

Homework 2
COMP543 Fall 2020 - Modern Cryptography
Erhan Tezcan 0070881
15.10.2020

1. QUESTIONS

Q1: What does it mean to be secure against an unbounded adversary? Alternatively, what do you understand when one says perfect secrecy? Does what you understand match what the one time pad provides? Why or why not?

A1: Being secure against an unbounded adversary means that the algorithm is secure against an adversary that has infinite computational power and unlimited time. This security is also known as “unconditional security”. Perfect secrecy is when the chances of guessing the message apriori is **perfectly** equal to the aposteriori probability. The emphasis on perfect here is due to the mathematical equivalence being without a margin of error. Even with the unlimited powers of the adversary, the fact that plaintext remains secret makes it sensible to use the word perfect too. OTP (One Time Pad) provides this, albeit it’s drawbacks. In fact, in a private key scheme with perfect requirements, OTP is the optimal perfectly-secret scheme, also proven by Shannon’s theory: $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$.

Q2: What are some advantages and disadvantages of the one time pad? Why don’t we use one time pad everywhere? Why do we need more research on cryptography?

A2: One Time Pad has several drawbacks. The immediately obvious one is the requirement of key length being at least equal to the message length. This is especially cumbersome if the message size is unbounded (not known apriori), and thus if parties decide to use a key they immediately bound their message length, which is not practical. Another case is the fact that this key is used only once -hence One Time-, as using a key more than once breaks perfect secrecy. Another problem is when the adversary is an “active attacker”, i.e. the adversary can change the content of ciphertext. The receiver will be unable to obtain exactly the encrypted message in that case. Note that One Time Pad is a perfect cipher. Almost never in real life can we have a representation of perfect. A scheme that can be broken with probability 1 if the adversary works to break it in 500 years, is actually pretty secure! The

further research in cryptography therefore approach this problem in terms of “asymptotic” or “concrete” security. Shannon already proved what is there to be proven regarding perfect schemes, and it was bad news for everyone.

Q3: Given any message m and a ciphertext c , how many one time pad keys provide $E_k(m) = c$? Explain your answer.

A3: In One Time Pad, we have $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$. When we fix for some message m and ciphertext c , we can say $\exists k \in \mathcal{K}$ s.t. $k = Dec_k(c) = m$. Since OTP is perfectly secret, thus correct:

$$Dec_k(Enc_k(m)) = m$$

We see that there is only 1 key that can provide this. If more than one key could provide this correctness for a fixed message, the general correctness would be broken.

Q4: For the following encryption scheme, state whether the scheme is perfectly secret or not. Justify your answer.

- The message space is $\mathcal{M} = \{0, \dots, 4\}$. Algorithm Gen chooses a uniformly random key from the key space $\{0, \dots, 5\}$. $Enc_k(m)$ returns $[(k + m) \bmod 5]$, and $Dec_k(c)$ returns $[(c - k) \bmod 5]$.

A4: This scheme is not perfectly secret.

Proof. Assume this scheme is perfectly secret. Fix a ciphertext c . Given $k_1 = 0$ and $k_2 = 5$, there exists a message m such that $c = Enc_{k_1}(m) = Enc_{k_2}(m)$. Let there be another message $m' = m + 1 \bmod |\mathcal{M}| = (m + 1) \bmod 5$. Let there be keys k'_1 and k'_2 such that $Enc_{k'_1}(m) = Enc_{k'_2}(m) = c$, which was our fixed ciphertext. To ensure this, we must compensate the plus 1 by decrementing the keys: $k'_1 = k_1 - 1$ and $k'_2 = k_2 - 1$. We get $k'_1 = 1 - 1 \bmod 6 = 5$, and $k'_2 = 5 - 1 \bmod 6 = 4$. Looking at the encryption function we see that:

$$Enc_{k'_1}(m') = [(5 + m') \bmod 5] \neq Enc_{k'_2}(m') = [(4 + m') \bmod 5]$$

As a result: $Pr[C = c | M = m] \neq Pr[C = c | M = m']$, which breaks perfect indistinguishability, and therefore the perfect secrecy. \square

Q5: For the following encryption scheme, state whether the scheme is perfectly secret or not. Justify your answer.

- The message space is $M = \{m \in \{0, 1\}^\lambda \mid \text{the last bit of } m \text{ is } 0\}$. Gen chooses a uniform key from $\{0, 1\}^{\lambda-1}$. $Enc_k(m)$ returns the

ciphertext as $[m \oplus (k||0)]$, and $Dec_k(c)$ returns the plaintext as $[c \oplus (k||0)]$.

