KG COLLEGE OF ARTS AND SCIENCE

(affiliated to Bharathiar University and Accredited by NAAC)

Research and Development Cell

Faculty Researcher Profile

FACULTY RESEARCHER PROFILE TEMPLATE

Name	Dr.S.Vidhya	Degrees	MCA, M.Phil. Ph.D., NET
Image for home page	https://drive.google.com/file/d/1jqim4jnamUqPwsWGfL0thGRAOOu4fq1f/view?usp=sharing		
Faculty Profile (200 Words Minimum)	received M.Phil. degree from Annamalai University in the year 2007 and got M.Phil. guideship in Bharathiar University in 2009. I have produced 8 M.Phil. scholars. completed Ph.D. in the year 2017 at SCSVMV University, Kancheepuram with the area specialization is Network security. She has been recognized as a Ph.D. guide by Bharathiar University in 2019. Three scholars are pursuing their Ph.D. under her guidance. She published more than 10 publications on UGC, Scopus and Web of Science Journals and presented papers at 3 International and 3 National conferences. She published 2 books “Handbook for M.Phil. Scholar of Computer Science” and “Linux for Beginners”.		
Keywords	Network Security		
RESEARCH PROJECTS / FOCUS AREAS			
Title and description of research projects and Ph.D Research / focus areas (Minimum 100 Words about each projects)	**Title of the Ph.D. thesis:** An efficient and secure format preserving scheme based on advanced encryption standard **Description:** Encryption is an important emerging technology, used to safeguard private data in computers, across private and public networks. Encryption is the method of transforming information in order to secure it from intruders. Encrypting an entire database can be inefficient because it is difficult to selectively access a part of the encrypted data in an encrypted file. It would be desirable to apply cryptographic techniques specifically on the selected fields in the database. Traditional encryption schemes change the database structure and applications related to the database. It requires re-engineering of databases and applications in order to store the modified data size and formats. In order to overcome the drawbacks of the traditional database encryption schemes, a new secure and efficient Format preserving encryption scheme is proposed. In format preserving encryption the length and format of the plaintext is preserved during the encryption process. The structure of the database, applications and the existing queries never change for the encrypted data. The proposed algorithm FPE is based on Encrypt-then-MAC concept		
PUBLICATIONS			

1. **Ph.D. thesis link on Shodhganga** http://shodhganga.inflibnet.ac.in:8080/jspui/handle/10603/183981
2. Format preserving encryption using Feistel cipher.
   http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.891.4939&rep=rep1&type=pdf
3. Efficient FPE Algorithm for Encrypting Credit Card Numbers
   http://www.iosrjournals.org/iosr-jce/papers/Vol14-issue6/D01462329.pdf?id=7545
4. An Efficient Encryption Scheme for Small Arbitrary Length Domains
   http://doi.org/10.22214/ijraset.2018.1397
4. International Review on Computers and Software (I.RE.CO.S.), Vol. 9, N. 5, Securing Data at Rest by Format Preserving Encryption Using PassPhrase, May 2014

   https://drive.google.com/file/d/1afTM6sV-bHKIy_lujO2RgjWl5mNaJXyN/view?usp=sharing

Google Scholar ID	https://scholar.google.com/citations?hl=en&user=Mr-BgfcAAAAJ
Orchid ID	https://orcid.org/0000-0002-1676-5134

FACULTY MEMBER CONTACT SECTION

Email	Vidhya.s@kgcas.com
Office Address	Assistant Professor, Department of Information Technology, KG College of Arts and Science, KGiSL Campus, Saravanampatti, Coimbatore.
Phone No & E-Mail ID.	9092923261 & vidhya.s@kgcas.com