CAS CS 538. Solutions to Problem Set 1

Due electronically via gradescope, Monday January 26, 2026 11:59pm

Problem 1. (30 points)

Bob is using the one-time-pad to encrypt a message he sends to Alice. The message is either

- M_0 = `Let's meet at 2.` or
- M_1 = `Let's meet at 5.`

Note that each of these messages has 16 characters in it. Bob converts his message to bytes using ASCII (or UTF-8) encoding with one byte per character, to get 128 bits. He then encrypts the message with the secret key K that only he and Alice know.

An attacker Marlow intercepts the ciphertext C (think of Marlow as being a router between Bob and Alice). Because the one-time pad has one-time secrecy, Marlow cannot understand the message. But, unlike the attacker we discussed in class, Marlow has an additional power: he can modify the ciphertext C to get some C' and then send C' to Alice. Marlow's goal is to get Alice to show up to the meeting at the wrong time. Show how, without knowing whether Bob sent M_0 and M_1, Marlow can ensure that Alice decrypts C' to the other message.

Solution. The solution to this problem comes from the ability that one can **modify** the end result of the OTP (otherwise known as malleability).

For the OTP:

- Enc: $c = k \oplus m$
- Dec: $m = k \oplus c$

Where k is the 128-bit key, m is the 128-bit msg, and c is the 128-bit ciphertext.

The only 2 possible msgs differ in just 1 character ():

- Let's meet at **2**.
- Let's meet at **5**.

So we can just look at these singular bytes (in ASCII).

- $2 \rightarrow$ ASCII 50 (or 00110010)
- $5 \rightarrow$ ASCII 53 (or 00110101)

We can now take the XOR of these values:

$$50 \oplus 53 = 00000111_2 = 7$$

So the product is just 0x07 (in hexa). We can also see from this how only the first 3 bits differ from the messages.

Now we can go ahead with making the atk.

Marlow will compute:

$$\delta = M_0 \oplus M_1$$

Since the msgs are identical expect for the numerical digit, δ will then be a 128-bit val with:

- 15 bytes of 0's (1-14, 16).
- @ position 15, 0x07
- All other bits are 0's

Now, when Marlow intercepts c, he will then compute:

$$c' = c \oplus \delta$$

I can show both cases to show why this works:

- If Bob sent M_0,
  $c = k \oplus M_0$
  $c' = c \oplus \delta = (k \oplus M_0) \oplus \delta$
  So Alice will decrpyt: $k \oplus c' = k \oplus (k \oplus M_0 \oplus \delta) = M_0 \oplus \delta = M_0 \oplus (M_0 \oplus M_1) = M_1$
- If Bob sent M_1,
  $c = k \oplus M_1$
  $c' = c \oplus \delta = (k \oplus M_1) \oplus \delta$
  So Alice decrpyts: $k \oplus c' = k \oplus (k \oplus M_1 \oplus \delta) = M_1 \oplus \delta = M_1 \oplus (M_0 \oplus M_1) = M_0$

Thusly, this proves how Marlow can modify and sent the incorrect message to Alice, without having to know k or which message Bob even sent.

Problem 2. (40 points, at 20 for each part) Alice is using one-time-pad and notices that when her key is the all-zero string 0^L, then $\mathsf{Enc}(K, M) = M$ and her message is sent in the clear! To avoid this problem, she modifies the scheme to sample keys uniformly from $\mathcal{K} = \{0,1\}^L - \{0^L\}$, the set of all L-bit strings except the all-zero string. Before we post the actual questions, we need to recall a definition.

Definition 1 (Textbook, Claim 1.4.1, generalized)**.** (One-Time Secrecy) An encryption scheme $\Sigma = (\mathsf{Enc}, \mathsf{Dec}, \mathcal{K}, \mathcal{M}, \mathcal{C})$ has **one-time secrecy** if for all choices of plaintext $M \in \mathcal{M}$, the ciphertext

$C := \mathsf{Enc}(K, M)$ is uniformly distributed in the ciphertext space $\mathcal{C}$, when the key K is sampled uniformly and used for only one encryption.

Equivalently, we can express this as an attack game. Note that the scheme being attacked is in the superscript and the input message is, as usual, in parentheses.

$\underline{\texttt{ots.attack}^{\Sigma}(M):}$
$K \twoheadleftarrow \Sigma.\mathcal{K}$
$C := \Sigma.\mathsf{Enc}(K, M)$
return C

Then we say Σ has **one-time secrecy** if for any arbitrary message $M \in \Sigma.\mathcal{M}$ and ciphertext $C \in \Sigma.\mathcal{C}$,

$$\Pr[\textsc{attack}^{\Sigma}(M) = C] = \frac{1}{|\mathcal{C}|}$$

Remark 1. There are multiple ways to rewrite Definition 1, because there are many ways to say "the output of ATTACK is uniformly distributed." We do so now.

