Applied Cryptography

Ivan Valentini
Telegram: @IvanV1337
Github: https://github.com/IvanValentini/XXX

October 4, 2022

Contents

1 Introduction to Cryptography **2**
1.1 Introduction . . . 2
1.2 Attacks . . . 3
1.2.1 Ciphertext-only attackers (COA) . . . 3
1.2.2 Known-plaintext attackers (KPA) . . . 4
1.2.3 Chosen-plaintext attackers (CPA) . . . 4
1.2.4 Chosen-ciphertext attackers (CCA) . . . 4
1.3 Shannon Theorem . . . 5
1.3.1 Consequences of Shannon Theorem . . . 6

Chapter 1

Introduction to Cryptography

1.1 Introduction

Cryptography refers to hidden writing. Its goal is to enable a secure communication between two users (Alice and Bob), and making it impossible for an eavesdropper to understand the information being exchanged.

By channel we mean any physical or logical medium of communication from one user to another. A channel becomes secure when the information exchanged over it cannot be overheard or tampered with by eavesdroppers. By default a channel is considered insecure, so the intent of cryptography is to make secure, an insecure channel.

To transmit data in a secure way Alice and Bob rather than transmitting the message in a plain form they first covert it to a disguised form. Formally these are called plaintext ($\mathcal{P}$) and ciphertext ($\mathcal{C}$). The idea is to transform a plaintext into a ciphertext, so that Alice sends the latter to Bob, and Bob is able to reconstruct the plaintext from the received ciphertext while this is very difficult (almost impossible) for Eve.

In practice there is a pair of functions:

- $enc : \mathcal{P} \to \mathcal{C}$
- $dec : \mathcal{C} \to \mathcal{P}$

Such that $dec(enc(m)) = m$ for every $m \in \mathcal{P}$. For this to work Alice and Bob need to agree on what encryption and decryption scheme to use without disclosing it to Eve. Eve will only be able to observe ciphertexts, but notice that if the sets of plaintexts and ciphertexts are too small, then Eve

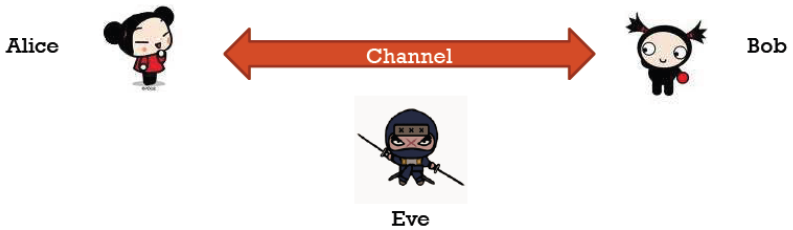

Figure 1.1

can try all the plaintext-ciphertext pairs (exhaustive search) or even if the sets of plaintexts and ciphertexts are large enough to make exhaustive search impractical, encryption and decryption can be defined in obvious way to allow Eve to easily reconstruct them (guessing). There is a problem with this formalization: these two functions, must be kept secret. These function can be used to create a secure channel, but how do you share these function? We need a secure channel, but if we had a secure channel, why not use it in the first place?

Since otherwise we would have to define and encryption and decryption functions for each pair of people that want to communicate securely we introduce the concept of a cryptographic key. We denote the set of (cryptographic) keys with $\mathcal{K}$, and consider a map $\varphi : \mathcal{P} \times \mathcal{K} \to \mathcal{C}$ such that for every key $k \in \mathcal{K}$ the function $\varphi(\cdot, k) : \mathcal{P} \to \mathcal{C}$ is an encryption function.

There are some key differences with respect to the old functions:

- The definition of φ (encryption algorithm) can be very complex but it can be public(i.e. known to anyone) and Alice and Bob can agree on it over an insecure channel. Before the encryption algorithm had to be private.
- The only component that must be kept secret(and thus exchanged over a secure channel) is the cryptographic key k, that defines the encryption function to use

The Kerchkhoff principle states that a cryptosystem should be secure even if everything about the system, except the key, is public knowledge. The advantages to only exchanging cryptographic keys rather than ciphers are that it is easier to keep secret k than φ, and if the key is discovered it is sufficient to choose another key. The main disadvantage is that the attacker only needs to find the key to break the system.

