ST. XAVIER'S COLLEGE

MAITIGHAR, KATHMANDU, NEPAL
Phone: 01-5321365, 01-5344636
Email: ktm@sxc.edu.np

LAB ASSIGNMENT NUMBER: 05

"INFORMATION SECURITY AND CYBER LAWS IN NEPAL"

Submitted By	Submitted To	Signature
Name: Shreyashkar Shah Roll No: 1025 Class: 11 Section: J	Mr. Jaya Sundar Shilpakar Department of Computer Science, St. Xavier's College	

Submission Date: 27th January, 2025

INFORMATION TECHNOLOGY

Information Technology (IT) is a modern concept or methodology of communication that combines Information and Communication Technology (ICT). It plays a crucial role in facilitating the flow of information and is widely applied in various fields. IT has brought the world closer together, enabling people to send and receive messages globally within seconds. It is extensively used in sectors like education, industry, banking, research, and healthcare. In education, IT is a valuable tool for teaching and learning, and it has made distant learning possible. In industries, IT helps manage product quantity and quality. It is also instrumental in hospital management and patient treatment. The entertainment sector, including animation, relies heavily on IT, and scientists use it for research and experiments. Space technology has become achievable thanks to IT. Overall, IT has had a significant positive impact on society. However, there are also some negative aspects. As the use of IT grows, so does the rise in cybercrime. Cybercriminals can steal personal data, reveal confidential information, and spread viruses across networks, disrupting social peace and security.
Some of the technologies used are briefly described:

ENCRYPTION

Encryption is a vital security technique used to protect sensitive data from unauthorized access. It involves converting plaintext into an unreadable format using an algorithm and an encryption key. The encrypted data, often called ciphertext, can only be decrypted back into its original form with the correct decryption key. Encryption is widely used in various fields, including online banking, communication, and data storage, ensuring the privacy and integrity of information. There are different types of encryption methods, such as symmetric encryption, where the same key is used for both encryption and decryption, and asymmetric encryption, which uses a pair of keys—a public key for encryption and a private key for decryption. Public Key Infrastructure (PKI) plays a crucial role in managing keys securely. Strong encryption is essential in protecting against cyber threats, such as data breaches and identity theft, making it a cornerstone of modern cybersecurity practices.

DECRYPTION

Decryption is the process of converting encrypted data (ciphertext) back into its original, readable form (plaintext) using a specific decryption key or algorithm. It is the reverse operation of encryption, ensuring that only authorized parties can access the original information. Decryption methods depend on the type of encryption used: in symmetric encryption, the same key is used for both encryption and decryption, while in asymmetric encryption, a private key is required to decrypt data that was encrypted with a corresponding public key. The security of the decryption process is crucial in protecting sensitive information from unauthorized access. Decryption is commonly used in various applications, such as secure communication, online transactions, and data storage, ensuring that information remains confidential and intact throughout its transmission and storage. It is a fundamental component of cybersecurity, preventing data breaches and ensuring privacy.

HASHING

Hashing is a cryptographic process that transforms data, such as a file or password, into a fixed-length string of characters, typically called a hash value or hash code. This transformation uses a mathematical algorithm known as a hash function, which produces a unique output for each unique input. Hashing is a one-way process, meaning that once data is hashed, it cannot be easily reversed or decrypted back to its original form. It is widely used in data integrity verification, where the hash value of the original data is compared with the hash value of the

transmitted or stored data to ensure no changes have occurred. Hashing is also crucial in password storage, as systems store the hash of a password rather than the password itself, adding a layer of security. Common hash functions include MD5, SHA-1, and SHA-256, with each offering different levels of security. Despite its utility, hashing is susceptible to vulnerabilities like collision attacks, where two different inputs produce the same hash value, which is why using secure, modern hashing algorithms is essential in cybersecurity.

