DRONTECHCONNECT

DRON TECH CONNECT

SIT EDITION

Vol IV Issue I (July -Dec 2023)

DRONTECHCONNECT

EDITORIAL MESSAGE

Dr. Megha Goel

Dear Readers,

Welcome to the latest edition of DronTechConnect!

Our Computer Science and Information Technology (CSIT) Department stands as an exemplary hub of innovation and learning. With cutting-edge curricula and state-of-the-art facilities, we offer an unparalleled academic experience. Our esteemed faculty comprises industry experts and dedicated researchers, fostering an environment that encourages critical thinking, creativity, and problem-solving skills. Through robust industry connections and internships, students gain practical exposure and hands-on experience in diverse technological domains. Our CSIT department prides itself on producing graduates equipped with the expertise and adaptability to thrive in the ever-evolving tech landscape, making a significant impact in the world of technology.

Throughout these pages, you'll discover insightful articles, thought-provoking research, and inspiring stories from our students. From groundbreaking projects to perspectives on emerging technologies, this magazine showcases the diverse talents and accomplishments that make the department truly exceptional.

We hope this edition sparks your curiosity, ignites your passion for technology, and provides a glimpse into the exciting advancements happening within department. Thank you to all the contributors for sharing your expertise and experiences. We invite you to explore, learn, and be inspired by the incredible work showcased in this edition of our CSIT department magazine.

Happy Reading!

Warm Regards
Dr. Megha Goel
Editor-in-Chief, DronTechConnect

EDITORIAL BOARD

Dr. Megha Goel

Editor in Chief

It gives me immense pleasure to present our college magazine, a culmination of creativity, innovation, and academic excellence. Within these pages, you'll witness the remarkable dedication and hard work of our Computer Science and Information Technology (CSIT) department. In this issue, I encourage you to explore the diverse perspectives and accomplishments featured here.

Kunal Desh Pandey

(23271; CSIT)

Co- Editor

Samridhi

(23284; CSIT)

Editor- Design

Nitin Mishra

(23277; CSIT)

Editor- Text

DRONTECHCONNECT

TABLE OF CONTENT

CSIT EDITION

VISION

Preparing technologists with in-depth insights into information technology, and embedding ethics via focused technical training.

MISSION

Empower technologists to excel in information technology through rigorous training and hands -on experience.

Foster a culture of integrity and responsibility by instilling ethical principles in every aspect of technical education.

Encourage technologists with new ideas and good leadership in the tech world, training to possess strong values.

PROGRAM EDUCATIONAL OBJECTIVES (PEO)

- **Demonstrate technical competence with analytical and critical thinking to understand and meet the requirements of Industry, academia and research.**
- **Exhibit leadership, team skills and entrepreneurship skills to provide solutions to real world problems.**
- **Work in multi-disciplinary industries with social and environmental responsibility, work ethics and adaptability to address engineering and social problems.**

PSOS (PROGRAM SPECIFIC OUTCOME)

- **Have proficiency in programming skills to design, develop and apply appropriate techniques, for solving engineering problems.**
- **Have knowledge to build, automate and manage business solutions using advanced technologies.**
- **Have pleasure towards research in applied computer technologies.**

PROGRAMME OUTCOME (PO)

Engineering Graduates will be able to:

PO1. Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO2. Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO3. Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

Po4. Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

Po5. Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

Po6. The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

Po7. Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

Po8. Ethics: Apply ethical principles and commit to professional ethics and responsibilities & norms of the engineering practice.

Po9. Individual & team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

Po10. Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give & receive clear instructions.

Po11. Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to oneâ€™s own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO12. Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Ethical Hacking: Securing Systems Through Responsible Means

Samridhi
(23284; CSIT)

STUDENTS ARTICLES

In an era where cyber threats loom large, ethical hacking emerges as a beacon of hope in the realm of cybersecurity. Ethical hacking, also known as penetration testing or white-hat hacking, involves authorized individuals employing their hacking skills to identify vulnerabilities in computer systems, networks, and applications. Unlike malicious hackers, ethical hackers operate with the consent of the system owner, aiming to strengthen cybersecurity defenses rather than exploit weaknesses.