Then Definition 1 is equivalent to saying that for any message M,

$$\begin{aligned}
\Pr[\textsc{attack}^{\Sigma}(M) = C] &= \Pr_{K \twoheadleftarrow \Sigma.\mathcal{K}}[\mathsf{Enc}(K, M) = C] && \text{Note the subscript notation } \twoheadleftarrow \text{ for sampling} \\
&= \Pr[\mathsf{Enc}(\mathsf{k}, M) = C] && \text{(where k is uniformly distributed over } \mathcal{K}) \\
&= \sum_{K \in \mathcal{K}} \Pr[\mathsf{Enc}(K, M) = C] \cdot \Pr[\mathsf{k} = K] && \text{(by total probability)}
\end{aligned}$$

Note that if $\mathsf{Enc}(K, M)$ is a deterministic algorithm (which it does not have to be!), then $\Pr[\mathsf{Enc}(K, M) = C]$ is either 0 or 1.

(a) Prove that this scheme does *not* have one-time secrecy as defined in Definition 1.

Solution. The solution to this problem comes from the fact that, even if we just *slighty* change the probabilites to not be uniform, it will break the entire shceme.

So firstly, recall the scheme, $\Sigma = (\mathsf{Enc}, \mathsf{Dec}, \mathcal{K}, \mathcal{M}, \mathcal{C})$:

- $\mathcal{K} = 0, 1^L \setminus 0^L$ (all L-bit strings except that one all-zero string),
- $\mathcal{M} = \mathcal{C} = 0, 1^L$,
- $\mathsf{Enc}(k, m) = k \oplus m$,
- $\mathsf{Dec}(k, c) = k \oplus c$.

Looking back at the Definition 1, Σ has OTS IFF for every message $M \in \mathcal{M}$ and every ciphertext $C \in \mathcal{C}$,

$$\Pr[\textsc{attack}^{\Sigma}(M) = C] = \frac{1}{|\mathcal{C}|}$$

where $\textsc{attack}^{\Sigma}(M)$ takes some key K uniformly from $\mathcal{K}$, computes $C = \mathsf{Enc}(K, M)$, and outputs C.

I can show that this equality will fail from a specific case of M and C. Let M be any msg in $\mathcal{M}$ (you could also consider it as taking $M = 0^L$ for more concreteness, but any M works). Now consider the ciphertext $C = M$. Then:

$$\Pr[\textsc{attack}^{\Sigma}(M) = M] = \Pr_{K \leftarrow \mathcal{K}}[\mathsf{Enc}(K, M) = M] = \Pr_{K \leftarrow \mathcal{K}}[K \oplus M = M] = \Pr_{K \leftarrow \mathcal{K}}[K = 0^L].$$

And since $0^L \notin \mathcal{K}$, this probability is 0. But, $|\mathcal{C}| = 2^L$, so $\frac{1}{|\mathcal{C}|} = \frac{1}{2^L} > 0$. Thus,

$$\Pr[\textsc{attack}^{\Sigma}(M) = M] = 0 \neq \frac{1}{2^L}.$$

Thusly, this shows how the scheme does not have OTS.

Remark 2. Demanding that the ciphertext distribution is uniform, regardless of the message, is a bit stronger than we need for secrecy. Even if the ciphertext distribution is not uniform (i.e., some ciphertexts are more likely than others), secrecy is assured as long as the distribution is the same for every M. So one could consider the following, weaker, definition, which is commonly known as "Shannon secrecy" (after Claude Shannon, who first stated it in 1948) or "perfect secrecy." Here it is, in different, equivalent, formulations.

Definition 2. An encryption scheme
$\Sigma = (\mathsf{Enc}, \mathsf{Dec}, \mathcal{K}, \mathcal{M}, \mathcal{C})$ has **Shannon secrecy** if the following, equivalent, statements hold:

- The output distribution of $\textsc{attack}^{\Sigma}(M)$ is the same regardless of which $M \in M$ is given as input
- (Unwrapping what "regardless of which $M \in \mathcal{M}$" means): $\forall M_0, M_1 \in \mathcal{M}$

  the output distribution of $\textsc{attack}^{\Sigma}(M_0)$ is the same as the output distribution of $\textsc{attack}^{\Sigma}(M_1)$.

