

5 Cryptography and detecting data attacks – Part 2

Name: _____ Class: _____ Date: _____

Vocabulary

Write each word three times.

English	Write it 3 times (English)		
plaintext	_____	_____	_____
key	_____	_____	_____
ciphertext	_____	_____	_____
Symmetric encryption	_____	_____	_____
AES	_____	_____	_____
key pair	_____	_____	_____
public key	_____	_____	_____
private key	_____	_____	_____
honeypot	_____	_____	_____
hash	_____	_____	_____

Recall

- You know a secret code turns a message into something unreadable.
- You have seen the padlock icon (HTTPS) in a browser.
- You understand that checking a file's fingerprint can show if it changed.

New ideas

Read these first. Each idea has a short worked example. Then do the Practice below.

■ 1 Symmetric encryption

Encryption combines **plaintext** with a **key** to make **ciphertext**. **Symmetric encryption** (like **AES**) uses the same key both ways; the challenge is sharing that key safely.

Worked example. A 4-bit key has $2^4 = 16$ possible values - a real key is far longer.

■ 2 Asymmetric encryption

A **key pair** has a **public key** (shared) and a **private key** (secret). To send Bob a secret, encrypt with Bob's public key; only his private key decrypts it.

Worked example. This solves symmetric's problem - no secret key had to be shared first.

■ 3 Detecting data attacks

A **honeypot** is a fake valuable file - any access is an alarm. A **hash** check re-hashes a file to see if it changed. Logs reveal attacks: `OR 1=1` = SQL injection, `<script>` = XSS, `../` = traversal.

Worked example. A fake `passwords.xlsx` triggers an alert the moment anyone opens it.

Watch out: To send a secret, use the recipient's PUBLIC key, not your own. Mixing up whose key to use is the most common mistake.

Practice

2.1 Explain what 'symmetric' means in symmetric encryption. [2]

2.2 How many possible keys does a 4-bit key have? [1]

2.3 Which key do you use to encrypt a message you are sending to someone? [1]

2.4 Explain how a honeypot detects an attacker. [2]

2.5 Match each log clue to its attack: OR 1=1, <script>, ../.

[3]
