

- a. Users A and B share a symmetric key K_{AB} . B receives an encrypted file F purporting to be from A, and decrypts it with K_{AB} , producing a file F'. From this B can conclude that A sent the file.
(t) True
(f) False
- b. The “one-time pad” approach to encryption can produce an unbreakable ciphertext (i.e., one that can never be broken without access to the secret keying material).
(t) True
(f) False
- c. Assuming a pre-image resistant hash function H, given the hash $h=H(m)$ of the message m, it is impractical to find the corresponding input m.
(t) True
(f) False
- d. An e-mail encrypted using the public key of the recipient prevents anyone from changing the email without it being detected.
(t) True
(f) False
- e. The heap spray technique is used to bypass the Stack Cookie/Canary defense.
(t) True
(f) False
- f. Cookies can be used to tie distinct HTTP requests to the same originating browser and thereby establish a “browsing session” with a particular site.
(t) True
(f) False
- g. One way to address the possibility of stolen/compromised Web certificates is for the Web browser to query the signing Certificate Authority to ask if the certificate has been revoked.
(t) True
(f) False
- h. A web site is generally free to load a Javascript file from any other site, regardless of the site’s origin.
(t) True
(f) False
- i. SQL injections attacks are possible because user input data incorporated into a SQL query can be misinterpreted as being SQL code itself.
(t) True
(f) False
- j. A network firewall is an effective mitigation against SQL injection attacks.
(t) True
(f) False
- k. Phishing is the act of cracking a user’s password from a leaked password database.
(t) True
(f) False

2. [2 pts] Bob wishes to send a message to Alice, such that Eve is unable to read it, such that any modifications made by Eve will be detected by Alice and such that Alice will know that any valid message from Bob was indeed sent by him (i.e., and not really sent by Eve). He and Alice have previously exchanged their public keys (Bob's being BK and Alice's being AK), and they each hold the corresponding private keys (Bk and Ak respectively). To send the message Bob will: (select one)
- (a) Encrypt with BK then sign with BK
 - (b) Encrypt with BK then sign with Bk
 - (c) Encrypt with BK then sign with AK
 - (d) Encrypt with Bk then sign with BK
 - (e) Encrypt with Bk then sign with Bk
 - (f) Encrypt with Bk then sign with AK
 - (g) Encrypt with AK and sign with BK
 - (h) **Encrypt with AK then sign with Bk**
 - (i) Encrypt with AK then sign with AK
3. [7pts] The SynCookie defense against Denial-of-service attacks defers the creation of new TCP state upon receiving a SYN packet and encodes the connection state into the *initial sequence number* it returns (aka the SYNCookie). Which of the following statements are true about this defense (fill in all that apply)?
- (a) It is a general denial-of-service defense
 - (b) It is a defense against SYN flood attacks with valid source addresses
 - (c) **It is a defense against SYN flood attacks with spoofed source addresses**
 - (d) **It assumes that the attacker cannot blindly calculate the SYNCookie**
 - (e) **It assumes that the attacker is unable to observe the SYNCookie**
 - (f) It can provide an effective defense against bandwidth consumption attacks
4. [6pts] The operating system kernel protects itself from user programs using which of the following techniques? (fill in all that apply)
- (a) **Only allowing user programs to execute in the processor's unprivileged execution mode**
 - (b) **Carefully validating the arguments passed in system calls from user programs**
 - (c) Encrypting the kernel heap to protect it from being read or altered by user programs
 - (d) **Protecting the memory holding kernel data structures from being read/written by user programs**
 - (e) Randomizing the order in which user programs execute
 - (f) Flushing the processor cache after each system call