- (Unwrapping what "same distribution" means): $\forall M_0, M_1 \in \mathcal{M}, \forall C \in \mathcal{C}$,

$$\Pr[\textsc{attack}^{\Sigma}(M_0) = C] = \Pr[\textsc{attack}^{\Sigma}(M_1) = C]\,.$$

- (Unwrapping what "$\textsc{attack}$" means): If k is uniformly distributed over $\mathcal{K}$, then $\forall M_0, M_1 \in \mathcal{M}$, $\forall C \in \mathcal{C}$,

$$\Pr[\mathsf{Enc}(\mathsf{k}, M_0) = C] = \Pr[\mathsf{Enc}(\mathsf{k}, M_1) = C]\,.$$

(b) Prove that this scheme does *not* have Shannon secrecy as defined in Definition 2.

Solution. The way we can show how this scheme doesn't have Shannon secrecy is through the fact that the probability distribution of the ciphertexts literally depend on the msg itself (as we basically can't have an all-0 message), causing a contradiction in the scheme.

Recall the scheme Σ, and the definitions of each of its parameters. Looking at Definition 2, Σ has Shannon secrecy IFF for every pair of messages $M_0, M_1 \in \mathcal{M}$ and every ciphertext $C \in \mathcal{C}$,

$$\Pr[\mathsf{Enc}(\mathsf{k}, M_0) = C] = \Pr[\mathsf{Enc}(\mathsf{k}, M_1) = C],$$

where k is uniformly distributed over $\mathcal{K}$.

I will show a case where this equality will fail. Let M_0 and M_1 be two distinct messages in $\mathcal{M}$ (you can say that $M_0 = 0^L$ and $M_1 = 0^{L-1}1$, but really any two distinct messages work). Consider the ciphertext $C = M_0$.

For any message M and ciphertext C, since $\mathsf{Enc}(k, M) = k \oplus M$, we have:

$$\Pr[\mathsf{Enc}(\mathsf{k}, M) = C] = \Pr[\mathsf{k} = C \oplus M].$$

Because k is uniform over $\mathcal{K}$, this probability is $1/(2^L - 1)$ if $C \oplus M \in \mathcal{K}$ (i.e., $C \oplus M \neq 0^L$), and 0 otherwise.

Now we can compute for M_0 and $C = M_0$:

$$\Pr[\mathsf{Enc}(\mathsf{k}, M_0) = M_0] = \Pr[\mathsf{k} = M_0 \oplus M_0] = \Pr[\mathsf{k} = 0^L] = 0,$$

since $0^L \notin \mathcal{K}$.
For the same $C = M_0$ but with message $M_1 \neq M_0$:

$$\Pr[\mathsf{Enc}(\mathsf{k}, M_1) = M_0] = \Pr[\mathsf{k} = M_0 \oplus M_1].$$

Since $M_0 \neq M_1$, we have $M_0 \oplus M_1 \neq 0^L$, hence $M_0 \oplus M_1 \in \mathcal{K}$. Therefore,

$$\Pr[\mathsf{Enc}(\mathsf{k}, M_1) = M_0] = \frac{1}{2^L - 1}.$$

And thusly,

$$\Pr[\mathsf{Enc}(\mathsf{k}, M_0) = M_0] = 0 \neq \frac{1}{2^L - 1} = \Pr[\mathsf{Enc}(\mathsf{k}, M_1) = M_0],$$

This contradicts the condition we need for Shannon secrecy, and therefore shows how this function does not have Shannon secrecy.

Problem 3. (30 points) Let $\Sigma = (\mathsf{Enc}, \mathsf{Dec}, \mathcal{K}, \mathcal{M}, \mathcal{C})$ be any one-time secure cipher scheme with $\mathcal{K} = \mathcal{M}$. Suppose Alice and Bob both know a key $K_1 \in \mathcal{K}$.

Now Alice encrypts a fresh random key K_2 with Enc to create a ciphertext C_1. She then encrypts M with Enc using this fresh random key K_2 to create a ciphertext C_2. She gives C_2 to Charlie and C_1 to Bob. Bob and Charlie have to work together in order to decrypt.

(a) (5 points) Describe what Bob and Charlie need to compute in order to decrypt M.

