**Practice Problem Set 2**

Prototype

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| Q1 | Midterm 201806 P4 | prototype | \_\_\_ / 12 points |
| Q2 | Midterm 201703 P3 | prototype | \_\_\_ / 12 points |
| Q3 | Midterm 201706 P2 | prototype | \_\_\_ / 10 points |
| Q4 | Midterm 201603 P6 | Prototype | \_\_\_ / 12 points |
| Q5 | 填空 | Data Tampering | \_\_\_ / 12 points |
| Q6 | Final 201703 P16 | Data Tampering | \_\_\_ / 12 points |
|  |  | Total | \_\_\_ / 70 points |
|  |  |  |  |
|  |  |  |  |

**Problem 5: Data Tampering Detection**

**Sender-recipient communication**

Step 1: sender computes \_\_\_ using \_\_\_ and \_\_\_.

Step 2: sender sent \_\_\_ and \_\_\_ to recipient.

Step 3: recipient computes \_\_\_ using \_\_\_ and \_\_\_.

Step 4: recipient compares when \_\_\_ from step \_\_\_ and \_\_\_ from step \_\_\_.

**Server-browser communication**

Step 1: server computes \_\_\_ using \_\_\_ and \_\_\_.

Step 2: server responds to HTTP requests. Server sends \_\_\_ and \_\_\_ to browsers.

Step 3: browsers return \_\_\_ and \_\_\_ to browsers in its subsequent requests.

Step 4: server validates computes \_\_\_ using \_\_\_ and \_\_\_.

Step 5: server validates requests when \_\_\_ from step \_\_\_ and \_\_\_ from step \_\_\_ matches.

Possible choices:

1. MAC
2. Data
3. key (cipher)