



Abhishek Das
Hari Narayan Khan
Atal Chaudhuri

Secret Variant Session Key Based Symmetric Cryptography



LAMBERT
Academic Publishing

Table of Contents

<u>Topics</u>	<u>Page No.</u>
<i>Abstract</i>	<i>1</i>
Chapter 1	2
Overview of Cryptography	2
1.1 Concept of Cryptography	2
1.2 General idea of Cryptography	4
1.3 Various types of Cryptography	5
1.3.1 Symmetric-Key Cryptography.....	5
1.3.2 Asymmetric-Key Cryptography.....	6
1.3.3 Concept of Session Key in Cryptography	7
1.3.4 General Idea of Secret Variant Session Key.....	8
Chapter 2	9
Background and Related Work	9
2.1 Preamble	9
2.2 Hash Function	10
2.3 Data Encryption Standard (DES)	11
2.4 Advanced Encryption Standard (AES)	13
2.4.1 Key Expansion.....	14
2.4.2 Substitute Bytes	16
2.4.3 Shift Row	16
2.4.4 Mix Column.....	17
2.4.5 Add Round Key	18
2.5 Columnar Transposition Cipher	18
Chapter 3	20
Review of different file formats	20
3.1 Format of the Digital Text (.TXT) file	20
3.1.1 Unformatted Text.....	21
3.1.2 Formatted Text.....	22
3.1.3 Hypertext	22
3.2 Format of Digital Image (.BMP) File	23
3.2.1 Pixel Storage.....	25
3.2.2 BMP Header Structure in Programming Concept	26
3.3 Format of the Digital Audio (. WAV) file	27

Chapter 4	Error! Bookmark not defined.
Our Proposed Scheme	30
4.1 Concept	30
4.2 Algorithm for generating Session key ₁	32
4.3 Algorithm for getting 16 bytes feature vector	32
4.4 Algorithm for hiding the invariant	33
4.5 Encryption Phase	33
4.6 Encryption Algorithm.....	34
4.7 Decryption Phase.....	35
4.8 Decryption Algorithm.....	36
Conclusion	37
References	38

A Study on Robust Secret Variant Session Key Based Symmetric Cryptography

By

Hari Narayan Khan¹, Dr. Abhisek Das^{2*}, Dr. Atal Chaudhuri³

¹ Department of Computer Science and Engineering, Regent
Education and Research Foundation, Kolkata, India

² Department of Computer Science and Engineering, Aliah University,
Kolkata, India

³ Department of Computer Science and Engineering, Jadavpur
University, Kolkata, India

*adas@aliah.ac.in