The primary goal of ethical hacking is to preemptively discover and address security vulnerabilities before they can be exploited by cybercriminals. By adopting the same techniques and tools used by malicious hackers, ethical hackers can uncover weaknesses that might otherwise remain hidden. This proactive approach allows organizations to fortify their defenses, safeguard sensitive data, and mitigate the risk of cyberattacks.

Ethical hacking encompasses various methodologies, including network scanning, vulnerability assessment, penetration testing, and social engineering. These techniques enable ethical hackers to assess the security posture of an organization comprehensively. Through simulated cyberattacks, they can identify weaknesses in firewalls, software configurations, user permissions, and other critical components of IT infrastructure.

Moreover, ethical hacking is not limited to traditional computing systems. With the proliferation of IoT devices, cloud computing, and mobile applications, ethical hackers must adapt to evolving technologies and emerging threats. They play a crucial role in ensuring the security and resilience of modern digital ecosystems.

However, ethical hacking is not without its ethical considerations. It requires a strong moral compass, integrity, and respect for privacy laws. Ethical hackers must adhere to strict codes of conduct, ensuring that their activities do not cause harm or infringe upon individuals' rights. Furthermore, they must obtain explicit authorization from organizations before conducting any penetration testing or security assessments.

In essence, ethical hacking serves as a vital pillar of cybersecurity, empowering organizations to stay one step ahead of cyber threats. By harnessing the skills of ethical hackers, businesses can bolster their defenses, safeguard sensitive information, and uphold the trust of their customers and stakeholders. As the digital landscape continues to evolve, the role of ethical hacking in securing systems remains indispensable.

Samridhi
(23284; CSIT)

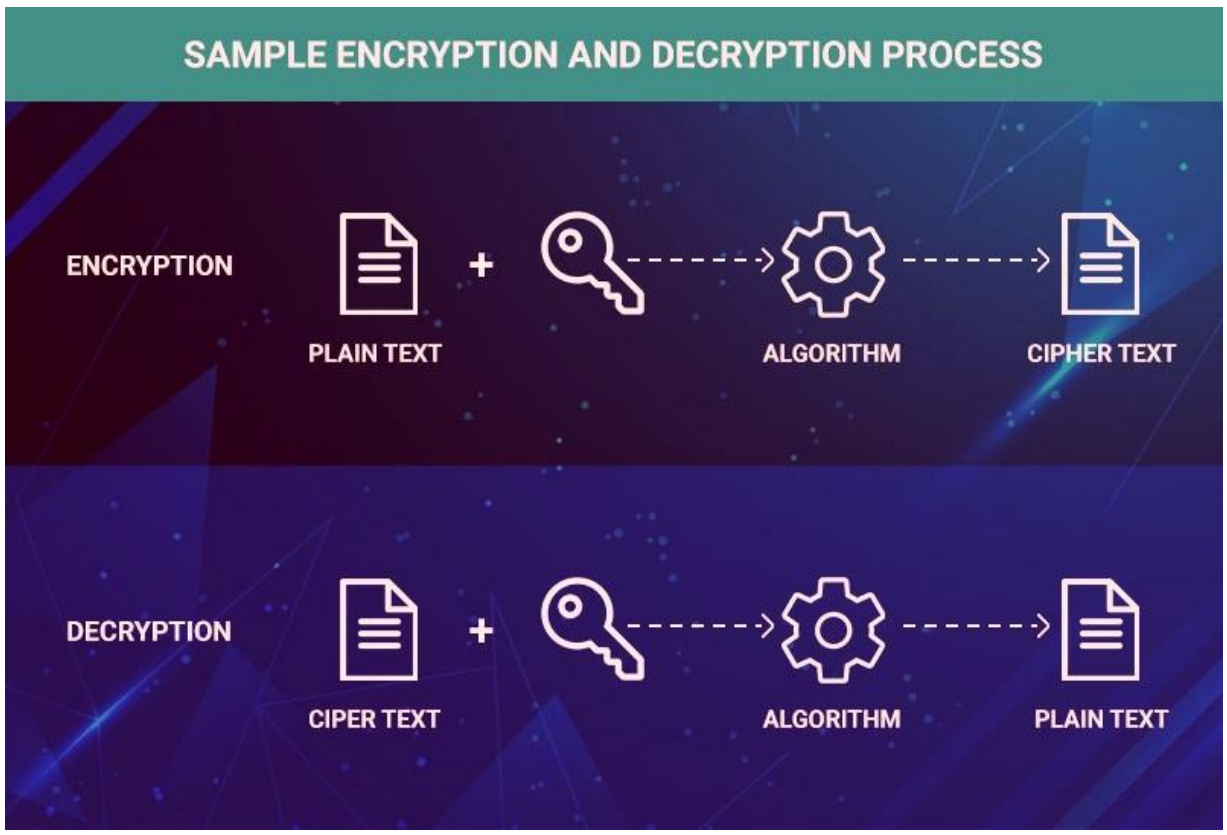
Decryption and Encryption: Safeguarding Data in the Digital Age

