

Cybersecurity B - Div B - 20201219 - Cybersecurity - December 19 SO Practice - 12-19-2020

Please note: HackerRank contest will not be extended.

1. (0.00 pts)

Please enter up to two HackerRank usernames that signed up for the hands-on portion at <https://www.hackerrank.com/so-p-b-1608384000> (<https://www.hackerrank.com/so-p-b-1608384000>). First username given below will be used for grading. **Do not enter your email address(es) and/or name(s).**

2. (1.00 pts) A client certificate is required to

- A) Prove the client is who it says it is
- B) Prove that the client can connect to the server
- C) Prove that the server is who it says is
- D) All of the above

3. (3.00 pts) Which numbers would you likely find in an RSA private key, but not in a public key

(Mark ALL correct answers)

- A)  $q$
- B)  $e$
- C)  $n$
- D)  $m$
- E)  $\phi$
- F)  $d$

4. (1.00 pts) To set cookies, what header should be sent by the server?

- A) Content-Type
- B) Set-Cookie
- C) DNT
- D) X-Powered-By
- E) Server

5. (1.00 pts) \_\_\_\_\_ HTTP header tells browsers not to load a page in an *iframe* element.

6. (3.00 pts) How many rounds are there in AES for 128-bit keys, 192-bit keys and 256-bit keys?

7. (4.00 pts) For RSA cipher, if the public key is (9797, 8849) and private key for decryption is 1649; then what is the decrypted value of 5442?

8. (2.00 pts) Decode *BOCSACYETFUKNORCIEASLOPTD* encoded with RailFence encoder with 3 rails.

Type your letters below the corresponding given letters. Your letters can be lower or upper case.

B	O	C	S	A	C	Y	E	T	F	U	K	N	O	R	C	I	E	A	S	L	O	P	T	D

9. (2.00 pts) What is a nonce in cryptography?

10. (2.00 pts)

You need to send the value "Jack & Jill" in the following URL for the query parameter "searchstring". The partial URL is "https://www.mydomain.com?searchstring=". Please **enter the full URL below** completing the portion after "=".

11. (1.00 pts) What is the length (in bits) of a hash generated by MD5?

- A) 16
- B) 256
- C) 128
- D) 64

12. (1.00 pts) \_\_\_\_\_ attribute is used to create a persistent cookie.

13. (3.00 pts) Which of the following are hashing algorithms?

(Mark **ALL** correct answers)

- A) Whirlpool
- B) Vigenère
- C) SHA-3
- D) MD4

