CSCI262 Assignment 2 Answers

1. Puzzle Hashing Analysis

1(a) Distribution of the number of cases that require each number of hashes

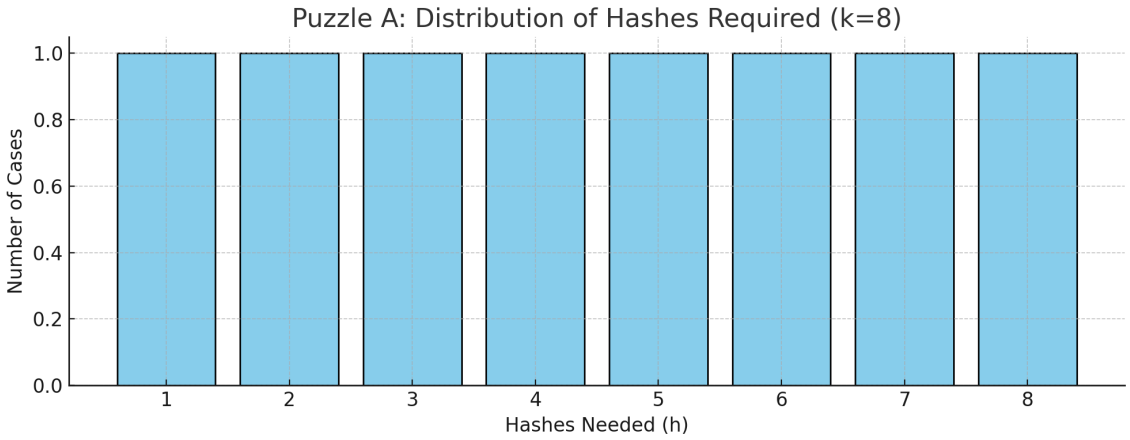
Puzzle A (1 sub-puzzle, k = 8). Total cases = 8

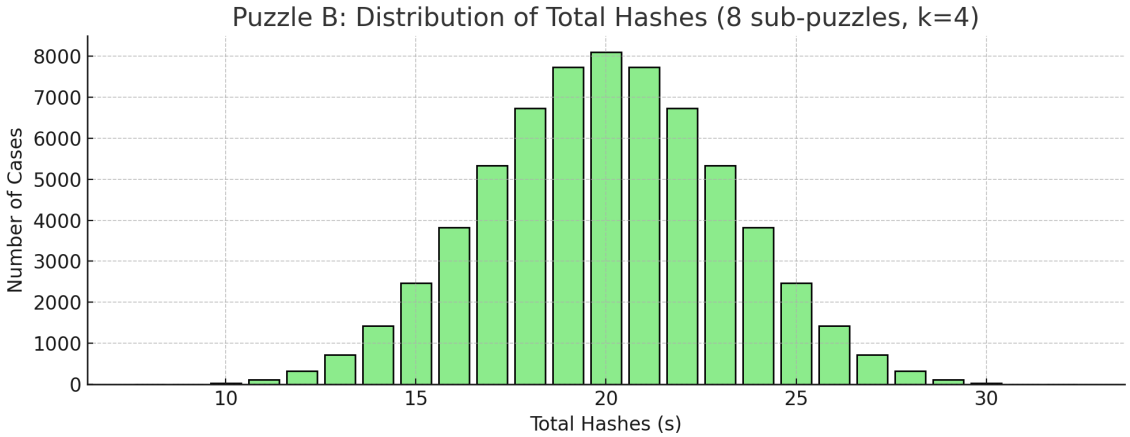
Puzzle B (8 sub-puzzles, each k = 4). Total cases = 4^8 = 65,536

1(b) Method used: Each sub-puzzle modeled as a discrete uniform variable on {1..k}

Puzzle A distribution is uniform. Puzzle B distribution computed exactly by discrete convolution (python enumeration over 4^8 outcomes) and tabulating the sum S frequencies.

1(c) Graph: Plot a discrete bar chart





1(d) Average number of hashes:

Puzzle A = 4.5

Puzzle B = 20.00.