A5: (Here $s_1||s_2$ denotes a concatenation of strings, see “Index of Common Notation”.) Our message space can be thought of $M' = \{m \in \{0,1\}^{\lambda-1} \text{ where every message } m = m'||0 \text{ and } m' \in M'\}$. So informally, a message of length $\lambda - 1$ ending with the bit 0. Our keys are also of $\lambda - 1$ randomly, and concatenated with 0. The *Enc* and *Dec* functions are in essence the same of One Time Pad, so actually this is just One Time Pad with the message and key ending in 0. As a result, this is perfectly secret.

Q6: Using OTP, Alice and Bob agreed on a perfectly random key, and that Alice will send Bob the answer to the question : “Are you taking Comp443/543” as either Y or N encoded using string-to-bits:

$$Y \rightarrow 1011001$$

$$N \rightarrow 1001110$$

Charlie knows nothing about the message or the key but intercepts the transmission: 1001110.

What should Charlie send to Bob so that Bob thinks the opposite of Alice’s answer? (If Alice indeed sent Y, Bob receives N. If Alice indeed sent N, Bob receives Y.)

A6: The adversary is defined to know the scheme and that $|\mathcal{M}| = \{Y, N\}$. The intercepted transmission is a ciphertext $c = k \oplus m_c$ where $k \in \mathcal{K}, m_c \in \mathcal{M}$. Let us represent the message space as $\mathcal{M} = \{m, m'\}$ without necessarily forcing any of these to equal Y or N. The adversary should do as follows:

$$tmp_1 = c \oplus m \text{ and } tmp_2 = c \oplus m'$$

$$tmp_1 = k \oplus m_c \oplus m \text{ and } tmp_2 = k \oplus m_c \oplus m'$$

Let us assume without loss of generality, that $m_c = m$.

$$tmp_1 = k \oplus m \oplus m \text{ and } tmp_2 = k \oplus m \oplus m'$$

$$tmp_1 = k \text{ and } tmp_2 = k \oplus m \oplus m'$$

At this point, the adversary knows that one of these hold the key, to find out which:

$$c_{tmp_1, m} = tmp_1 \oplus m$$

$$c_{tmp_1, m'} = tmp_1 \oplus m'$$

$$c_{tmp_2, m} = tmp_2 \oplus m$$

$$c_{tmp_2, m'} = tmp_2 \oplus m'$$

The adversary will then compare these 4 results to find the one that equals to c . Again, without loss of generality, let us say $c_{tmp_1, m} = c$. Then, the adversary can infer that the key is tmp_1 and Alice sent the message m . So, the adversary can create a new ciphertext by using the same key but the other message: $c' = Enc_k(m')$. This c' should hold the opposite information. The adversary will forward c' to Bob, and the mission will be complete!

2. EXERCISES

E1¹: Prove that, by redefining the key space, we may assume that the keygeneration algorithm Gen chooses a key uniformly at random from the key space, without changing $Pr[C = c|M = m]$ for any m, c .

A1:

E2²: Prove that, by redefining the key space, we may assume that Enc is deterministic without changing $Pr[C = c|M = m]$ for any m, c .

A2:

E3³: Prove or refute: An encryption scheme with message space \mathcal{M} is perfectly secret if and only if for every probability distribution over \mathcal{M} and every $c_0, c_1 \in \mathcal{C}$ we have $Pr[C = c_0] = Pr[C = c_1]$.

A3:

E4⁴: Prove Lemma 2.6. “Encryption scheme Π is perfectly secret if and only if it is perfectly indistinguishable.”

A4:

E5⁵: Same as **Q4** and **Q5**.

A5: Same as **Q4** and **Q5**.

E6⁶: When using the one-time pad with the key $k = 0^l$, we have $Enc_k(m) = k \oplus m = m$ and the message is sent in the clear! It has therefore been suggested to modify the one-time pad by only encrypting

¹KL Ed.2 Ch.2 Exc. 2.1

²KL Ed.2 Ch.2 Exc. 2.2

³KL Ed.2 Ch.2 Exc. 2.3

⁴KL Ed.2 Ch.2 Exc. 2.5

⁵KL Ed.2 Ch.2 Exc. 2.6

⁶KL Ed.2 Ch.2 Exc. 2.7

with $k \neq 0^l$ (i.e., to have Gen choose k uniformly from the set of nonzero keys of length l). Is this modified scheme still perfectly secret? Explain.

A6:

E7⁷: Let Π denote the Vigenere cipher where the message space consists of all 3-character strings (over the English alphabet), and the key is generated by first choosing the period t uniformly from $\{1, 2, 3\}$ and then letting the key be a uniform string of length t .

