Curriculum Vitae

Full name:Dr. Ali Habeb Kashmar   **Workplace:University of Al-Farabi Collage / Cyber Security Department**

Job title: Assistant Prof.

Major: Mathematics   **Specialty: Cryptography**

Work E-mail: ali.habib@alfarabiuc.edu.iq

Academic Qualifications:

PhD. Mathematics/2016/UKM/Malaysia/ Blostream Hybrid Stream Cipher

MSc. Mathematics/1999/University of Baghdad/Shrinkage Bayesian Estimator for Normal distribution

B.Sc. Mathematics/1993/University of Baghdad

Present Appointment

Assistant Prof.

Previous Appointments

Lecturer

Professional Recognition

Efforts Appreciation Certificate:Number of Certificates from the Ministry of High Education /University of Baghdad/Collage of Science and other Universities inside/outside of Iraq

Other awards or recognition:Number of awards from the Ministry of High Education /University of Baghdad/Collage of Science and other Universities inside/outside of Iraq

Teaching

	Subject	Stage	Theoretical / Practical	Academic Year
1	Statistical Analysis and Probability Advance Cryptography	MSc.	**Theoretical**	-2020-2021 -2021-2022 -2022-2023
2	Statistic and Probability	High Diploma	**Theoretical**	-2020-2021 -2021-2022 -2022-2023
3	Advance Numerical Analysis	2nd Stage	**Theoretical and Practical**	-2020-2021 -2021-2022 -2022-2023
4	Cryptography	3rd Stage	**Theoretical and Practical**	-2020-2021 -2021-2022 -2022-2023

Supervision Graduate Students

No. of PhD students: 2 students

No. of Master's students: 8 students

No. of Higher Diploma students: 4 students

Scientific Research

Scopus:https://www.scopus.com/authid/detail.uri?authorId=565845

ResearchGate:https://www.researchgate.net/profile/Dr-Kashmar

Google Scholar:

https://scholar.google.com/citations?user=1DU83H8AAAAJ&hl=en

Research Interests:

Design and Analysis Cryptography Systems and Cyber Security

Research Projects in the field of specialization to the environment and society or the development of education:

No.	Research Title	Place of Publication	Year
1	FCNN Model for Diagnosis and Analysis of Symmetric Key Cryptosystem	Iraqi Journal for Computer Science and Mathematics, Vol.4, 1(2023), p53-61	2022
2	A predicted for Unscheduling Maintenance System in Aircraft using SVM	4 th International Conference on Accounting, Business, Economics and Politics, Erbil, Iraq	2022
3	An Amendment RSA and A modified SHA3 for A new Design of Blockchain Technology	EAI/Springer Innovations in Communication and Computing	2022
4	Efficient Image Encryption Schemes based on Developing AES Algorithm with Fuzzy Function	3 rd international Conference of Pure, Applied and Technology Sciences	2021
5	An Amendment RSA and A modified SHA3 for A new Design of Blockchain Technology	IOP Journal of Physics (Online ISSN: 1742-6596, Print ISSN: 1742-6588, ICPAS-2021). 2nd International Conference on Physics and Applied Sciences (ICPAS)	2021
6	An Improvement of ECDSA Weak Randomness in Blockchain	ISCAU – 2020 15-16 July 2020 AlAyen University, IOP Conference Series: Materials Science and Engineering. iopscience.iop.org/journal/1757-899X	2020
7	Data Analysis and Classification of Autism Spectrum Disorder Using Principal Component Analysis	Advances in Bioinformatics. Volume 2020, Article ID 3407907	2020
8	A Cryptosystem for Database Security Based on TSFS Algorithm	Baghdad Science Journal Vol.17(2),2020	2020
9	Key Generator to Encryption Images based on Chaotic Maps	Iraqi Journal of Science .Vol. 60, No. 2(2019) 362-370	2019
10	Develop AES algorithm based on	2 nd International Conference for Applied and Pure	2019

		Fuzzy Set Theory	Mathematics, SICAPM 2019,Baghdad, Iraq	
11		Hybrid Chaotic Keystream Generation (Hckg) For Symmetric Image Encryption	Journal of Theoretical and Applied Information Technology (JATIT) 15th February 2019. Vol.97. No 3 PP: 984-993	**2019**
12		Construct Mathematical S -box for Symmetric Key Cryptosystem	Proceeding of 184th The IIER International Conference, Langkawi, Malaysia	**2018**
13		Design a Secure Hybrid Stream Cipher	International Journal of Applied Physics and Mathematics (IJAPM) Volume 5,No.3,PP:153-159 July, 2015	**2015**
14		Pseudorandom Number Generator Using Rabbit Cipher	Applied Mathematical Sciences (AMS) Vol. 9, 2015, no. 88, 4399 - 4412	**2015**
		A Secure Auto-Key Round Combiner Algorithm	International Journal of Applied Engineering Research (IJAER), Vol.10, No.3, 2015	**2015**
15		A-KRCA: a New Combiner Algorithm	The 14th Postgraduate Colloquium. Faculty of Science and Technology. UKM AIP Conference Proceedings 1614, PP:880-885 Kebangsaan Malaysia	**2014**
16		Asymptotic Properties of the Most generalized Optimal Scochastic Approximation Procedures	Journal of Al -Nahrain University Vol.16 (2), July, 2013, pp.202-209	**2013**
17		A stochastic Approximation Iterative Least Squares Estimation Procedure	Iraqi Journal of Science. University of Baghdad, College of Science, Iraq Vol 53.No 2 .2012.PP: 367-385	**2012**
18		Some-time Pool Estimator of Reliability for Exponential Dist.	Iraqi Journal of Science, University of Baghdad, College of Science, Iraq 2011 Volume: 52 Issue: 1 Pages: 70-77	**2011**
19		Statistical system for detection hackers	AL-Mamon University collage 2010	**2010**
20		New High speed stream cipher	Iraqi Association of Information Technology (IAIT)	**2010**

21	Extending "Lebrantih", High Speed Stream Cipher	Proceeding of 3 rd Scientific Conference of the Collage of Science, University of Baghdad, 24-26 March	**2009**
22	Second-stage Estimator of Reliability R(t) for TSPE	University of Mustinseri, College of Education, Journal of Education, No. 5, 2005	**2005**