Network Security

Professor Gaurav S. Kasbekar
Department of Electrical Engineering
Indian Institute of Technology, Bombay

Week - 02

Lecture - 11

Principle of Cryptography: Part 1

Hello, recall that in the last lecture, we discussed the mathematical background for cryptography. In this lecture and the next few lectures, we will discuss the principles of cryptography. So, the context is that a sender of information, say Alice, wants to send some information to a receiver, Bob. Cryptography allows a sender to replace the original text, which is known as the plaintext, with its disguised or encrypted version, which is known as the ciphertext. So, this shows the transformation. The original information is, say, a PDF file, which is the plaintext.

And then, it is transformed to its disguised version, which is known as the ciphertext, and the ciphertext is sent over the communication channel from Alice to Bob. Now, Bob transforms the ciphertext back to the original plaintext and uses the plaintext. The advantage of this transformation from plaintext to ciphertext is that an intruder, say Trudy, who intercepts this message during transit from Alice to Bob, this intruder does not gain any useful information from the intercepted message. So, Trudy might intercept the message using a packet sniffer, but since the information has been disguised, Trudy is not able to gain any useful information from the collected message. Cryptography has been used since ancient times by spies, military personnel, diplomats, and so on.

So, cryptography has a number of applications. First, we focus on the use of cryptography for achieving confidentiality. That is, when Alice is communicating with Bob, an intruder, Trudy, should not be able to understand the information that is being communicated. That's confidentiality. So, first, we focus on the use of cryptography for achieving confidentiality. Later on, we'll see that cryptography is also an essential building block for achieving several other functions, such as authentication and message integrity.

Let's start with a very simple cipher, which is known as the Caesar cipher. It was used by the Roman general, Julius Caesar, to encrypt his messages. So, we discussed the English version of the Caesar cipher. Each letter in the plaintext is replaced with the letter, that is,

k letters later in the alphabet. And once we reach ‘z’, then we wrap around to the first alphabet, that is ‘a’.

So, k here is an integer; it might be, for example, 3 or 5 or whatever. As an example, if k = 3, then we replace ‘a’ with the letter that is 3 letters to the right, that is, ‘a’ is replaced with ‘d’, ‘b’ is replaced with the letter, that is, 3 letters to the right, that is, ‘e’, and so on and so forth. Once we reach ‘z’, then we wrap around. ‘z’ is replaced with the letter, that is, 3 letters to the right with wraparound, that is, a, b, c., so ‘z’ is replaced with ‘c’. As an example, suppose k = 23, which means the right shift of 23, since there are 26 letters; this is equivalent to a left shift of 3. Suppose the plaintext is this. It is replaced with the following ciphertext. This is the ciphertext.

And this is obtained as follows. For the first letter of the plaintext, that is T, we shifted 3 letters to the left, and the letter that is 3 letters to the left is Q, because QRST, so Q is the letter that is 3 letters to the left of T. Then, the next letter of the plaintext is H; we replace it with the letter that is 3 letters to the left, which is E, then E is replaced with B, and so on and so forth. So, this plaintext is replaced with this ciphertext. Now, if an intruder intercepts the message, then they will get this ciphertext. So, we can see that from this, this ciphertext will not make any sense to the intruder.

The original message was this, but this is a scrambled message; it does not make any sense to the intruder. That's the advantage of encryption. That is, the message is disguised. So, this is the original message, which contains information, but then it is disguised, and this information is sent. Now, the receiver has to get back the plaintext from the ciphertext.

So, that can be done by reversing the cipher, that is, shifting k letters to the left. We take each letter of the ciphertext and shift k letters to the left to get back the plaintext. So, that's what the receiver does. But the point is that the intruder may not know that the Caesar cipher is being used, and the intruder also may not know the value of k. So, that's why the intruder is not able to recover the plaintext from the ciphertext, but the receiver is able to recover the plaintext from the ciphertext. Now, suppose the interceptor knows that the Caesar cipher is used, but the value of k is unknown to the interceptor.

Then, how can the interceptor go about trying to break the cipher? The intruder needs to try out all possible 25 values of the shift k. So, the intruder might first try k = 1, and then see what is the plaintext the intruder gets. If k = 1, then tries k = 2, and so on and so forth, up to the point where the plaintext that is recovered makes sense. That is, it is a valid

plaintext. Then, the interceptor has guessed the value of k. At that point, the cipher has been broken.

So, to break this Caesar cipher, the interceptor only has to try out 25 possible values of k. One of them will be correct, and the interceptor can thus break the cipher. So, the Caesar cipher is highly insecure. It is not used in present-day communications. We'll see more sophisticated ciphers that are used. We now introduce some terminology.

So, again, consider the same scenario, where there is plaintext sent by Alice to Bob after encryption. The algorithm used to transform the plaintext into the ciphertext is called the encryption algorithm. So, the encryption algorithm is used at the sender's side. The plaintext is transformed to the ciphertext using the encryption algorithm. The algorithm used to transform the ciphertext into the plaintext is called the decryption algorithm.