STUDENTS ARTICLES

Kunal Desh Pandey
(23271; CSIT)

In the age of digital communication and information exchange, the concepts of encryption and decryption play a pivotal role in ensuring the confidentiality, integrity, and authenticity of data. Encryption is the process of converting plaintext information into ciphertext, rendering it unreadable to anyone without the appropriate decryption key. Decryption, on the other hand, is the reverse process of converting ciphertext back into plaintext, allowing authorized recipients to access the original data.

Encryption serves as a fundamental technique for protecting sensitive information from unauthorized access and interception by malicious actors. Through the use of cryptographic algorithms, encryption scrambles data into an unintelligible format, effectively shielding it from prying eyes during transmission or storage. This process is particularly crucial in safeguarding sensitive financial transactions, personal communications, and proprietary business data from cyber threats such as eavesdropping, data breaches, and identity theft.



Revolutionizing Healthcare: The Design and Development of Wearable Health Monitoring Devices

STUDENTS ARTICLES

Aspect	Encryption	Decryption
Definition	Encryption is the process in which a sender converts the original information to another form and transmits the resulting unintelligible message over the network.	Decryption inverts the encryption process in order to convert the message back to its original form.
Procedure	The data is encrypted/coded automatically with the help of a secret key when data is being transferred between two different machines.	The data receiver lets you to automatically decipher the code in its actual form using the data that was sent.
Location	The sender while sending the data to the destination will convert it.	The receiver while receiving the data would convert it.
Algorithm	The algorithm used is the same for both encryption and decryption process. The keys used depend on the cryptosystem used, symmetric vs asymmetric key.	
Functionality	To transform easily understandable and human decipherable messages into a non – decipherable and obscure form that is almost incomprehensible to interpret	It is the transformation of an obscure message into a decipherable form which is understood by a human.

Various encryption algorithms exist, each with its unique strengths and applications. Commonly used encryption methods include symmetric-key encryption, where the same key is used for both encryption and decryption, and asymmetric-key encryption, which utilizes a pair of public and private keys for encryption and decryption, respectively. Advanced encryption standards (AES), Rivest-Shamir-Adleman (RSA), and elliptic curve cryptography (ECC) are among the widely adopted encryption algorithms in modern computing.

Decryption, on the other hand, enables authorized users to retrieve and interpret encrypted data by applying the appropriate decryption key or algorithm. This process is essential for ensuring data confidentiality while facilitating secure communication and data access within authorized channels.

In conclusion, encryption and decryption are indispensable tools for safeguarding data privacy and security in the digital age. By employing robust encryption techniques and adhering to best practices in cryptographic security, individuals and organizations can mitigate the risk of data breaches, protect sensitive information, and uphold the trust of their stakeholders in an increasingly interconnected world.

