Worksheet 4: Error Detection & Encryption Solutions

Section A: Multiple Choice Questions

1. **b) To detect errors in transmitted data**
   The parity bit is used for error detection in data transmission.
2. **c) Parity block**
   Parity blocks can identify the exact corrupted bit by using row and column parity checks.
3. **a) 0**
   The byte has four 1s (even number), so the even parity bit is 0 to keep the total number of 1s even.
4. **b) Requires secure key distribution**
   Symmetric encryption uses the same key for encryption and decryption, which must be securely shared.
5. **b) Private key**
   In asymmetric encryption, the private key decrypts messages encrypted with the public key.
6. **c) ARQ**
   Automatic Repeat Request (ARQ) resends data if an error is detected.
7. **b) 1**
   Sum = 14 + 22 + 9 = 45. Remainder of 45 ÷ 5 is 0, but wait: 45 ÷ 5 = 9 exactly, so remainder is 0. (Correction: The correct answer is 0, option a).
8. **b) It doubles bandwidth usage**
   Echo check requires sending data back to the sender for verification, using twice the bandwidth.
9. **d) All are detectable**
   Check digits can detect single-digit errors, transposition errors, and some multiple errors.
10. **b) To make data unreadable to unauthorized users**
    Encryption's primary purpose is to ensure data confidentiality.

Section B: Short Answer Questions

6. Two causes of errors during data transmission:

- **Electrical interference/noise** (e.g., from power lines or other devices).
- **Signal attenuation** (weakening over long distances, leading to data corruption).

7. Even parity bit for the byte 1 0 1 1 0 0 1 **_:**

- Count the 1s: 1 (first) + 0 + 1 + 1 + 0 + 0 + 1 = 4 (even).
- Parity bit must be 0 to keep the total number of 1s even.

8. How parity blocks localize errors:

- A parity block organizes data into rows and columns, with parity bits for each row and column.
- If an error occurs, the row and column parity checks will intersect at the corrupted bit, pinpointing its exact location.

9. Checksum calculation for 12, 25, 8, 19 **(remainder ÷ 7):**

- Sum = 12 + 25 + 8 + 19 = 64.
- 64 ÷ 7 = 9 with remainder **1**.
- Checksum = **1**.

10. Symmetric vs. asymmetric encryption (two differences):

1. **Keys**: Symmetric uses one shared key; asymmetric uses public/private key pairs.
2. **Speed**: Symmetric is faster; asymmetric is slower due to complex calculations.

11. Private key is never shared in asymmetric encryption:

- The private key decrypts messages and must remain secret to ensure only the intended recipient can read them.

12. Real-world use of check digits:

- **ISBNs** (International Standard Book Numbers) use check digits to validate book codes.

Section C: Structured Questions

13. Echo Check Process:

- **(a) Diagram**:

text

Sender → Data → Receiver → Echoed Data → Sender (verifies)

- **(b) Disadvantage**: Doubles bandwidth usage, inefficient for large data.

14. Automatic Repeat Request (ARQ):

- **(a) ACK and NAK roles**:
    - **ACK** (Acknowledgment): Confirms error-free receipt.
    - **NAK** (Negative Acknowledgment): Requests retransmission if errors are detected.
- **(b) Unsuitability for real-time streaming**: ARQ causes delays due to retransmissions, disrupting real-time playback.

15. ISBN-13 Check Digit Calculation

Given: 978-1-56619-909 (first 12 digits)

1. **Remove hyphens:** 9 7 8 1 5 6 6 1 9 9 0 9
2. **Sum odd positions (×1) + even positions (×3):**
    - Odd (1,3,5,7,9,11): 9 + 8 + 5 + 6 + 9 + 0 = 37
    - Even (2,4,6,8,10,12): (7 + 1 + 6 + 1 + 9 + 9) × 3 = 33 × 3 = 99
3. **Total sum:** 37 + 99 = 136
4. **Remainder when divided by 10:** 136 ÷ 10 = 13 R6
5. **Check digit:** 10 - 6 = 4

Result: Check digit = **4** → Full ISBN: 978-1-56619-909-4