Solution. To decrypt the message M, Bob and Charlie has to do the following:

- Using the shared key K_1, Bob will decrypt the ciphertext C_1 to get the fresh key K_2:

$$K_2 = \mathsf{Dec}(K_1, C_1).$$

- Bob will then send K_2 to Charlie.
- Finally, using the key K_2 received from Bob, Charlie decrypts the ciphertext C_2 to recover the original msg:

$$M = \mathsf{Dec}(K_2, C_2).$$

(b) (25 points) Let us know formalize what Alice does. Let $\Sigma_{\text{new}} = (\mathsf{Enc}_{\text{new}}, \mathsf{Dec}_{\text{new}}, \mathcal{K}_{\text{new}}, \mathcal{M}, \mathcal{C}_{\text{new}})$ have key space $\mathcal{K}_{\text{new}} = \mathcal{K} \times \mathcal{K}$, the same message space, and ciphertext space $\mathcal{C}_{\text{new}} = \mathcal{C} \times \mathcal{C}$, defined as follows: $\mathsf{Enc}_{\text{new}}((K_1, K_2), M) = (\mathsf{Enc}(K_1, K_2), \mathsf{Enc}(K_2, M))$. Prove that $\mathsf{Enc}_{\text{new}}$ has one-time secrecy. You do not need to use anything beyond in Chapter 1 of the textbook and some probability theory.

Solution. I'm essentially trying to prove how for any two msgs $m_0, m_1 \in \mathcal{M}$, the distributions of:

$$\mathsf{Enc}_{\text{new}}((K_1, K_2), m_0) \quad \text{and} \quad \mathsf{Enc}_{\text{new}}((K_1, K_2), m_1)$$

are identical when (K_1, K_2) is uniformly chosen from $\mathcal{K} \times \mathcal{K}$.

Let $\Sigma = (\mathsf{Enc}, \mathsf{Dec}, \mathcal{K}, \mathcal{M}, \mathcal{C})$ be a OTS cipher. By its definition, for any two msgs $x, x' \in \mathcal{M}$, the distributions of $\mathsf{Enc}(K, x)$ and $\mathsf{Enc}(K, x')$ are the same when K is uniform over $\mathcal{K}$ We can denote this common distribution by D, and thus for any fixed $x \in \mathcal{M}$ and any $c \in \mathcal{C}$,

$$\Pr[\mathsf{Enc}(K, x) = c] = \mathcal{D}(c),$$

where the probability is taken over $K \leftarrow \mathcal{K}$.

We can now Fix an arbitrary message $m \in \mathcal{M}$. The algorithm $\mathsf{Enc}_{\text{new}}$ will output (C_1, C_2), where

$$C_1 = \mathsf{Enc}(K_1, K_2), \qquad C_2 = \mathsf{Enc}(K_2, m).$$

We now compute the joint distribution of (C_1, C_2) when $(K_1, K_2) \leftarrow \mathcal{K} \times \mathcal{K}$. For any fixed $c_1, c_2 \in \mathcal{C}$,

$$\begin{aligned}
&\Pr[(C_1, C_2) = (c_1, c_2)] \\
&= \sum_{k \in \mathcal{K}} \Pr[K_2 = k] \cdot \Pr[C_1 = c_1, C_2 = c_2 \mid K_2 = k] \\
&= \sum_{k \in \mathcal{K}} \frac{1}{|\mathcal{K}|} \cdot \Pr[\mathsf{Enc}(K_1, k) = c_1 \text{ and } \mathsf{Enc}(k, m) = c_2 \mid K_2 = k].
\end{aligned}$$

Given that $K_2 = k$, K_1 is still uniform over $\mathcal{K}$ and independent of k. Moreover, Enc is deterministic, so $\mathsf{Enc}(k, m)$ is a fixed value. Hence,

$$\Pr[\mathsf{Enc}(K_1, k) = c_1 \text{ and } \mathsf{Enc}(k, m) = c_2 \mid K_2 = k] = \begin{cases} \Pr[\mathsf{Enc}(K_1, k) = c_1] & \text{if } \mathsf{Enc}(k, m) = c_2, \\ 0 & \text{otherwise.} \end{cases}$$

By the OTS of Σ, $\Pr[\mathsf{Enc}(K_1, k) = c_1] = \mathcal{D}(c_1)$ for every $k \in \mathcal{K}$. Therefore, the last equality follows because $Pr[Enc(K_2, m) = c_2] = \mathcal{D}(c_2)$ by OTS.

Thus, the distribution of (C_1, C_2) is the product distribution $D \times D$ which does not depend on the msg m. Consequently, this means that for any two msgs $m_0, m_1 \in M$, the distributions of $Enc_{new}((K_1, K_2), m_0)$ and $Enc_{new}((K_1, K_2), m_1)$ are identical. This proves that Enc_{new} has OTS.