

---

# CONTENTS

<b>APPROVAL</b>	<b>ii</b>
<b>SELF DECLARATION AGAINST PLAGIARISM</b>	<b>iii</b>
<b>ABSTRACT</b>	<b>iv</b>
<b>ABSTRAK</b>	<b>v</b>
<b>DEDICATION</b>	<b>vi</b>
<b>ACKNOWLEDGMENTS</b>	<b>vii</b>
<b>PREFACE</b>	<b>viii</b>
<b>CONTENTS</b>	<b>ix</b>
<b>LIST OF TABLES</b>	<b>xi</b>
<b>LIST OF FIGURES</b>	<b>1</b>
<b>1 THE PROBLEM</b>	<b>2</b>
1.1 Rationale . . . . .	2
1.2 Theoretical Framework . . . . .	3
1.3 Conceptual Framework . . . . .	3
1.4 Statement of the Problem . . . . .	4
1.5 Objective and Hypotheses . . . . .	5
1.6 Assumption . . . . .	5
1.7 Scope and Delimitation . . . . .	6
1.8 Significance of the Study . . . . .	6
<b>2 REVIEW OF STUDIES AND LITERATURE</b>	<b>7</b>
2.1 Related of Studies . . . . .	7
2.1.1 Dynamic Identity Based Authentication . . . . .	7
2.1.2 Attacks on the Authentication System . . . . .	10
2.1.3 Wang's Scheme . . . . .	12
2.1.4 Attack on Wang's Scheme . . . . .	17
2.2 Related Literature . . . . .	21
2.2.1 Discrete Logarithms . . . . .	21
2.2.2 Hash Function . . . . .	22
2.2.3 Hash Collision . . . . .	22

2.2.4	Probability . . . . .	23
2.2.5	Brute Force Attack . . . . .	24
<b>3</b>	<b>RESEARCH METHODOLOGY</b>	<b>25</b>
3.1	Improvement of Wang's scheme . . . . .	25
3.1.1	Basic idea . . . . .	25
3.1.2	The Design of Proposed Scheme . . . . .	25
3.2	Evaluation scenario . . . . .	34
3.3	Instrument & Data Analysis . . . . .	35
3.3.1	Performance of the Scheme . . . . .	35
3.3.2	Probability of Successful Attack . . . . .	35
<b>4</b>	<b>EXECUTION OF THE EVALUATION SCENARIO AND THE ANALYSIS</b>	<b>42</b>
4.1	Data Observation . . . . .	42
4.1.1	Data Observation in Wang's Scheme . . . . .	43
4.1.2	Data Observation in the Proposed Scheme . . . . .	46
4.2	Performance of the Scheme . . . . .	50
4.2.1	Performance of Wang's Scheme . . . . .	51
4.2.2	Performance of the Proposed Scheme . . . . .	51
4.3	Execution of the Attack Scenario . . . . .	53
4.3.1	Offline Password Guessing Attack-1 in Wang's Scheme . . . . .	53
4.3.2	Offline Password Guessing Attack-2 in Wang's Scheme . . . . .	54
4.3.3	Offline Password Guessing Attack-1 in the Proposed Scheme . . . . .	55
4.3.4	Offline Password Guessing Attack-2 in the Proposed Scheme . . . . .	56
4.3.5	User Impersonation Attack in Wang's Scheme. . . . .	57
4.3.6	User Impersonation Attack in the Proposed Scheme . . . . .	59
4.4	Summary Finding . . . . .	63
<b>5</b>	<b>CONCLUSION AND RECOMMENDATIONS</b>	<b>65</b>
5.1	Conclusions . . . . .	65
5.2	Recommendations . . . . .	65
	<b>BIBLIOGRAPHY</b>	<b>66</b>
	<b>Appendices</b>	<b>66</b>
<b>A</b>	<b>The Large Integer Exponentiation in the Modulus</b>	<b>68</b>
<b>B</b>	<b>The Hash Function MD5</b>	<b>70</b>