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:

(A) MAC
(B) Data
(C) key (cipher)