Public Key Cryptography

23.1. In the Diffie-Hellman key exchange, Alice sends $g^x \mod p$ to Bob, and Bob sends $g^y \mod p$ to Alice. How do they get a common secret?

23.2. In the Diffie-Hellman key exchange protocol, attackers know g, p, and $g^x \mod p$. Why can't attackers figure out x from these data?

23.3. Let $n = 3 * 11$ and $e = 3$, find the private exponent d.

23.4. Let $n = 2419 = 41 * 59$ and $e = 7$. (1) Find the private key d. (2) Encrypt the message 6. (3) Sign the message 10. Assume RSA is used. You only need to show the formula; there is no need to calculate the final results.

23.5. We choose $p = 17$ and $q = 13$, can we choose $e = 3$ as the public exponent?

23.6. Bob just discovered an efficient algorithm to factor large numbers, i.e., for any given number n, Bob can factor the number in $O(log(n))$ time. Please describe the impact of this discovery on the RSA algorithm.

23.7. In RSA, decryption is much more expensive than encryption, why?

23.8. Why do we use hybrid encryption? Why can't we use public key to encrypt everything?

23.9. Let M be a string of size 1000 bytes, Bob tries to encrypt M directly using a 2048-bit RSA key, i.e., calculating $M^e \mod n$. Will he be able to do this?

23.10. In the RSA algorithm, since doing $(M^e)^d \mod n$ and $(M^d)^e \mod n$ always get the same result M. Bob decides to keep e as the private key and use e to do the decryption, and publish d as the public key, and use d to do the encryption. Is this safe?

23.11. In the PKCS#1 v1.5 and OAEP padding schemes, the first byte of the padding is always 00, what is its main purpose?

23.12. A message M is padded using the PKCS#1 v1.5 scheme. The padded data are shown in the following. Which part is the original message M?

```
0002 19ba 93fa 39af ... 039a 8818 1903 dfa0 3300 fa31 ff93 dd19
cad5 6356 fa30 f003
```

23.13. When a message is encrypted twice, the ciphertext should be different. This is an important requirement for encryption. Please describe how AES-128-CBC and RSA encryption achieve this property.

23.14. Both AES-128-CBC and RSA use paddings, but their purposes are different. What are their differences?

23.15. ★

Digitial signature is typically put on the one-way hash of the message, instead of on the message directly. One of the reasons is the cost, because signing a short hash value is more efficient than signing a message that can be very long. Bob says that his message is always short, so he decides to directly sign the message, rather than signing its hash. (1) Without knoing Bob's private key, can you generate a pair (m, s), where s is Bob's signature on m, and m can be anything? (2) If Bob signs the one-way hash of the message, can you still generate such a pair?

23.16. What is the benefit of public-key based authentication scheme, compared to the password-based scheme?

23.17. Charlie has arranged a blind date for Alice and Bob, who are both cryptographers, and they do not know each other before. Bob wants to make sure that the person he is dating is actually Alice, not somebody else. Before going to the dating, he got a copy of Alice's public key from Charlie. Please describe how Bob can ask Alice to prove that she is Alice (please do not try this in the real life, or you will probably never see your date again).

23.18. ★

Somebody ask you to sign a number that seems like a random number. You think there is no harm to sign such a number using your private key. Do you agree or not? Why?

23.19. In the chip technology used in credit cards, how does the terminal know that a credit card is issued by an authorized bank?

23.20. In the chip technology used in credit cards, how does the card issuer know that the owner of the card has approved a payment?