**DEC – 2021**

**1. Explain the following in brief: (4×5=20)**

**(a) The concept and need for cyber security**

**Concept**: Cyber security involves the protection of internet-connected systems, including hardware, software, and data, from cyber attacks. It encompasses a range of practices and technologies designed to safeguard information and ensure the integrity, confidentiality, and availability of data.

**Need**:

* **Protection of Sensitive Data**: Prevents unauthorized access, data breaches, and identity theft.
* **Business Continuity**: Ensures that businesses can operate without disruptions caused by cyber attacks, maintaining productivity and service delivery.
* **Compliance**: Meets legal and regulatory requirements for data protection, avoiding fines and legal consequences.
* **Trust and Reputation**: Maintains customer trust and protects the reputation of organizations by ensuring data security and privacy.
* **Economic Impact**: Reduces financial losses associated with cyber crimes, including fraud, theft, and operational downtime.

**(b) Types of conventional ciphers**

**Substitution Ciphers**: Replace each letter in the plaintext with another letter according to a fixed system.

* **Caesar Cipher**: Shifts each letter by a fixed number of positions in the alphabet. For example, with a shift of 3, A becomes D, B becomes E, etc.
* **Monoalphabetic Cipher**: Uses a single substitution alphabet to replace each letter in the plaintext with a corresponding letter in the ciphertext.
* **Polyalphabetic Cipher**: Uses multiple substitution alphabets to encrypt the plaintext. The Vigenère cipher is a well-known example, where a keyword determines the substitution pattern.

**Transposition Ciphers**: Rearrange the positions of the characters in the plaintext to form the ciphertext.

* **Rail Fence Cipher**: Writes the message in a zigzag pattern across multiple rows (rails) and then reads it off row by row to create the ciphertext.
* **Columnar Transposition Cipher**: Writes the message in rows of a fixed length and then reads it off column by column after rearranging the columns according to a key.

**(c) Filtering devices and rating systems**

**Filtering Devices**: Tools used to control access to content on the internet by blocking or allowing specific websites or types of content.

* **Firewalls**: Monitor and control incoming and outgoing network traffic based on predetermined security rules. They can block unauthorized access and protect against cyber threats.
* **Content Filters**: Block access to inappropriate or harmful websites based on content categories, keywords, or URLs. Commonly used in schools, workplaces, and homes to protect users from harmful content.

**Rating Systems**: Systems that classify content based on its suitability for different audiences, helping users make informed decisions about what to access.

* **PICS (Platform for Internet Content Selection)**: Allows content providers to label their content with metadata that describes its nature, enabling filtering software to block or allow access based on user preferences.
* **ICRA (Internet Content Rating Association)**: Provides a rating system for web content, allowing users to filter out content that is inappropriate for certain age groups or preferences.

**(d) Difference between cyber crimes and traditional crimes**

**Cyber Crimes**:

* **Nature**: Committed using computers, networks, and the internet. They often involve unauthorized access, data breaches, and digital fraud.
* **Scope**: Can have a global reach, affecting victims across different countries and jurisdictions.
* **Examples**: Hacking, phishing, identity theft, cyberstalking, ransomware attacks, and online fraud.

**Traditional Crimes**:

* **Nature**: Physical crimes committed in the real world, often involving direct interaction between the perpetrator and the victim.
* **Scope**: Usually localized to a specific area or community, with limited cross-border implications.
* **Examples**: Theft, assault, vandalism, burglary, and physical fraud.

**2. Discuss the core elements of data security. (10 marks)**

**Core Elements**:

* **Confidentiality**: Ensures that sensitive information is accessible only to authorized individuals and entities. Methods to maintain confidentiality include:
  + **Encryption**: Converts data into a coded format that can only be read by someone with the decryption key.
  + **Access Controls**: Restrict access to data based on user roles and permissions.
  + **Authentication**: Verifies the identity of users before granting access to data.
* **Integrity**: Ensures that data remains accurate, complete, and unaltered during storage, transmission, and processing. Methods to ensure integrity include:
  + **Checksums and Hash Functions**: Generate unique values based on the data content, allowing verification of data integrity.
  + **Digital Signatures**: Provide a way to verify the authenticity and integrity of digital messages or documents.
  + **Version Control**: Tracks changes to data and allows rollback to previous versions if unauthorized modifications are detected.
* **Availability**: Ensures that data is accessible to authorized users when needed. Methods to ensure availability include:
  + **Redundancy**: Implements multiple copies of data and systems to prevent single points of failure.
  + **Backups**: Regularly copies data to secure locations to enable recovery in case of data loss or corruption.
  + **Disaster Recovery Plans**: Establishes procedures to restore data and systems after a disruption, such as a cyber attack or natural disaster.

