Academic CV

Name : Basim Najim AL-Din Abed AL-Obaidi
Address : Iraq- Diyala-Baquba
Phone – Email : +9647705673798- basim007@yahoo.com

EDUCATION

- Baccalaureate from Iraq/high school in academic year 1992, with graduation rate 80.33
- Bachelor in mathematics science from Iraql/ Al-Mustansiriya University/faculty of science / mathematics department with graduation rate 65.71 in academic year 1996
- Bachelor in computer science from Iraq/Diyala university/faculty of education for pure science / computer science department with graduation rate 90.87 in academic year 2008
- Master in computer science from Jordan/Yarmouk university/faculty of information technology and computer science / computer science department with graduation rate 82.5 in academic year 2015

(DISSERTATION)

Title: MAPPING PRIVATE KEYS INTO ONE PUBLIC KEY USING BINARY MATRICES AND MASONIC CIPHER: APPLYING CAESAR CIPHER AS A USE CASE

Abstract: Organizations worldwide employ various security measures across their boundaries to protect their information infrastructure. Therefore, most of today's organizations adopt at least two levels of security; level-1: data security through encryption, and level-2: network boundary security such as firsewalls…etc. Therefore, encryption takes a vital role in securing organizations daily operations. Therefore, protecting data at level-1 aims to hide the characteristics of the data from being exposed in case it falls in the hands of unauthorized individuals. Therefore, various methods and algorithms are being researched and developed to fill this gap of securing texts and make it difficult to break by unauthorized individuals. One of the very old encryption methods is Caesar cipher method. However, this method did not last long due to its limited key space. Therefore, we believe that strengthen the key mechanism should increase its complexity against the various cryptanalysis attacks. As a result, this thesis proposes two private keys mechanisms tied to the character positions (i.e. odd and even). These two private keys are mapped into one public key to be transferred to the recipient for the decryption process. The one public key generation is a one way function utilizing binary matrices that are generated and shared between the two communicating parties. The one way function is considered Nphard problem that is easy to compute and difficult to inverse. At the end, the results, shows that the new cryptosystem is inevitable to cryptanalysis attack.

Committee chair/members:
Ahmed Manasrah …..……………………… Chairman
Associate Professor of Computer Science, Yarmouk University
Ahmad T. Al-Taani …………………………. Member
Professor of Computer Science, Yarmouk University
Emad E. Abdallah ………………………….. Member
Associate Professor of Computer Science, Hashimiya University

GRANTS AND FELLOWSHIPS (HONORS AND AWARDS)

Scholarship from Hashemite kingdom of Jordan / Yarmouk university / faculty of information technology and computer science in 2013 for studying Master degree in computer science

RESEARCH EXPERIENCE

Data security , cybersecurity , information security and network security

TEACHING EXPERIENCE

Mathematics teacher in high school/iraq from 1997 to 2009 , Assistant teacher in computer science department / faculty of education for pure science / diyala university/ iraq from 2009 to 2013

Lecturer in computer science department / faculty of education for pure science / diyala university/ iraq from 2015 till now , and I I taught the subjects , data security , neural networks , artificial intelligent, programing language , web design , automata theory , data base

(RELEVANT WORK EXPERIENCE)

Teacher , high school/ministry of education , Baquba, Diyala 1997-2009

Description: Mathematics teacher

Assistant teacher , Diyala university/ministry of higher education and scientific research, Baquba, Diyala 2009-2013

Description: assistant teacher in computer lab , manager for the faculty website

Lecturer, Diyala university/ministry of higher education and scientific research, Baquba, Diyala 2015 till now

UNIVERSITY SERVICE

Design and manage the faculty website from 2010 to 2013

Design the data base system for the postgraduate student in faculty

I participated in many local and international conferences

I have published many research papers in local and international scientific journals in partnership with research groups

PUBLICATIONS

1- Anew cryptosystem based on converting many matrices into one large matrix to encrypt text published in Alrafiden university/Iraq conference in 2017

2- A new technique to encrypt the text based on the principle of GCD published in Kalar Private Technical Institute/ Iraq conference in 2017

3- ALDIN, Abed Basim Najim; NOAMAN, Salam Abdulkhaleq; SALMAN, Aseel Dawod. CRYPTOSYSTEM BASED ON THE PRINCIPLES OF INDEFINITE INTEGRAL. Наука и Мир, 2017, 1.3: 8-15. https://elibrary.ru/item.asp?id=28875664

4- New algorithm for encrypt the Arabic text by using distance rule published in Baghdad university/ faculty of science / Iraq conference , 2017

5- ABDULAZEEZ SHABAN, Saad; NAJIM AL-DIN, Basim. A NEW ALGORITHM FOR ENCRYPTING ARABIC TEXT USING THE MATHEMATICAL EQUATION. DIYALA JOURNAL OF ENGINEERING SCIENCES, 2017, 10.1: 21-30. https://dengs.iraqjournals.com/article_125292.html

6- ABDULAZEEZ SHABAN, Saad; NAJIM AL-DIN, Basim. A NEW ALGORITHM FOR ENCRYPTING ARABIC TEXT USING THE MATHEMATICAL EQUATION. DIYALA JOURNAL OF ENGINEERING SCIENCES, 2017, 10.1: 21-30. https://dengs.iraqjournals.com/article_125292.html

7- MANASRAH, Ahmad M.; AL-DIN, Basim Najim. Mapping private keys into one public key using binary matrices and masonic cipher: Caesar cipher as a case study. Security and Communication Networks, 2016, 9.11: 1450-1461. https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1431

8- USING THE PRINCIPLE OF DEFINITE DOUBLE INTEGRAL IN CRYPTOSYSTEM AS A NEW TECHNIQUE FOR THE CRYPTOGRAPHY published in al- mustansiriyah university/ Iraq conference for computer science and mathematics in 2017

9- CIPHER TEXT AS AN RGB COLOR IMAGE published in Science and world. 2018

10- ABED, Basim Najim Al-din; NOAMAN, Salam Abdulkhaleq. McLaurin series as a new technique to improve encryption process. In: Journal of Physics: Conference Series. IOP Publishing, 2019. p. 042008., https://iopscience.iop.org/article/10.1088/1742-6596/1294/4/042008/meta

11- mathematical model for single character cipher text , AUS journal

12- SIMPLE ENCRYPTION ALGORITHM USING MATHEMATICAL COMPLEMENT published in Science and world

13- THE EXTRACTING ACTIONABLE IMPERATIVE SENTENCES FROM THE INTERNET FOR CHATBOT published in Science and world

MANUSCRIPTS IN PROGRESS

A novel Approach to Improve Encryption Process Using Taylor Expansion, Basim Najim Al-din Abed , Sameera A'amer Abdul-Kader & Salam Abdulkhaleq Noaman
Department of computer science/ Faculty of Education for Pure Sciences/
University of Diyala/Iraq (Completed and under review in the scientific journal)
ANOVEL APPROCH BY USING A NEW ALGORITHM: WOLF ALGORITHM AS A NEW TECHNIQUE IN CRYPTOGRAPHY . Basim najim al-din
University of diyala ,diyala, Iraq
Basim007@yahoo.com & Ahmad M. Manasrah , ahmad.a@yu.edu.jo. Yarmouk University, Irbid, Jordan (Completed and under review in the scientific journal)

PRESENTATIONS AND POSTER SESSIONS

Bibliographic format
Bibliographic format

(PATENTS)

Item, date, number

(RESEARCH INTERESTS)

Cybersecurity, Cryptography , Data and information security & network authentication and security

(TEACHING INTERESTS)

Cyber security , Cryptography , data security , neural networks , artificial intelligent