1. [5 points] State whether the following statements are True (T) or False (F).

Statement	T/F?
The Principle of Economy of Mechanism states that secure software mechanisms should be economically feasible to implement.	
Write XOR Execute can be used to defend systems against Return-Oriented Programming.	
It is better to encrypt passwords than to hash and salt them for storage.	
Spear-phishing is an effective way to infect the victim with trojan horses.	
Each browser comes with a store of private signing keys from Certificate Authorities to facilitate SSL/TLS.	

2. [8 points] CIRCLE the correct answer for the following multiple choice questions.

(I) What is Heartbleed?

A. A buffer overflow vulnerability in OpenSSL.

B. An unintentional flaw in OpenSSL that allowed an attacker to gain root privileges on the server.

C. A vulnerability in OpenSSL that allowed a worm to spread to servers that were running it.

D. A missing bounds check in OpenSSL that allowed the web client to specify an arbitrary amount of data that the server should reply with.

(II) Which of the following is **not** helpful when writing a security patch?

A. Integration testing.

B. Regression testing.

C. Security testing.

D. Penetration testing.

(III) Which of the following Saltzer and Schroeder's Principle is violated when a TOCTTOU attack succeeds?

A. Complete mediation

B. Fail-safe defaults

C. Separation of Privileges

D. Least Privilege

(IV) SQL injection occurs because:

A. The SQL server code has a buffer overflow vulnerability.

B. The SQL server code has no backup.

C. The SQL server code redirects users to malicious pages.

D. The SQL server code parses inputs incorrectly.

3. **KRACK on WPA2** [13 points]

On October 16, 2017, researchers announced the discovery of a new attack against WPA2 called KRACK (Key Reinstallation Attack) that threatens almost all encrypted Wi-Fi access points (AP). WPA2 uses RC4, which has a publicly known keystream generation function G, which takes as input some key K and initialization vector IV to produce keystream $G(K, IV)$. (Assume RC4 is secure.) K is 128 bits long and IV is 48 bits long. The plaintext M is encrypted to become $C = Enc_{K,IV}(M) = G(K, IV) \oplus M$. KRACK allows a Man-in-the-Middle (MITM) to compromise a Wi-Fi client.

(a) [3 points] A particularly deadly variant of this attack allows the MITM to set the key K to 0 for both the AP and the client. This works on some versions of Android. Describe exactly how this can be used to decrypt some message C using our notation.

(b) [4 points] On non-Android systems, KRACK does the following: After the client and the AP agree on some secret key K, the IV will be set to 0. It will increment by 1 for every message sent. After some messages have been sent, the attacker can retransmit some messages to force the client to reset the IV to 0. Describe exactly how this can be used to decrypt some message C using our notation.

(c) [3 points] One may suggest that a fix to the attack is not to use a counter, but to simply use a random IV for every message. Explain why this fix does not work by using the birthday paradox.

(d) [3 points] An attacker can use KRACK to both encrypt and decrypt packets. How can an attacker use KRACK to infect a user with malware? Consider a user who is browsing websites.