

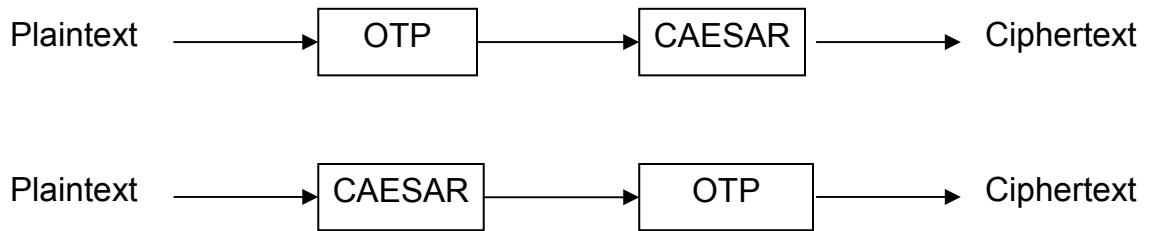
ICS 134

Homework 1

Due Friday January 26, 5pm PST
Submission by email to the TA: plaintext or PDF only.

1. Encrypt the plaintext “KEEPYOURKEYSECRET” using the following ciphers:
 - Caesar cipher using $K=10$
 - Vigenere cipher using “UCI” as the key
2. Decrypt WGVFKUGTBCGHHDKVICKTJDIMQB which was encrypted with the AFFINE cipher. Use the “inside” information that “WG” decrypts to “BA”.
3. ADRFGVK is the output of a Caesar cipher, given some plaintext as input. Which of the followings CAN be true?
 - A is the ciphertext of Q and D is the ciphertext of T
 - A is the ciphertext of S and D is the ciphertext of A
 - None of the above
4. A technique provides message integrity by appending to each message the hash of that message. A hash function is used to compute the hash and it’s infeasible to find two messages that hash into the same value. (Assume each message is sent from A to B over the Internet).
 - Does this technique prevent messages from being modified by the active adversary?
 - If yes, how? If not, modify the technique so that an attacker will be unable to modify messages.
5. List the following attacks from the most powerful to the least powerful:
 - Chosen ciphertext
 - Ciphertext only
 - Known plaintext

6. An double-encryption system encrypts plaintext first with One-Time-Pad (OTP) and, then, with the Caesar cipher. Suppose that the OTP key-stream has been discovered by the attacker. How many trials does the attacker have to do in order to recover the plaintext from any given ciphertext? Would the system more secure if the two ciphers are used in inverse order?



7. Suppose that the following is the output of a substitution cipher:

SIAA ZQ LKBA. VA ZOA RFPBLUAOAR.

What is (with high probability) the ciphertext of the letter 'E'? Explain...

8. Suppose there are n students in a class who want to send encrypted messages to one another, using conventional encryption.

- How many keys would each student have to set up and manage? Why?
- How many different keys would exist in the system overall (i.e., among all n students)? Why?