

ICS 134

Homework 1 Solution

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

1. Encrypt the plaintext “KEEP YOUR KEY SECRET” using the following ciphers:
 - Caesar cipher using $K=10$
 - Vigenere cipher using “UCI” as the key

SOLUTION:

UOOZIYEBUOICOMBOD
EGMJAWOTSYAAYEZYV

2. Decrypt WGVFKUGTBCGHHDKVICKTJDIMQB which was encrypted with the AFFINE cipher. Use the “inside” information that “WG” decrypts to “BA”.

SOLUTION:

$W=22, G=6, B=1, A=0$

$$a + b = 22 \pmod{26}$$

$$a \cdot 0 + b = 6 \pmod{26}$$

$$b=6$$

$$a=16$$

As 16 and 26 have 2 as common factor, the decryption is not possible.

The old version of the problem has the following solution

$$a = 7$$

$$b = 6$$

Plaintext: GARLICANDSAPPHIRESINTHEMUD

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

SOLUTION:

A is the ciphertext of Q and D is the ciphertext of T is the only possible answer because in the Caesar cipher, different letters in the plaintext, once encrypted keep their distance.

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.

SOLUTION:

If the hash function is known, the system is not secure as an adversary can create a fake message with a valid hash. B will think that the message was sent by A. A keyed hash, with a secret common key between A and B would suffice to provide protection against active attackers.

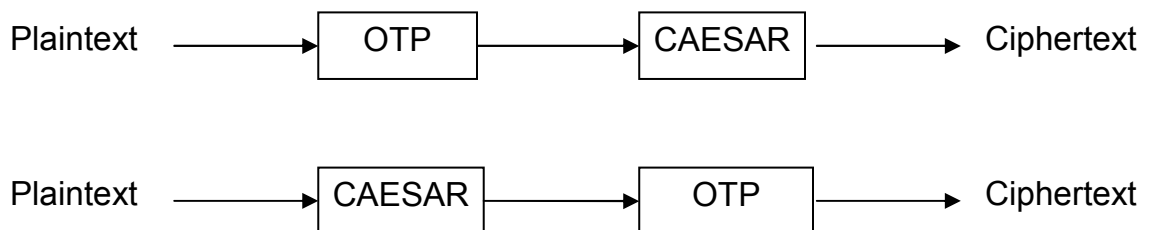
5. List the following attacks from the most powerful to the least powerful:

- Chosen ciphertext
- Ciphertext only
- Known plaintext

SOLUTION:

Ciphertext only
Known plaintext
Chosen ciphertext

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?



SOLUTION:

As we have the keystream for the otp, we can reverse that operation. In the first case, with 26 trials (in the worst case), given the ciphertext, we can recover the output of the otp. Then, as we know the keystream, we can get the plaintext.

In the second case nothing changes as we get the output of the Caesar cipher from the ciphertext (because we know the keystream). Then, with 26 trials (again worst case) we recover the plaintext.

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

SIAA ZQ LKBA. VA ZOA RFPBLUAROAR.

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

SOLUTION

A is probably the ciphertext for E because the former is the letter with the highest frequency in the given ciphertext

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?

SOLUTION:

Each student will manage $n-1$ keys, one for each “communication channel” with each of the other student in the class.

As there are n students, the number of keys in the system is $n(n-1)$. Anyway, as each pair of students shares one key, the former must be divided by 2. Thus, the number of key in the system is $n(n-1)/2$.