DIGITAL SIGNATURE

A digital signature is a cryptographic technique used to verify the authenticity, integrity, and non-repudiation of digital messages or documents. It is created using a signer's private key to encrypt a hash of the message or document, ensuring that the content has not been altered. The recipient can verify the digital signature using the signer's public key, confirming the identity of the sender and the integrity of the data. Digital signatures rely on asymmetric encryption, where the private key is kept secret by the signer, and the corresponding public key is shared openly. They are commonly used in secure communications, legal documents, software distribution, and financial transactions to prevent fraud and ensure that the sender cannot deny sending the message or document (non-repudiation). Digital signatures are often part of a Public Key Infrastructure (PKI), which manages the generation, distribution, and validation of keys. They play a critical role in modern cybersecurity, providing trust and security in digital interactions.

CRYPTOGRAPHY

Cryptography is the practice of securing communication and data through the use of mathematical algorithms to protect information from unauthorized access or tampering. It plays a vital role in maintaining confidentiality, integrity, authentication, and non-repudiation in digital communications.

TYPES OF CRPTOGRAPHY:

1. **Symmetric Cryptography (Secret Key Cryptography):**

- Uses the same key for both encryption and decryption.
- Fast and efficient for large amounts of data.
- The main challenge is secure key distribution because both the sender and receiver must have the same key.
- Common algorithms: AES (Advanced Encryption Standard), DES (Data Encryption Standard), and 3DES (Triple DES).

2. **Asymmetric Cryptography (Public Key Cryptography):**

- Uses a pair of keys: a public key for encryption and a private key for decryption.
- The public key can be shared openly, while the private key is kept secret.
- Solves the key distribution problem and is more secure for communication between parties who have never met before.
- Common algorithms: RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), and DSA (Digital Signature Algorithm).

3. **Hashing:**

- A one-way function that converts data into a fixed-length string, known as a hash value.
- It is irreversible, meaning you cannot recover the original data from the hash.
- Primarily used for data integrity checks, digital signatures, and storing passwords securely.

- Common algorithms: MD5 (Message Digest Algorithm 5), SHA-1 (Secure Hash Algorithm 1), and SHA-256 (part of the SHA-2 family).

FIREWALLS

Firewalls are critical security tools designed to monitor and control incoming and outgoing network traffic based on predefined security rules. They act as barriers between trusted internal networks and potentially harmful external networks, blocking unauthorized access while permitting legitimate communication. Firewalls can be hardware-based, software-based, or cloud-based, and they play a key role in defending against cyberattacks like unauthorized intrusions, malware, and data breaches.

ANTIVIRUS AND ANTI-MALWARE SOFTWARES

Antivirus and anti-malware software are essential for detecting, preventing, and removing malicious programs such as viruses, worms, ransomware, spyware, and trojans. These tools continuously scan files, applications, and websites for known threats and use heuristic analysis to identify emerging risks. Regular updates are crucial to ensure protection against the latest malware variants, helping to maintain the integrity of devices and networks.

BIOMETRIC SECURITY

Biometric security is an advanced authentication technology that uses unique biological traits, such as fingerprints, facial recognition, iris patterns, voiceprints, or even behavioral characteristics, to verify and grant access to systems, devices, or secure facilities. Unlike traditional methods such as passwords or PINs, biometric data is inherently tied to an individual and is nearly impossible to replicate or steal. This makes it a highly reliable and convenient solution for securing sensitive information and environments. Biometric systems are widely adopted in industries like banking, healthcare, and law enforcement, as well as in personal devices like smartphones.

PASSWORD PROTECTION AND MANAGEMENT

Strong password protection involves creating complex, unique passwords and regularly updating them to minimize the risk of unauthorized access. Password management tools simplify this process by securely storing and generating strong passwords. Best practices include using multi-factor authentication (MFA) to add an extra layer of security and avoiding the reuse of passwords across multiple accounts.