- a Define \mathcal{A} as follows: \mathcal{A} outputs $m_0 = \text{aab}$ and $m_1 = \text{abb}$. When given a ciphertext c , it outputs 0 if the first character of c is the same as the second character of c , and outputs 1 otherwise. Compute $\Pr[\text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}} = 1]$.
- b Construct and analyze an adversary \mathcal{A} for which $\Pr[\text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}} = 1]$ is greater than your answer from part (a).

A7:

E8⁸: In this exercise, we look at different conditions under which the shift, mono-alphabetic substitution, and Vigenere ciphers are perfectly secret:

- a Prove that if only a single character is encrypted, then the shift cipher is perfectly secret.
- b What is the largest message space \mathcal{M} for which the mono-alphabetic substitution cipher provides perfect secrecy?
- c Prove that the Vigenere cipher using (fixed) period t is perfectly secret when used to encrypt messages of length t .

A8:

E9⁹: Prove that a scheme satisfying Definition 2.5 must have $|K| \geq |M|$ without using Lemma 2.4. Specifically, let Π be an arbitrary encryption scheme with $|K| < |M|$. Show an \mathcal{A} for which $\Pr[\text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}} = 1] > \frac{1}{2}$.

Hint: *It may be easier to let \mathcal{A} be randomized.*

A9:

⁷KL Ed.2 Ch.2 Exc. 2.8

⁸KL Ed.2 Ch.2 Exc. 2.9

⁹KL Ed.2 Ch.2 Exc. 2.10

E10¹⁰: Assume we require only that an encryption scheme (Gen, Enc, Dec) with message space \mathcal{M} satisfy the following: For all $m \in \mathcal{M}$, we have $\Pr[Dec_K(Enc_K(m)) = m] \geq 2^{-t}$. (This probability is taken over choice of the key as well as any randomness used during encryption.) Show that perfect secrecy can be achieved with $|\mathcal{K}| < |\mathcal{M}|$ when $t \geq 1$. Prove a lower bound on the size of \mathcal{K} in terms of t .

A10:

E11¹¹: Let $\epsilon \geq 0$ be a constant. Say an encryption scheme is ϵ -perfectly secret if for every adversary \mathcal{A} it holds that:

$$\Pr[PrivK_{\mathcal{A}, \Pi}^{eav} = 1] \leq \frac{1}{2} + \epsilon$$

(Compare to Definition 2.5.) Show that ϵ -perfect secrecy can be achieved with $|\mathcal{K}| < |\mathcal{M}|$ when $\epsilon > 0$. Prove a lower bound on the size of \mathcal{K} in terms of ϵ .

A11:

E12¹²: In this problem we consider definitions of perfect secrecy for the encryption of two messages (using the same key). Here we consider distributions over pairs of messages from the message space \mathcal{M} ; we let M_1, M_2 be random variables denoting the first and second message, respectively. (We stress that these random variables are not assumed to be independent.) We generate a (single) key k , sample a pair of messages (m_1, m_2) according to the given distribution, and then compute ciphertexts $c_1 \leftarrow Enc_k(m_1)$ and $c_2 \leftarrow Enc_k(m_2)$; this induces a distribution over pairs of ciphertexts and we let C_1, C_2 be the corresponding random variables.

- a Say encryption scheme (Gen, Enc, Dec) is perfectly secret for two messages if for all distributions over $\mathcal{M} \times \mathcal{M}$, all $m_1, m_2 \in \mathcal{M}$, and all ciphertexts $c_1, c_2 \in \mathcal{C}$ with $\Pr[C_1 = c_1 \wedge C_2 = c_2] > 0$:

$$\Pr[M_1 = m_1 \wedge M_2 = m_2 | C_1 = c_1 \wedge C_2 = c_2] = \Pr[M_1 = m_1 \wedge M_2 = m_2].$$

Prove that no encryption scheme can satisfy this definition.

- b Say encryption scheme (Gen, Enc, Dec) is perfectly secret for two distinct messages if for all distributions over $\mathcal{M} \times \mathcal{M}$ where the first and second messages are guaranteed to be different (i.e.,

¹⁰KL Ed.2 Ch.2 Exc. 2.11

¹¹KL Ed.2 Ch.2 Exc. 2.12

¹²KL Ed.2 Ch.2 Exc. 2.13

distributions over pairs of distinct messages), all $m_1, m_2 \in \mathcal{M}$,
and all ciphertexts $c_1, c_2 \in \mathcal{C}$ with $Pr[C_1 = c_1 \wedge C_2 = c_2] > 0$:

$$Pr[M_1 = m_1 \wedge M_2 = m_2 | C_1 = c_1 \wedge C_2 = c_2] = Pr[M_1 = m_1 \wedge M_2 = m_2].$$

Show an encryption scheme that provably satisfies this definition.

A12: