

Question 1: What Must Stay Secret? A company publishes its encryption algorithm but keeps each user's key secret. Does publishing the algorithm necessarily make the system insecure? Name the principle from class that supports your answer.

Question 2: Breaking a Shift Cipher A shift cipher uses $\text{Enc}_k(m) = (m + k) \bmod 26$, with $a = 0, b = 1, \dots, z = 25$. You learn that plaintext **cat** encrypts to **fdw** using the same key as an intercepted message.

2.1. What is the key, and what plaintext does **grj** decrypt to?

2.2. Is this exhaustive search or cryptanalysis? Briefly explain.

Question 3: What Can the Attacker Do? Match each scenario to an attack model. Use each letter once.

- | | |
|---------------------|----------------------|
| A. Ciphertext-only | B. Known-plaintext |
| C. Chosen-plaintext | D. Chosen-ciphertext |

- 3.1. ____ The attacker submits messages of their choice and receives their encryptions.
- 3.2. ____ The attacker observes encrypted messages but has no corresponding plaintexts or access to an encryption/decryption service.
- 3.3. ____ The attacker submits modified ciphertexts and receives their decryptions, but cannot request decryption of the target ciphertext itself.
- 3.4. ____ The attacker obtains existing messages and their corresponding ciphertexts, without choosing those messages.