1.2 Attacks

Let's now consider some useful attack models expressed in terms of what the attacker can observe and what queries they can make to the cipher. A query for our purposes is the operation that sends an input value to some function and gets the output in return, without exposing the details of that function. An encryption query, for example, takes a plaintext and returns a corresponding ciphertext, without revealing the secret key. We call these models black-box models, because the attacker only sees what goes in and out of the cipher. There are several different black-box attack models. Note that the higher the attacker skills and complexity of the attack the less (computational) effort the attacker needs to put to break the system.

1.2.1 Ciphertext-only attackers (COA)

Ciphertext-only attackers (COA), or known-ciphertext attackers, observe ciphertexts but don't know the associated plaintexts, and don't know how the plaintexts were selected. Attackers in the COA model are passive and can't perform encryption or decryption queries.The task of the attacker is very difficult and a lot of computational power is required to mount such an attack, this is because the attacker needs to check for every possibile key of if the decrypted ciphertext is meaningful.

In some cases the attacker only needs to know the probability distribution of the plaintexts, it could obtain a lot of information merely by observing some ciphertexts. This holds under the assumption that all plaintexts are encrypted with the same cipher and the same key. The method may be difficult (if possible at all) to apply to short messages or messages that contain words with many occurrences of letters with low frequencies. More information can be found here.

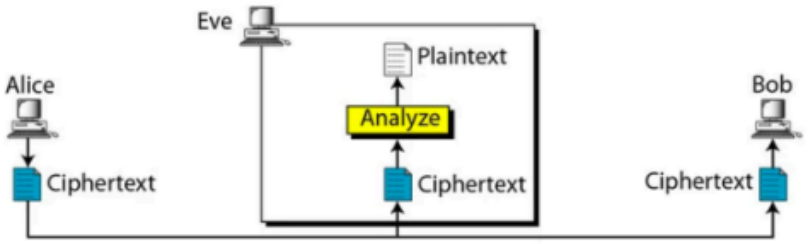

Figure 1.2

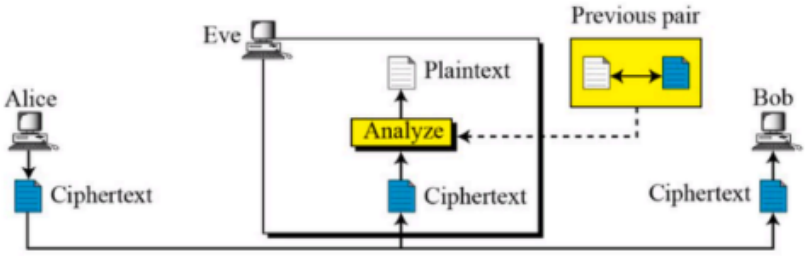

Figure 1.3

1.2.2 Known-plaintext attackers (KPA)

Known-plaintext attackers (KPA) observe ciphertexts and do know the associated plaintexts. Attackers in the KPA model thus get a list of plaintext–ciphertext pairs, where plaintexts are assumed to be randomly selected. Again, KPA is a passive attacker model, thus the attacker can not choose a plaintext to encrypt.

Essentialy the attacker will attempt to do what is known as a key recovery attack. But recovering the key might be a difficult problem to solve, so Eve might try to discover a functionally equivalent algorithm for encryption and decryption, or else design cryptographic algorithm that, even without knowing the key k, produces the same result as those of the cipher with the key k§This kind of attacks are known as Global Deduction/Reconstruction attacks.

1.2.3 Chosen-plaintext attackers (CPA)

Chosen-plaintext attackers (CPA) can perform encryption queries for plaintexts of their choice and observe the resulting ciphertexts. This model captures situations where attackers can choose all or part of the plaintexts that are encrypted and then get to see the ciphertexts. Unlike COA or KPA, which are passive models, CPA are active attackers, because they influence the encryption processes rather than passively eavesdropping.