1(e) Standard deviation:

Puzzle A = 2.2913

Puzzle B = 3.1623.

2. Intrusion Detection vs Deception Technologies

Part A:

Signature-based NIDS passively inspects live network traffic for matches to known patterns, triggering alerts on rule hits. A low-interaction honeypot simulates limited services and records any incoming connections as inherently suspicious activity.

Part B: Honeypots reveal intelligence that IDS cannot:

(1) detection of zero-day or novel attacks without signatures

(2)capturing insider reconnaissance or lateral movement attempts. They also help in adversary profiling and early threat research.

Part C:

A honeytoken is a planted fake data object. Example: a fabricated database credential such as 'svc_rnd_ro:P@55-T0k3n-7uQ9'. Any use of this token indicates insider data theft or credential misuse, revealing source and method of compromise.

3. AI-Enhanced Malware and Adaptive Defense

Part A:

Infection counts over time (t = 0–12): 1, 1, 1, 1.10, 1.21, 1.46, 1.77, 2.36, 3.14, 4.60, 6.73, 10.83, 17.45.

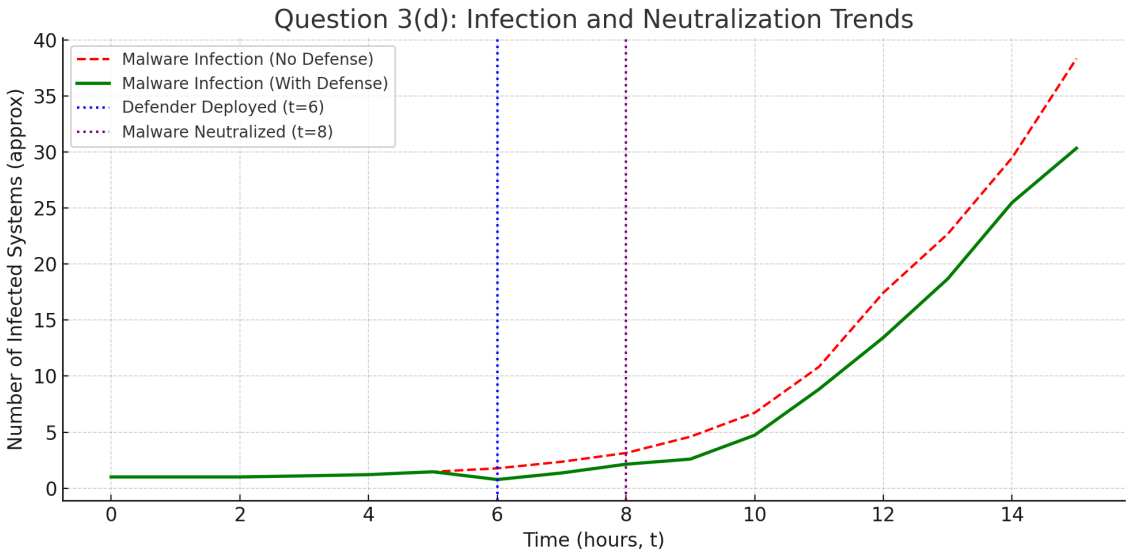
Part B:

With defender from t = 6 to 15, neutralization begins at 1/hour and doubles every 3 hours. Defender fully neutralizes malware by t = 8.

Part C:

Adaptive learning on both sides creates non-linear escalation cycles. The side with faster learning and telemetry advantage gains dominance. Late defender deployment leads to exponential containment costs.

Part D:



4. Access Control Models

Part A:

DAC grants authority to object owners to assign permissions. MAC enforces centrally defined security labels that even owners cannot override.

Part B:

In a corporate R&D setting, DAC allows compromised accounts to leak data via permission changes. MAC enforces data classification and prevents such cross-project leakage by policy-level constraints.

Part C:

DAC relies on user-set minimal permissions to achieve least privilege. MAC encodes least privilege in policy labels and confined process domains, offering stronger system-enforced containment.