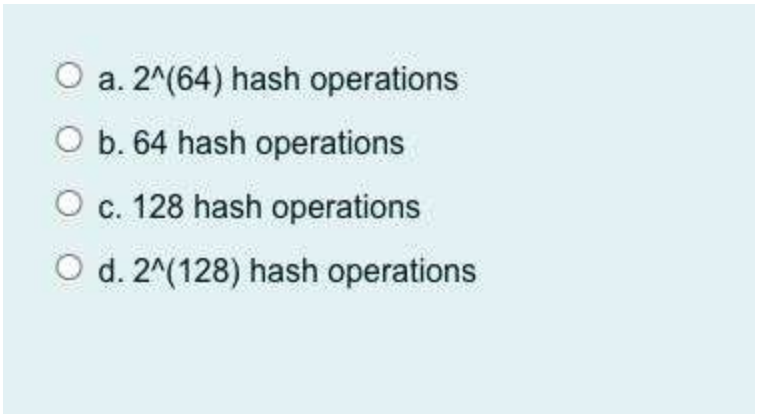
1. Spam emails are just annoying to the user but they cannot be used as attack vectors for malware
    a. **False**
2. A cryptographically secure MAC scheme ensures the confidentiality of the message
    a. **False**
3. The use of constant exponentiation time provides protection against timing analysis attacks of RSA
    a. **True**
4. A faster Tor connection can be obtained by configuring the Tor circuit to have a large number of relays
    a. **False**
5. Let H denote a cryptographically secure hash function. If the output of H is 128 bits, then one can find a collision in about
    a. 

    b. **2^64**
6. A cryptographically secure MAC scheme ensures the confidentiality of the message
    a. **False**
7. Reverse engineering the domain generation algorithm can lead to takeover of the botnet by another botmaster.
    a. I think this is **true**. You can buy the domains before them and give them new instructions of your own.
8. Nonces are used to defend against replay attacks

    a. **True**
9. Let H denote a cryptographically secure hash function. If there are only a few possibilities for M, an eavesdropper who sees H(M) can figure out what M is.
    a. **True**
10. During an off-line dictionary attack, suppose the attacker has a dictionary of 100,000 entries, and he/she downloaded a password file from the server, which contains password hashes for 100 users. If the server is not using salt, and the attacker's goal is to get a particular user's password, then at most how many hash values will the attacker compute?
    a. **100 000** ← because no salt means the hash is the hash, so the dictionary will have those 100 in it stored like that
    b. 10 000 000
    c. 100
11. During an off-line dictionary attack, suppose the attacker has a dictionary of 100,000 entries, and he/she downloaded a password file from the server, which contains password hashes for 100 users. If the server is using salt and among the 100 salts only 50 are distinct, and the attacker's goal is to get as many passwords as possible, then at most how many hash values will the attacker compute?
    a. 50
    b. 100,000
    c. **5,000,000** ← because since there are 50 salts, any of the 100 could be using them
12. An air-gapped computer does not need to have additional protection by an antivirus
    a. **False** - For example USB stick attack
13. Let H denote a secure hash function, Ek(.) denotes a secure (symmetric key) encryption of the enclosed argument using key k. Also let a|b denote the concatenation of a and b. Alice computes the ciphertext c=Ek1(m|H(k2|m)) using two secret keys k1 and k2 that are shared with the receiver Bob. Using the above scheme achieves **both confidentiality and integrity o**f the message m.

    a. **True**
14. Let H denote a secure hash function, Ek(.) denotes a secure (symmetric key) encryption encryption of the enclosed argument using key k. Also let a|b denote the concatenation of a and b. Alice computes the ciphertext c=Ek1(m|H(k2|m)) using two secret keys k1 and k2 that are shared with the receiver Bob. Using the above scheme achieves non-repudiation (i.e., prevents Alice from denying that she sent the message m to Bob)
    a. **False** - alice and bob both know the secret keys, so alice could deny it was her and say its possible it was bob
15. Compared to IRC-based botnets, P2P botnets are easier to takedown
    a. FALSE
16. One of the countermeasures against Botnets is to dilute the stolen identity information from a botnet with false credentials
    a. True
17. Cryptographic hardware implementations using the square and multiply algorithm are susceptible to power analysis attacks
    a. True
18. Let H denote a cryptographically secure hash function. If there are only a few possibilities for M, an eavesdropper who sees H(M) can figure out what M is.
    a. **TRUE**
19. Let m be a binary message of length 128 bits. Let k be a seceret key of length 128 bits. The following mapping (m,k) -> ((m^2 mod (2^128)) XOR k) is a possible encryption function of m.
    a. **true** because it boils down to One time pad
20. To improve the resilience of Botnets, Random Domain Generation can be combined with fast fluxing.
    a. **True**
21. Password reuse across different online services does not present a threat to user
    a. **False**
22. Malware can target both the IT (Information Technology) network and the OT (Operational Technology) network

    a. **True**

23. When fast fluxing is used by botnets, numerous domain names will be associated with a single IP address
    a. **False**, its one domain name, multiple IP addresses
24. Crowds is a P2P system and it does not require a central server
    a. **False**(Need a central blender)
25. Consider a server using Lamport Scheme for authentication. Suppose the current value on the server is H90(k) (where Hx(k) means hashing the secret k for x times). If an attacker somehow knows the value H40(k), then at most how many times could he/she logon?
    a. **50**. Hash your H(40) 50 more times and get H90. Then you know the next 50 passwords to give, from 90 to 40
    b. 40
    c. 90
26. Compared to static analysis, dynamic analysis of malware is more complete
    a. **False** - static makes you see all the code.
27. Vishing is a cybercrime in which a target is contacted by email
    a. **false**: its by voice