Secret-Key Encryption

Copyright © 2019 by Wenliang Du, All rights reserved.
Personal uses are granted. Use of these problems in a class is granted only if the author's book is adopted as a textbook of the class. All other uses must seek consent from the author.

C1.1. A message is encrypted twice using the same key and same algorithm, but the ciphertexts are different. What could be the reason?

C1.2. How does the Enigma machine solve the frequency issues faced by monoalphabetic ciphers?

C1.3. AES is a block cipher; can we use it as a stream cipher, i.e., encrypting messages bits by bits (without using paddings)?

C1.4. Why is ECB not safe?

C1.5. Using ECB mode, students found that if they use a high-resolution BMP file, the encrypted results also look like noise. Please explain.

C1.6. A message of 59 bytes is encrypted using AES with the CBC mode. The padding scheme is PKCS#7. Please describe what the padding data are. What if this message has 64 bytes.

C1.7. Alice encrypts a message using the Counter (CTR) mode, and sends it to Bob. Mallory has intercepted the ciphertext. Although she does not know the entire message, she does know that the 17th byte of the plaintext is 1; she wants to change the value to something else (the rest of the messages should not be changed). Mallory does not know the encryption key, so she can only modify the ciphertext. (1) How can she do that? (2) If Mallory wants to change the value from 1 to 9, what is the probability that she can successfully achieve that?

C1.8. What encryption mode can we use if we want to know whether a ciphertext is tampered with by others?

C1.9. We need to protect a packet, such that the payload of the packet is encrypted, but the integrity of the entire packet, including its header, is protected. What encryption mode can we use to achieve this goal?

C1.10. Alice uses the OFB mode to encrypt her emails sent to Bob, but instead of using randomly generated IVs, she always uses the same IV to encrypt her emails. Charlie somehow got a copy of one of her emails (both plaintext and ciphertext). Is Charlie able to decrypt Alice's other encrypted emails? If yes, please describe how. If no, please provide your reasoning.

C1.11. Alice uses the OFB mode to encrypt her emails sent to Bob, but instead of using randomly generated IVs, she always uses the same IV to encrypt her emails. Charlie somehow gets the following data:

- The first 8 bits of the first ciphertext block: `0x11010101`
- The first 8 bits of the first plaintext block: `0x01111001`

- The first 8 bits of the second ciphertext block: `0x10100100`
- The first 8 bits of the second plaintext block: `0x11001010`

Charlie also get a copy of Alice's newly encrypted message, the first 8 bits of the first two blocks are `0x01010010` and `0x01101001`, respectively. Please derive the first 8 bits of the first two blocks of the plaintext.

C1.12. An encryption machine encrypts data using the CBC mode. Given a plaintext, it can generate a ciphertext. The IV used for different messages is the time when the encryption is performed. The time is the epoch time, i.e., the number of seconds that have elapsed since January 1, 1970 at 00:00:00 GMT. Alice used the encryption machine to encrypt a secret number at Time T (the time T is known to Bob). Bob also knows Alice's ciphertext G. Moreover, he knows that Alice's secret number is either A, B, or C. How can he figure out what exactly Alice's secret number is? Please describe what Bob should do (assuming all the numbers are exactly 128 bits, which is the block size of the cipher).

C1.13. This problem is similar to Problem C1.12., except that the encryption mode used by the encryption machine is the OFB mode. Can Bob find out Alice's secret number?

C1.14. When Alice communicates with Bob, she encrypts her messages using the AES algorithm with the CBC mode. For each of her message, she randomly generate a new IV. She knows that the IV should be sent to Bob in the plaintext, or Bob will not be able to know the IV. However, when encrypting her message, Alice decides to prepend the IV to the beginning of her message, and then encrypt the combined message. She thinks this will not cause any harm, and it may bring some benefits. Do you agree with her? Is this practice safe?

C1.15. Alice encrypts a message using AES, and sends the ciphertext to Bob. Unfortunately, during the transmission, the 2nd bit of the third block in the ciphertext is corrupted. How much of the plaintext can Bob still recover if the mode of encryption is one of the followings: CBC, CFB, OFB, or CTR?

C1.16. Alice encrypts a message using AES, and sends the ciphertext to Bob. Unfortunately, during the calculation of the third block, a lightning struck Alice's house, corrupting the 2nd bit of the AES output (for the third block). Fortunately, nothing else of the calculation was affected. How much of the plaintext can Bob still recover if the mode of encryption is one of the followings: CBC, CFB, OFB, or CTR?

C1.17. An encryption machine has encrypted a message P using the CBC mode and a secret key. The key K is fixed, and it is not known to users. Bob knows the ciphertext C and the IV used in the encryption. The encryption machine has a padding checking functionality, i.e., given an IV and a ciphertext, it decrypts the message and tell you whether the padding is valid or not. The machine will not tell you the decrypted message. Please describe how you can use this functionality to decrypt the ciphertext C. You only need to provide the details to show how you can decrypt the last three bytes of the second block (P has 10 blocks).

C1.18. (April Fools' Day's pranking question ☺☺☺): Please describe a way so we can encrypt a message using the DES algorithm, and then decrypt it using the AES algorithm.

✍ **Answer:** This problem is impossible to solve. This is meant to be given as a quiz question on the April Fool's day. Please do not use it on other days.