CONTENTS

APPROVAL ii

SELF DECLARATION AGAINST PLAGIARISM iii

ABSTRACT iv

ABSTRAK v

DEDICATION vi

ACKNOWLEDGMENTS vii

PREFACE viii

CONTENTS ix

LIST OF TABLES xi

LIST OF FIGURES 1

1 THE PROBLEM 2

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

2 REVIEW OF STUDIES AND LITERATURE 7

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

3 RESEARCH METHODOLOGY 25
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

4 EXECUTION OF THE EVALUATION SCHENARIO AND THE ANALYSIS 42
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

5 CONCLUSION AND RECOMMENDATIONS 65
5.1 Conclusions 65
5.2 Recommendations 65

BIBLIOGRAPHY 66

Appendices 66

A The Large Integer Exponentiation in the Modulus 68

B The Hash Function MD5 70