Cybersecurity C - Div C - 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-c-1608369600 (https://www.hackerrank.com/so-p-c-1608369600). 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. (1.00 pts) ____ is needed to ensure same password, when hashed twice does not result in same output.

4. (2.00 pts)
Give an example of how information-theoretic security and computational security were used in the year 2000 -- after modern cryptography, but before any quantum communications existed.

5. (1.00 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) Φ

□ F) d

6. (1.00 pts) As a best practice, which of the following headers should be suppressed by web servers when servicing the requests?

(Mark **ALL** correct answers)

□ A) Content-Type

□ B) Set-Cookie

□ C) DNT

□ D) X-Powered-By

□ E) Server

7. (3.00 pts) For RSA cipher, if the public key is (222559, 47171) and private key for decryption is 133311; then what is the decrypted value of 99563?

8. (1.00 pts) ______ HTTP header tells browsers not to load a page in an *iframe* element.

9. (4.00 pts) Compute d for RSA key given the following information:

p = 6823, q = 1021, n = 6966283, Φ = 6958440, e = 884587

10. (3.00 pts) How many rounds are there in AES for 128-bit keys, 192-bit keys and 256-bit keys?

11. (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?

12. (2.00 pts) Decode *TOEOOSPCDTFDSRIASLAIATYEUKYCBC* encoded with RailFence encoder and variable number of rails.

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

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

13. (4.00 pts) What is a nonce in cryptography? Give three or more characteristics and/or usages of nonce .

14. (1.00 pts) Check all that apply to prevent a SQL injection attack.

(Mark **ALL** correct answers)

□ A) Allow any user input

□ B) Parameterized queries

□ C) Use stored procedures

□ D) Always return error no matter what the user wants

□ E) Use nosql databases.

15. (2.00 pts) Consider an application with this snippet of code:

```
if ($_POST["secret"] == $SUPERSECRET) {
admin_login();
} else {
get_mad();
}
```

What character should be added to make the above code secure?