# Grade Book Detail

## 吴杰枫,

### Quiz 7

Started: January 2, 2024, 11:43 am
Last change: January 2, 2024, 11:58 am

**Showing Scored Attempts** | Show Last Attempts | Show Review Attempts

Hide Perfect Score Questions | Hide Not Answered Questions

**Which protocol uses UDP?**

- ○ TELNET
- ◉ DNS
- ○ SMTP
- ○ HTTP

1. Show Answer DNS

Question 1: 5 out of 5 in 1 attempt(s)

**The general format for URL is _____.**

- ◉ protocol://hostname/pathname
- ○ protocol:/hostname/pathname
- ○ /hostname/pathname
- ○ //hostname/pathname:protocol

1. Show Answer protocol://hostname/pathname

Question 2: 5 out of 5 in 1 attempt(s)

**A host would like to know the IP address for www.zju.edu.cn. Suppose that this host has configured the DNS server as 210.32.32.1. Furthermore suppose the IP address for the top DNS server is 12.12.12.12 and the IP address for the actual DNS server storing the www.zju.edu.cn and its IP address is 210.32.1.1. Then this host will first contact the DNS server with the IP address as _____.**

- ○ 210.32.1.1
- ○ 12.12.12.12
- ◉ 210.32.32.1
- ○ undefined

1. Show Answer 210.32.32.1

Question 3: 5 out of 5 in 1 attempt(s)

**Which is used to keep track of a user and its related information by the Web server?**

- ○ web cache
- ○ persistent connection
- ◉ cookie
- ○ conditional GET

1. Show Answer cookie

Question 4: 5 out of 5 in 1 attempt(s)

**The resource record type _____ is related to the mail server.**

- ○ CN
- ◉ MX
- ○ NS
- ○ SOA

1. Show Answer MX

Question 5: 5 out of 5 in 1 attempt(s)

**When you configure static IP address parameters: IP address, subnet mask, default gateway, IP address relating to DNS, which name server's IP address is used?**

- ○ proxy name server
- ○ authoritative name server
- ◉ local name server

○ top-level name server

1. Show Answer local name server

Question 6: 5 out of 5 in 1 attempt(s)

**Which encryption algorithm is the slowest one?**

○ SHA-1

○ AES

◉ RSA

○ IDEA

1. Show Answer RSA

Question 7: 5 out of 5 in 1 attempt(s)

**Public-key algorithms have the property that _____ keys are used for encryption and decryption and that the decryption key cannot be derived from the encryption key. These properties make it possible to publish the public key.**

○ one time

○ random

○ same

◉ different

1. Show Answer different

Question 8: 5 out of 5 in 1 attempt(s)

The basic concept of RSA algorithm is to compute $P^e$ mod n and $C^d$ mod n. Bob wants to make a test for RSA algorithm. To generate a pair RSA key, he chooses 3 and 11 for the two prime p and q, so, the modulo number n will be 33 , the number z, product of p-1 and q-1, will be 20 . Then he chooses 7 as the value of number d, relatively prime to z, and find the minimum value of number e (will be 3 ), such that e x d = 1 mod z.

Now, he has the public key pair (e, n) and the private key pair (d, n). Bob and Alice uses a coding scheme like following:

| code | char | code | char | code | char | code | char | code | char |
|---|---|---|---|---|---|---|---|---|---|

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | NUL | 1 | A | 2 | B | 3 | C | 4 | D |
| 5 | E | 6 | F | 7 | G | 8 | H | 9 | I |
| 10 | J | 11 | K | 12 | L | 13 | M | 14 | N |
| 15 | O | 16 | P | 17 | Q | 18 | R | 19 | S |
| 20 | T | 21 | U | 22 | V | 23 | W | 24 | X |
| 25 | Y | 26 | Z | 27 | space | 28 | + | 29 | – |
| 30 | * | 31 | / | 32 | = | 33 | : | 34 | ? |

Alice send a encrypted message to Bob using RSA algorithm: **EZNGQZXI**

Please help Bob to decrypted the message and write the plaintext here:
23

1. Show Answer 33
2. Show Answer 20
3. Show Answer 3
4. Show Answer NET+HERO

Question 9: 15 (parts: 5, 5, 5, 0) out of 20 in 1 attempt(s)

Alice wants to send a signed plaintext email message, P, to Bob in a secure way. Please help Alice and Bob to achieve the goal.

Fill in the blank with the corresponding number of the alternative answer:

1) the public key of Alice 2) the private key of Alice 3) the public key of Bob

4) the private key of Bob 5) the public key of CA 6) the private key of CA

7) the RSA algorithm 8) the AES algorithm 9) the SHA–2 algorithm

Firstly, Bob sends a certificate to Alice. and Alice must check it. Which algorithm should Alice use? 3 , and which key should Alice use? 7

Alice hashes her message, P, using 9 , and then encrypts the resulting hash using 8 (algorithm) with 2 (key).

The encrypted hash and the original message are now concatenated into a single message, P1, and then compressed using the ZIP program. Call the output of this step P1.Z. Next, Alice generate a 256–bit random session key, KM, which used to encrypt P1.Z with 5 . In addition, KM is encrypted with 8 (algorithm) using 6 (key). These two components are then concatenated and converted to base64 to send in email system.

| | |
|---|---|
| 1. Show Answer | 7 |
| 2. Show Answer | 5 |
| 3. Show Answer | 9 |
| 4. Show Answer | 7 |
| 5. Show Answer | 2 |
| 6. Show Answer | 8 |
| 7. Show Answer | 7 |
| 8. Show Answer | 3 |

Question 10: 10 (parts: 0, 0, 5, 0, 5, 0, 0, 0) out of 40 in 1 attempt(s)

Total: 65/100

Return to GradeBook