Kunal Desh Pandey

(23271; CSIT)

The Hazards of Computer Viruses: Protecting Digital Ecosystems

Mudit Chauhan

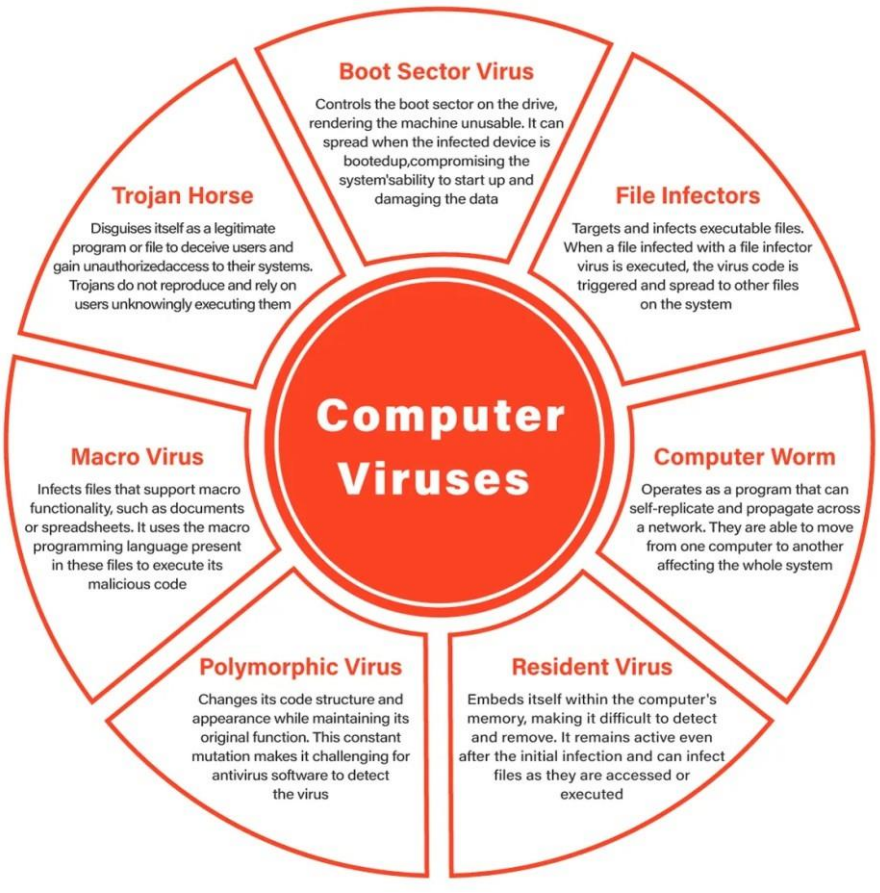
(23273; CSIT)

STUDENTS ARTICLES

Computer viruses, the insidious agents of digital disruption, pose significant hazards to individuals, businesses, & entire digital ecosystems. These malicious programs, designed to replicate & spread across computers & networks, can wreak havoc on data, infrastructure, and user privacy. Understanding the hazards of computer viruses is essential for safeguarding against their damaging effects and preserving the integrity of digital environments.

One of the primary hazards of computer viruses is their ability to corrupt or destroy data. Once unleashed, viruses can infect files, applications, and even system software, leading to data loss, system crashes, and operational disruptions. Whether through the deletion of critical files or the encryption of data for ransom, viruses can inflict substantial financial and operational losses on individuals and organizations.

Moreover, computer viruses pose a significant threat to information security and user privacy. Certain types of viruses, such as keyloggers and spyware, are specifically designed to harvest sensitive information, including login credentials, financial data, and personal communications. By compromising the confidentiality and integrity of data, viruses can facilitate identity theft, financial fraud, and other cybercrimes, jeopardizing the trust and s afety of users.



STUDENTS ARTICLES

Additionally, the rapid proliferation and evolution of computer viruses contribute to their hazardous nature. With new variants and sophisticated attack techniques emerging regularly, traditional antivirus measures may struggle to keep pace with the evolving threat landscape. This dynamic nature makes viruses a persistent and adaptive adversary, requiring continuous vigilance and proactive cybersecurity measures to mitigate their risks effectively.

To combat the hazards of computer viruses, individuals and organizations must adopt a multi-layered approach to cybersecurity. This includes implementing robust antivirus software, regularly updating systems and software patches, practicing safe browsing habits, and educating users about the importance of cybersecurity hygiene. By prioritizing proactive measures and staying informed about emerging threats, stakeholders can fortify their defenses and mitigate the hazards posed by computer viruses in today's digital world.

Mudit Chauhan

(23273; CSIT)