Here are **2 marks, 5 marks, and 10 marks questions** on **Cyber Security** topics:

Basics of Cyber Security & Cyber Space

2 Marks

1. **What is Cyber Security?**
   Protecting systems, networks, and data from cyber threats.
2. **What is Cyber Space?**
   The virtual environment where online activities occur, including internet, social media, and cloud services.

5 Marks

1. **Cyber Security Goals**:
   Protect confidentiality, integrity, and availability (CIA) of data. Ensure privacy and prevent unauthorized access.
2. **Cyber Space Risks**:
   Include threats like hacking, data breaches, and malware. Security measures involve firewalls, encryption, and access controls.

10 Marks

1. **Cyber Security Framework**:
   - **Identify**: Understanding risks and assets.
   - **Protect**: Implement controls and safeguards.
   - **Detect**: Monitor for potential threats.
   - **Respond**: Take action during incidents.
   - **Recover**: Ensure business continuity after an attack.

E-commerce Related Topics

2 Marks

1. **What is E-commerce?**
   Buying and selling of goods/services over the internet.
2. **E-commerce Security**:
   Measures like secure payment gateways, SSL certificates, and encryption protect online transactions.

5 Marks

1. **Types of E-commerce**:
   - **B2C**: Business to Consumer.

- **B2B**: Business to Business.
- **C2C**: Consumer to Consumer.

2. **E-commerce Payment Security**:
Secure protocols like HTTPS, encryption, and multi-factor authentication (MFA) to protect transactions.

10 Marks

1. **E-commerce Security Threats and Countermeasures**:
   - Threats: Phishing, fraud, data breaches.
   - Countermeasures: Secure payment gateways, regular audits, encryption, and fraud detection systems.

Cyber Threats & Cyber Laws

2 Marks

1. **What is a Cyber Threat?**
A potential danger that could exploit vulnerabilities in a system.
2. **Cyber Law**:
Laws governing online activities, such as data privacy, intellectual property, and cybercrime.

5 Marks

1. **Types of Cyber Threats**:
   - **Malware**: Harmful software (e.g., viruses, worms).
   - **Phishing**: Deceptive emails or websites to steal information.
   - **DDoS**: Distributed Denial of Service attack.
2. **Cyber Laws**:
   - **IT Act, 2000**: Indian law governing online activities.
   - **GDPR**: European regulation on data protection and privacy.

10 Marks

1. **Cyber Laws and Regulations**:
   - **IT Act**: Governs cybercrime, digital signatures, and e-commerce.
   - **Cybercrime Categories**: Data theft, identity theft, phishing.
   - **International Laws**: Include GDPR, US Cybersecurity Act.
2. **Challenges in Cyber Law Enforcement**:
Cross-border jurisdiction, anonymity, and rapid technological changes pose challenges in enforcement.

Cryptography Basics, Attacks, Plain Text, Cipher Text Algorithms

2 Marks

1. **What is Cryptography?**
   The practice of securing communication through encoding messages.
2. **Plaintext vs Ciphertext**:
   - **Plaintext**: Readable data.
   - **Ciphertext**: Encrypted data.

5 Marks

1. **Types of Cryptography**:
   - **Symmetric**: Same key for encryption and decryption (e.g., AES).
   - **Asymmetric**: Different keys for encryption and decryption (e.g., RSA).
2. **Cryptographic Attacks**:
   - **Brute Force**: Trying all possible keys.
   - **Man-in-the-Middle**: Intercepting communication between two parties.

10 Marks

1. **Cryptographic Algorithms**:
   - **AES**: Advanced Encryption Standard (symmetric, widely used).
   - **RSA**: Asymmetric encryption based on large prime numbers.
   - **SHA-256**: Hashing algorithm for data integrity.
2. **Cryptographic Attacks**:
   - **Known Plaintext Attack**: Using known plaintext-ciphertext pairs to crack encryption.
   - **Chosen Ciphertext Attack**: Decrypting ciphertext to retrieve plaintext.
   - **Side-Channel Attacks**: Extracting information from the system by observing its physical operation (e.g., power consumption).

Let me know if you'd like to dive deeper into any of these topics or need more elaborated answers!