DATA BACKUPS

Data backups involve creating copies of critical information and storing them securely, either on physical devices or cloud-based platforms. Regular backups protect against data loss caused by hardware failure, cyberattacks, or accidental deletion. An effective backup strategy includes implementing the 3-2-1 rule: three copies of data, stored on two different media, with one copy stored offsite.

VIRTUAL PRIVATE NETWORKS (VPNs)

Virtual Private Networks (VPNs) establish secure, encrypted connections over the internet, protecting data from interception by hackers or unauthorized entities. VPNs mask the user's IP address and allow safe access to resources remotely. They are widely used for securing public Wi-Fi connections, ensuring privacy, and bypassing geographic restrictions on content.

PUBLIC KEY INFRASTRUCTRE (PKI):

Public Key Infrastructure (PKI) is a framework for securely managing digital certificates and encryption keys. It enables secure communication, authentication, and data integrity through the use of asymmetric cryptography. PKI is fundamental to establishing trust in online transactions, enabling encrypted communications, and authenticating users and devices in secure environments.

RULES AND POLICIES FOR CYBER LAWS IN NEPAL

UNDER THE PROVISION OF PIRATING, DESTROYING OR ALTERING COMPUTER SOURCE CODE:

Any person who, with malafide intention, pirates, destroys, or alters computer source code, which is required to be kept in its current state as per prevailing law, for use in any computer, computer program, computer system, or computer network, or causes others to do so, shall be liable to the following punishment:
Imprisonment: Not exceeding three years
Fine: Not exceeding two hundred thousand Rupees

UNDER THE PROVISION OF UNAUTHORIZED ACCESS IN COMPUTER MATERIALS:

Any person who, with the intention to access any program, information, or data on a computer, uses the computer without the authorization of the owner or the responsible person, or even with authorization, engages in acts contrary to the authorization, shall be liable to the following punishment:
Fine: Not exceeding Two Hundred Thousand Rupees
Imprisonment: Not exceeding three years

UNDER THE PROVISION DAMAGE TO ANY COMPUTER AND INFORMATION SYSTEM:

Any person who, knowingly and with malicious intent to cause wrongful loss or damage to any institution, destroys, damages, deletes, alters, disrupts any information of any computer source, diminishing its value and utility or affecting it injuriously, or causes another person to carry out such an act, shall be liable to the following punishment:
Fine: Not exceeding two thousand Rupees
Imprisonment: Not exceeding three years

UNDER THE PROVISION OF PUBLICATION OF ILLEGAL MATERIALS IN ELECTRONIC FORM:

Any person who publishes or displays material in electronic media, including computer and the internet, which is prohibited by prevailing law or contrary to public morality or decent behavior, or materials spreading hate or jealousy or jeopardizing harmonious relations among various castes, tribes, and communities, shall be liable to the following punishment:
Fine: Not exceeding One Hundred Thousand Rupees
Imprisonment: Not exceeding five years

UNDER THE PROVISION OF CONFIDENTIALITY TO DIVULGE:

Any person who, without lawful authority provided in this Act, Rules, or prevailing law, having

access to records, books, registers, correspondence, information, documents, or any other material under the authority conferred by this Act or Rules, divulges or causes to divulge the confidentiality of such materials to any unauthorized person, shall be liable to the following punishment:
Fine: Not exceeding Ten Thousand Rupees
Imprisonment: Not exceeding two years

UNDER THE PROVISION OF INFORMING FALSE STATEMENT:

Any person who, with the intention of obtaining a license from the Certifying Authority under this Act, or with any other intention towards the Controller or obtaining a Digital Signature Certificate, knowingly conceals or lies about any statement to be submitted to the Certifying Authority, shall be liable to the following punishment:
Fine: Not exceeding One Hundred Thousand Rupees
Imprisonment: Not exceeding two years

CONCLUSION

By the completion of this project work, I get to know about different technologies that are in practice in Nepal. I also came to know about different laws, policies and regulations enforced by the Government of Nepal for which I am thankful to my teachers.