

An Ordeal Random Data Encryption Scheme (ORDES)

Ramveer Singh

Research Scholar Singhania University, Jhunjhunu, Rajasthan
Department of Information Technology, Raj Kumar Goel Institute of Technology,
5th K.M. Stone Delhi – Meerut Road, Ghaziabad, U.P.201003, INDIA
e-mail: ramveersingh_rana@yahoo.co.in

Deo Brat Ojha

Professor, Department of Mathematics, Raj Kumar Goel Institute of Technology,
5th K.M. Stone Delhi – Meerut Road, Ghaziabad, U.P.201003, INDIA
e-mail: ojhdb@yahoo.co.in

Abstract- In this paper, authors presented a new Data encryption scheme named as Ordeal Random Data Encryption Scheme (ORDES). The theoretical security measures are also discussed and ORDES advocates its competency. Through this paper, we encourage the user to use ORDES with more efficiency and security. Mainly we emphasize on secrecy of key because all knows key always play vital role in cryptography. Using a variable random number and a function, the new generated key for each block of message make this approach attractive and more usable. The portability and usability of key changes the state of affairs of DES in every block of structure. This approach ORDES motivates the user to use DES with new destiny of confidence, integrity and authentication.

Keywords- Cryptography, Data Encryption Standard, Encryption, Decryption, Secret key, Hardware Random Number Generator.

Remarks: *The full paper may be found in www.elearningap.com*