**3. Critically examine the copyright issues in digital medium. (10 marks)**

**Copyright Issues**:

* **Digital Reproduction**: The ease of copying and distributing digital content leads to widespread unauthorized reproduction, impacting creators' revenue and intellectual property rights.
* **Piracy**: Illegal downloading and sharing of copyrighted material, such as music, movies, software, and e-books, is rampant in the digital medium. This undermines the market for legitimate sales and distribution.
* **Digital Rights Management (DRM)**: Technologies used to control the use of digital content, such as preventing copying or restricting access. While DRM aims to protect copyright, it is often criticized for limiting legitimate use and creating inconvenience for consumers.
* **Fair Use**: The challenge of defining and enforcing fair use in the digital age, where content can be easily modified, shared, and repurposed. Fair use allows limited use of copyrighted material without permission for purposes such as criticism, comment, news reporting, teaching, scholarship, or research.
* **International Enforcement**: Difficulty in enforcing copyright laws across different jurisdictions with varying legal frameworks. The global nature of the internet complicates efforts to protect intellectual property rights and prosecute offenders.
* **User-Generated Content**: Platforms that host user-generated content, such as social media and video-sharing sites, face challenges in monitoring and managing copyright infringement. The DMCA provides a "safe harbor" for these platforms if they promptly remove infringing content upon notification.

**4. Discuss the law in United States for regulation of cyberspace. (10 marks)**

**US Cyber Laws**:

* **Computer Fraud and Abuse Act (CFAA)**: Prohibits unauthorized access to computers and networks, criminalizing activities such as hacking, spreading malware, and committing fraud using computers. The CFAA is a key statute for prosecuting cyber crimes.
* **Digital Millennium Copyright Act (DMCA)**: Addresses copyright infringement in the digital environment. It includes provisions for DRM, safe harbor for internet service providers (ISPs), and procedures for removing infringing content. The DMCA aims to balance the rights of copyright holders with the interests of technology companies and users.
* **Electronic Communications Privacy Act (ECPA)**: Protects the privacy of electronic communications, including email, phone calls, and data stored electronically. The ECPA regulates government access to electronic communications and sets standards for wiretapping and surveillance.
* **Children's Online Privacy Protection Act (COPPA)**: Regulates the collection of personal information from children under 13. COPPA requires websites and online services to obtain parental consent before collecting, using, or disclosing personal information from children.
* **Cybersecurity Information Sharing Act (CISA)**: Facilitates the sharing of cyber threat information between the government and private sector. CISA aims to improve the nation's cyber defenses by encouraging collaboration and information exchange to detect and respond to cyber threats.

**5. What is meant by Cryptography? Discuss RSA algorithm. (10 marks)**

**Cryptography**: Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries. It involves transforming readable data (plaintext) into an unreadable format (ciphertext) to protect it from unauthorized access. Cryptography ensures the confidentiality, integrity, and authenticity of information.

**RSA Algorithm**: The RSA algorithm is a widely used public key cryptographic system that enables secure data transmission. It is named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman.

**Key Concepts:**

* **Public Key Cryptography**: RSA 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.
* **Asymmetric Encryption**: Unlike symmetric encryption, which uses the same key for both encryption and decryption, RSA uses different keys for these processes.

**Key Generation:**

1. **Select Two Large Prime Numbers**: Choose two distinct large prime numbers, ( p ) and ( q ).
2. **Compute ( n )**: Calculate ( n ) by multiplying ( p ) and ( q ) (( n = p \times q )). The value of ( n ) is used as the modulus for both the public and private keys.
3. **Calculate the Totient**: Compute the totient function ( \phi(n) ), where ( \phi(n) = (p-1) \times (q-1) ).
4. **Choose Public Key ( e )**: Select an integer ( e ) such that ( 1 < e < \phi(n) ) and ( e ) is coprime with ( \phi(n) ). The pair ( (e, n) ) forms the public key.
5. **Determine Private Key ( d )**: Calculate ( d ) such that ( d \times e \equiv 1 \ (\text{mod} \ \phi(n)) ). The pair ( (d, n) ) forms the private key.

**Encryption:**

To encrypt a message ( M ):

1. Convert the plaintext message ( M ) into an integer ( m ) such that ( 0 \leq m < n ).
2. Compute the ciphertext ( c ) using the public key ( (e, n) ): [ c = m^e \mod n ]

**Decryption:**

To decrypt the ciphertext ( c ):

1. Compute the original message ( m ) using the private key ( (d, n) ): [ m = c^d \mod n ]
2. Convert the integer ( m ) back to the plaintext message ( M ).

**Security:**

The security of the RSA algorithm is based on the computational difficulty of factoring large composite numbers. While it is easy to multiply two large primes to get ( n ), it is extremely difficult to factor ( n ) back into ( p ) and ( q ), especially when ( n ) is large (e.g., 2048 bits).

**Applications:**

* **Secure Communication**: RSA is used to encrypt sensitive data transmitted over the internet.
* **Digital Signatures**: RSA can be used to sign digital documents, ensuring their authenticity and integrity.
* **Key Exchange**: RSA facilitates the secure exchange of symmetric keys used in other encryption algorithms.

By understanding and applying the RSA algorithm, secure and confidential communication can be achieved, protecting data from unauthorized access and ensuring its integrity.