Here’s your sentence-by-sentence professional study note breakdown — fully comprehensive and formatted for easy pasting into Word without excessive spacing.

**Encrypted Browsing – Detailed Study Notes**

1. **Lesson Objective**
   * Topic: How to ensure secure, encrypted communication between a client (workstation) and a remote server over the internet.
2. **Importance of Secure Browsing**
   * Before entering personal or sensitive details on a website, verify the connection is secure.
   * Example: When purchasing an exam voucher from diontraining.com, ensure the transaction page is encrypted.
3. **Checking Website Security**
   * Look for the lock icon in the front of the browser’s address bar before entering any information.
   * Clicking the lock displays security details of the connection.
4. **Certificate Information**
   * Clicking on the Certificate shows:
     + Domain name (e.g., cart.diontraining.com).
     + Common name, organizational name, and unit.
     + Issuer (e.g., Let’s Encrypt, a trusted Certificate Authority).
     + Issue and expiration dates.
     + Fingerprints (SHA-256, SHA-1).
   * Certificate hierarchy example:
     + Site certificate signed by R3 → signed by ISRG Root X1.
5. **Technical Certificate Details**
   * Can view algorithms, serial numbers, versions, and chain of trust.
   * Purpose: Validate that the website is authentic and the connection is encrypted.
6. **Function of Digital Certificates**
   * Provides a secure tunnel between browser and website.
   * Valid certificate + HTTPS ensures data confidentiality and integrity.
7. **Invalid Certificate Example**
   * Site: expired.badssl.com.
   * Browser warning: “Connection is not private” (Google Chrome).
   * Cause: Certificate date invalid — issued in 2015 and expired in 2015.
8. **Risks of Expired Certificates**
   * Even if a site has a certificate, if it’s expired, the connection is not considered secure.
   * HTTPS requires a valid, unexpired certificate.
9. **Bypassing Security Warnings**
   * Possible via “Advanced” → “Proceed to…” but strongly discouraged.
   * Demonstrated for educational purposes only.
10. **Exploring badssl.com**
    * Resource for viewing intentional SSL/TLS issues:
      + Expired certificates.
      + Revoked certificates.
      + Weak cryptographic keys (e.g., Diffie-Hellman 480-bit, insecure by modern standards).
11. **Weak Key Example**
    * Diffie-Hellman 480-bit key is vulnerable to compromise.
    * Represents a “bad” SSL/TLS configuration.
12. **Key Takeaway**
    * Always verify the presence of a lock icon in the browser’s address bar.
    * This confirms a valid, secure connection between browser and remote website.