Question 1: Multiple Choice . . . . . *30 points*

For each question, clearly fill in the bubble for *all* that apply. Some questions may have more than one correct answer. For every wrong answer, you will lose 1 point, but the lowest score you can get for any part (e.g., 1a, 1b) is 0.

(a) (2 points) C stack frames in x86 start from lower addresses and grow towards higher addresses.

- ◯ True
- ◯ False

(b) (2 points) The Same-Origin Policy (SOP) considers two pages to have the same origin when which of the following match?

- ◯ Domain (e.g., `a.com` vs. `b.com`)
- ◯ Fragment identifier (`#anchor`)
- ◯ Scheme (e.g., `http` vs. `https`)
- ◯ Query string
- ◯ Port (e.g., `:80` vs. `:8080`)

(c) (2 points) Which of the following are required properties of a cryptographic hash function?

- ◯ Pre-image resistance
- ◯ Key-dependent output
- ◯ Second pre-image resistance
- ◯ Reversibility
- ◯ Collision resistance

(d) (2 points) Which of the following are true about ARP (Address Resolution Protocol)?

- ◯ ARP messages are encrypted
- ◯ ARP maps IP addresses to MAC (hardware) addresses
- ◯ ARP spoofing can be used to perform man-in-the-middle attacks on a local network
- ◯ ARP operates at the transport layer (Layer 4)
- ◯ ARP has no built-in authentication mechanism

(e) (2 points) Which of the following are defenses against DNS cache poisoning?

- ◯ DNSSEC (cryptographically signing DNS records)
- ◯ Increasing DNS TTL values
- ◯ DNS cookies (a cryptographic challenge-response mechanism)
- ◯ 0x20 encoding (randomizing the case of query names to add entropy)
- ◯ Randomizing the UDP source port used for DNS queries

(f) (2 points) Which of the following are established secure design principles?

- ◯ Defense in depth
- ◯ Security by obscurity
- ◯ Least privilege
- ◯ Complete mediation
- ◯ Privilege separation

(g) (2 points) Which of the following are types of Denial-of-Service (DoS) or DDoS attacks?

- ◯ HTTP flood
- ◯ SQL injection
- ◯ SYN flood
- ◯ Logic-based DoS (exploiting bugs to exhaust server resources)
- ◯ Reflection and amplification attacks

(h) (2 points) Which of the following are x86 general-purpose registers?

- ◯ EAX
- ◯ EIP
- ◯ ECX
- ◯ EDX
- ◯ EBX

(i) (2 points) Which of the following are true about DNS cache poisoning?

- ◯ An attacker can inject forged DNS responses into a recursive resolver's cache
- ◯ DNS cache poisoning requires physical access to the DNS server
- ◯ Bailiwick checking limits what records a name server is allowed to include in a response
- ◯ HTTPS prevents DNS cache poisoning
- ◯ The Kaminsky attack targets an entire zone by flooding a resolver with forged responses for random subdomains

(j) (2 points) Which of the following are true about Subresource Integrity (SRI)?

- ◯ SRI is applied automatically by all browsers without any developer action
- ◯ SRI uses cryptographic hashes embedded in HTML tags to verify third-party resource content
- ◯ SRI prevents all forms of Cross-Site Scripting
- ◯ SRI can prevent malicious code injection when a CDN is compromised
- ◯ SRI encrypts third-party resources in transit

(k) (2 points) Which of the following encryption approaches or modes are considered insecure?

- ◯ Cipher Block Chaining (CBC) mode with a random IV
- ◯ Electronic Codebook (ECB) mode
- ◯ Caesar cipher (easily broken by frequency analysis)
- ◯ AES-256
- ◯ Reusing a one-time pad key for more than one message

(l) (2 points) Which of the following are true about Diffie-Hellman (DH) key exchange?

- ◯ DH allows two parties to establish a shared secret over an insecure public channel
- ◯ DH requires a pre-shared secret to initiate the exchange
- ◯ The security of DH relies on the hardness of the discrete logarithm problem
- ◯ DH directly encrypts messages between the two parties
- ◯ DH is vulnerable to an active man-in-the-middle attack when used without authentication

(m) (2 points) Which of the following are true about BGP (Border Gateway Protocol)?

- ◯ BGP is used for routing between different Autonomous Systems on the Internet
- ◯ BGP hijacking can redirect Internet traffic through an attacker-controlled network
- ◯ BGP provides end-to-end encryption of routed traffic
- ◯ BGP has no built-in mechanism to authorize route announcements
- ◯ BGP is only used within a single organization's internal network

(n) (2 points) Which of the following are true about HTTP cookies?

- ◯ Cookies are set by the server using the `Set-Cookie` response header
- ◯ The browser validates the authenticity of cookie contents
- ◯ Persistent cookies have a specified expiration date
- ◯ Cookies are encrypted by default
- ◯ Session cookies are deleted when the browser session ends

(o) (2 points) Which of the following are true about Certificate Authorities (CAs) and the PKI?

- ◯ Root CA certificates are hardcoded into browsers and operating systems
- ◯ CAs can decrypt TLS traffic to any site for which they issued a certificate
- ◯ A CA signs a server's public key (in a certificate) to vouch for its identity
- ◯ A misissued certificate for a domain can enable a man-in-the-middle attack against that domain
- ◯ Intermediate CAs can issue certificates on behalf of a root CA

Question 2: Short Answer . . . . . *6 points*

Fill in your answers as succintly as possible.

(a) (2 points) What is RSA, and how would you encrypt a message to Bob with an RSA scheme assuming a public modulus N, message m, and Bob's public key (e, N)?

(b) (2 points) List two network protocols that seek to *add* security on top of an existing, insecure protocol.

(c) (2 points) What was the Mirai botnet, and what was the fundamental vulnerability that enabled Mirai to wreak havoc on the Internet in 2016?

Question 3: PA5 Question . . . . . *9 points*

(a) (2 points) A message has been encrypted using a Vigenere cipher with the following key. What is the plaintext?

```
Encrypted message: "GFSDNVEQS"
Vigenere cipher key: "AREALKEY"
```

You can use the alphabet below to help you decode the message:

```
A B C D E F G H I J K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
```

(b) (2 points) Assume that MD5 operates on blocks of size 512 bits. What would be the length of the padding (in bits) generated by the algorithm if you apply the cipher to a message that is 1536 bits long?

(c) (3 points) Examine at the following code snippet.

```
m = "message"
h = md5()
digest = h.hexdigest()
print(digest)

h = md5(state = digest.decode("hex"), count = 512)
print(h.hexdigest())
```

Assume the proper libraries from PA5 has been imported. Will the two print statements print the same string? Explain.

(d) (2 points) Ben Bitdiddle decides to write code for an actual length extension attack, but his code doesn't work:

```
from md5 import md5
m="im ben"
x="im bennnnn"
h=md5()
h.update(m)
d=h.hexdigest()
```

```
h=md5(state=d.decode("hex"),count=512)
h.update(x)
assert(h.hexdigest()==md5(m+x).hexdigest())
```

He expects the assertion to be true, demonstrating a hash collision. Instead, it throws an assertion error. What did Ben forget?