

Question 1: AES Ready Signal An AES module takes a secret **key** as input and produces a **ready** signal.

Write an information flow property stating that the secret key should not influence the ready signal.

Question 2: Privileged Register A processor contains a secret privileged register called **kernel_secret**. A user program can observe **user_output**.

Write an information flow property stating that privileged information should not flow to the user-visible output.

Question 3: Debug Interface A chip contains a secret cryptographic key and a debug output.

When the user is not authenticated, information about the key should not flow to the debug output.

Write an information flow property for this policy.

Question 4: Timing Side Channel Consider:

```
if (secret)
    access(array[0]);
else
    access(array[1000]);
```

An attacker cannot read **secret**, but can measure memory access timing.

Write an information flow property describing what should **not** be revealed through timing.