (8102)

Class : B.E. – III(Computer), Semester - V

Year : 2010 – 2011

Guided By : **Prof. Vivaksha Jariwala**

**CERTIFICATE**



This is to certify that **Mr. Jalpan Randeri (Roll No.8145)** & **Vivek Champaneria (Roll No. 8102)** of Third year Computer engineering has successfully delivered the seminar on **“Advanced Encryption Standard”.** The report work prepared by them is found satisfactory.

***Guide Jury Member(s) Head of Department***

----------------------- ------------------------------ ----------------------------

(Prof. Vivaksha Jariwala) (Prof. Ami Chokshi)

**ABSTRACT**

*The Rijndael algorithm is the new advanced encryption standard (AES) approved by the US National Institute of Standards and Technology (NIST). With this algorithm supporting significantly larger key sizes than DES (data encryption standard) supports, NIST believes that the AES has the potential of remaining secure for the next few decades. In overall performance, based on the speed of encryption and decryption and on key set-up time, the Rijndael algorithm has attained top scores in tests conducted by NIST. The belief is that almost all US government agencies will shift to the AES algorithm for their data security needs in the next few years. Also, that the algorithm will find its way in smart cards and other security-oriented applications used for safely storing private information about individuals.*

**Acknowledgement**

I express my sincere thanks to Prof. Vivaksha Jariwala (Computer Engineering Department, C. K. Pithawalla Collage of Engineering and Technology, Surat).For their kind Guidance for presenting the seminar.

I also extend my sincere thanks to all other member of the faculty of Computer Engineer-ing Department and my friends for their encouragement and co-operation.