With this the attacker may try to guess previously unknown plaintext-ciphertext pairs

1.2.4 Chosen-ciphertext attackers (CCA)

Chosen-ciphertext attackers (CCA) can both encrypt and decrypt; that is, they get to perform encryption queries and decryption queries. The CCA model may sound ludicrous at first—if you can decrypt, what else do you need?—but like the CPA model, it aims to represent situations where

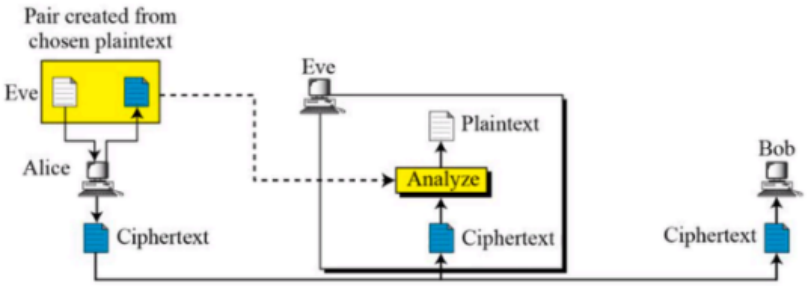

Figure 1.4

attackers can have some influence on the ciphertext and later get access to the plaintext. Moreover, decrypting something is not always enough to break a system.

1.3 Shannon Theorem

A cipher is broken if a method of determining the plaintext from the ciphertext is found without being legitimately given the decryption key. Any cryptosystem can be broken by an exhaustive key search. There exist ciphers that cannot be broken that are called perfect, and even exhaustive key search is of limited use for these ciphers. A cipher is perfect if, after seeing the ciphertext, an attacker gets no extra information about the plaintext other than what was known before the ciphertext was observed. The attacker might know the kind of content hidden but not the content itself, the point is that the knowledge of the attacker about the plaintext is not increased after intercepting the ciphertext .

Clever boy assumption states that plaintext and the keys are indipendent. So we do not select a particular key for a particular plaintext, for any plaintext we can choose any key.

$$\forall m \in \mathcal{P}, \forall k \in \mathcal{K} : P(mk) = P(m) \cdot P(k)$$

In other words Alice and Bob choice of the cryptographic key is made independently from the messages that they intend to transmit. More formally assume that Eve can just intercept ciphertexts. We are interested in the conditional probability that the plaintext m is sent, given that the ciphertext c is received. We would like to have ciphers for which Eve cannot derive additional knowledge about a plaintext after intercepting a (single) given ciphertext even knowing the probability distribution of the plaintexts. A cipher is called *perfect* if

$$\forall m \in \mathcal{P} and \forall c \in \mathcal{C} \Longrightarrow P(m) = P(m|c)$$

So the probability of having the plaintext m is equal to the conditional probability of observing m over the channel once you have seen the ciphertext c. So seeing the ciphertext c does not add any knowledge about the plaintext message sent.

Let us fix an integer n. Assume that: keys, plaintext, ciphertext have all n bits. Assume also that the plaintexts and the keys are independent (Clever boy assumption) and any n-bit string may be either a key or a plaintext. Then φ is a perfect cipher if and only if both the following conditions hold:

1. the keys are perfectly random
2. for any pair $(m,c)$of plaintext-ciphertexts, there is one and only one key k such that $c = \varphi(m,k)$

1.3.1 Consequences of Shannon Theorem

If φ is a perfect cipher, then all ciphertexts have the same probability to be received. Even if Eve knows the probability distribution of the plaintexts, she observes is a perfectly random cipher. Hence Eve cannot recover any information on the sent message from the intercepted ciphertext. But we made a very big assumpion: this is true only if Eve can intercept **one** ciphertext. If Eve intercepts more ciphertexts encrypted with the same key, then the Shannon theorem no longer guarantees perfect secrecy. So in practical sense, a perfect cipher is not unbreakable, so a perfect cipher is not necessarily ideal, because every time we need to use a different key also the key has to be as large as a message transfered.