Mahmut **Kapkiç**

✉ mahmutkapkic@gmail.com | MKBV | mahmut-kapkiç

Objective

A resourceful and self-driven undergraduate student who has been experienced and interested in Cybersecurity for almost six years with strong research experience and leadership. Nowadays, works on Cryptanalysis and Binary Exploitation. Willing to have a solid academic background in Cybersecurity and be an academic researcher.

Education

BSc Computer Science/Engineering
Ankara, Turkey

Atilim University — *Sep 2021 - PRESENT*

- GPA: 3.06/4.00 (With 1 semester High Honor)

Minor in Mathematics
Ankara, Turkey

Atilim University — *Sep 2022 - PRESENT*

- GPA: 3.39/4.00

Skills Summary

Security Skills	Binary Analysis, Reverse Engineering, Cryptology, Network Security, Pentesting, Wireless Security
Programming	Python, C/C++, Bash, x86-64 Assembly, Sage
OS/App Experiences	IDA, Ghidra, GDB, Wireshark, Burp Suite

Experience

Fame Crypt, Cryptosystem Design Analysis Consultancy and Test Co. Ltd.
Ankara, Turkey

Research and Developer Internship — *July 2023 - Oct 2023*

- Developed a block cipher analysis framework, which is used for constructing more secure designs. It contains calculators for DDT, LAT, etc., and a new cryptanalysis technique based on MILP.
- Research on CRYSTALS-Kyber Algorithm, which is a post-quantum cryptographic algorithm.

Interprobe Information Technologies Inc.
Ankara, Turkey

Candidate Engineer at Cryptology Department — *Apr 2023 - Jun 2023*

- Private due to information disclosure statement.

Conference and Journal Publications

Privacy Issues in MR Images
Oral

INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND CRYPTOLOGY (ISCTURKEY 2022) — *Oct. 2022*

- Mahmut Kapkiç, Şeref Sağıroğlu

Notable Projects

Auto Focus Portable Laser Communication System
Ankara, Turkey

Undergraduate Research Project (Participant) — *Dec. 2021 - Jun. 2022*

- Undertook a laser communication project at the Undergraduate Research Project to gain experience applying communication protocols in real-world cases.

Autonomous Ransomware Decryptor
Ankara, Turkey

Head Coordinator — *Nov. 2022 - PRESENT*

- Contributed to this project by utilizing my skills in Project Management, Cryptographic Algorithm Detection, and Binary Analysis.

Prime Number Dataset Generation and Checking Model
Gebze, Turkey

Poster Presentation — *May. 2023*

- Accepted poster presentation by TUBITAK (The Scientific and Technological Research Council of Turkey)

References

Prof. Dr. Şeref Sağıroğlu	Gazi University, Computer Engineering Department, ss@gazi.edu.tr
Assoc. Prof. Dr. Fatih Sulak	Atılım University, Mathematics Department, fatih.sulak@atilim.edu.tr

Professional Development

COMPETITIONS(SELECTED)

Aug 2023	**1st Place**, TurkTelekom Cybersecurity Education and Competition	*Istanbul, Turkey*
Nov 2023	**5th Place**, ICTF 2023	*Online*
Oct 2020	**6th Place**, Battleware CTF	*Turkey*
Aug 2021	**7th Place**, HackIstanbul2021 Bug Bounty Competition	*Istanbul, Turkey*
Aug 2022	**7th Place**, HackKaradeniz2022 Cybersecurity Competition	*Zonguldak, Turkey*
Oct 2022	**9th Place**, STM 2022 CTF	*Istanbul, Turkey*
Sep 2020 - Aug 2021	**District Representative**, 81SiberKahraman long-term Cybersecurity Education and Competition	*Ankara, Turkey*

ATTENDED WORKSHOPS(SELECTED)

Apr 2017	**Hacktrick'17**, Fundamentals of Cyber Security
May 2018	**Hacktrick'18**, Practical Penetration Testing
May 2022	**Hacktrick'22**, Practical IoT Hacking

Undergoing Projects and Researches

Block Cipher Cryptanalysis Framework

- A framework is being developed to examine and analyze block cipher algorithms. It aims to create an analysis report on the tested block cipher algorithm using the existing literature's differential and linear cryptanalysis methods.
- It contains actively used cryptanalysis calculations such as (Shamir Biham, 1991) Differential Distribution Table, (Matsui, 1994) Linear Approximation Table, (Mouha, 2011) Cryptanalysis with MILP, (Sun, 2014) Bit-oriented Cryptanaly, and (Cid, 2018) Boomerang Connectivity Table.

8x8 APN Function Generation with Evolutionary Algorithms and Chaos Theorem

- Block ciphers use substitution functions to randomize their process, but with linear and differential cryptanalysis, it is possible to find the secret key. Using an APN function for substitution function makes that attack impossible to crack.
- And I believe that finding the 8x8 APN function could be possible with evolutionary algorithms and chaos theorem.

IoT Attack Surfaces and Vulnerability Classification Mapping

- IoT devices play a significant role in shaping the current technology landscape. Due to their architecture, they are often susceptible to many vulnerabilities. There should be a report on the problems for further mitigation and awareness.