That is done at the receiver. The ciphertext is transformed to the plaintext using the decryption algorithm. Now, in many cryptographic systems, including those used in the internet, the encryption and decryption algorithms are standardized and published, and they are available to everyone, including potential intruders. We'll see the reasons for this. So, since the encryption and decryption algorithms are well known, there must be some secret information, which the intruder Trudy doesn't have, and that prevents the intruder from decrypting the message.

This secret information is known as the key. It is only known to the sender and the receiver. The intruder doesn't know the key, and that is what prevents the intruder from decrypting the message. The key is a string of letters, numbers, or bits. For example, the key in the Caesar cipher is the shift value k. The sender and receiver know the shift value k, but the intruder doesn't know the shift value k. So, before communication, the sender and receiver must somehow agree on the key that they will use for communication.

And they have to keep it secret from any potential intruders. Now, we go back to this statement that we made that the encryption and decryption algorithms are standardized and published and only the key is secret. So, why are the encryption and decryption algorithms standardized? So, why not keep them secret as well? That would make it harder for the intruder to recover the plaintext.

So, there are a couple of reasons for this system where the encryption and decryption algorithms are standardized and published. So, one reason for this is that any user who wants to send some information after encryption to some receiver, if the encryption and

decryption algorithms are standardized and published, then they can use the published algorithms to do their encryption and decryption. So, one reason for this is that the encryption and decryption algorithms are well known, so they can be used by any users who might require them. So, legitimate users can use the algorithms since they are standardized and published. So, that's one reason for making the encryption and decryption algorithms standardized and published.

The other reason is that, since these are published algorithms, any security experts can analyze them, and they can find out if there are any security flaws in these algorithms and whether they can be broken by the intruder because of any loopholes. So, cryptographers and security researchers can study the algorithms and uncover any loopholes or flaws in them. If such flaws or loopholes are found, then the algorithms can be modified. So, publishing the algorithms has this advantage as well. So, for these reasons, the encryption and decryption algorithms are standardized and published, but only the keys are secret.

We use the following notation. Suppose Alice sends an encrypted message to Bob. Let K_A denote the key of Alice and K_B denote the key of Bob. If 'm' is the plaintext message, then we denote the ciphertext obtained by encrypting 'm' with K_A as $K_A(m)$. And the plaintext obtained by decrypting C using K_B is denoted by $K_B(C)$. So, in particular, note that if we start with the plaintext message 'm' and encrypt it with K_A and then apply the key K_B to it, then we get back the original message 'm'.

$K_A(m)$ is the ciphertext obtained by encrypting 'm' with K_A, and $K_B(K_A(m))$ is the plaintext obtained by decrypting $K_A(m)$ with K_B. So, we get back the original plaintext message 'm'. So, there are two types of cryptography. One is symmetric key cryptography, and the other is public key cryptography. In symmetric key cryptography, the keys of the sender and receiver are the same, that is, $K_A = K_B$, and this key is a secret, which is known only to the sender and receiver. No one else should know the secret key $K_A = K_B$.

An example is Caesar cipher, where the secret key is the shift value k. This key should be known only to the sender and receiver. If someone else comes to know the secret key, then they can easily recover the plaintext from the ciphertext. So, this is symmetric key cryptography, where, as the name suggests, it is symmetric key cryptography because the keys of the sender and receiver are the same. The other kind of cryptography is public key cryptography.

Here, the keys of the sender and receiver are different. That is, $K_A \neq K_B$. The sender's key is known as the public key, and the receiver's key is known as the private key. The public

key is used for encryption, and the private key is used for decryption. The public key, as the name suggests, is available to everyone.

For example, it might be included in a database similar to a telephone directory. But the receiver's key, known as the private key, again, as the name suggests, it is a secret, and it is only known to the receiver. So, for example, if Alice wants to send a secret message to Bob, then Alice first looks up Bob's public key from this database, such as a telephone directory. So, once Alice has obtained Bob's public key, she encrypts her plaintext message using the public key and generates a ciphertext, which is sent to Bob. Bob applies his private key to the ciphertext; he's able to recover the plaintext from the ciphertext.

So, in summary, the public key is used for encryption, and the private key is used for decryption. And the public key is well known too; it is not a secret. The public key is known to everyone, but the private key is secret and is only known to the receiver, Bob. That is, Bob's private key is only known to Bob, Alice's private key is only known to Alice, and so on. So, later on, we will discuss these types of cryptography in detail. We start with symmetric key cryptography, and then we will discuss public key cryptography.

We will now discuss a type of symmetric cipher called the monoalphabetic cipher. Recall that the Caesar cipher, which is symmetric key-based, is easy to break. The monoalphabetic cipher is a generalization of the Caesar cipher. The way the monoalphabetic cipher operates is as follows. It replaces each letter in the plaintext with another letter.

An example is shown in the figure below. In this figure, suppose the upper row has the plaintext letters, and the lower row has the corresponding ciphertext letters. For example, if the letter in the plaintext is ‘a’, it is replaced with ‘m’. If the letter in the plaintext is ‘b’, then it is replaced with ‘n’, and so on and so forth. So, notice that the ciphertext letters are a permutation of the alphabet, that is, the plaintext letters. So, this monoalphabetic cipher replaces each letter in the plaintext with another letter according to this table here.

And the substitute for a given letter is fixed throughout the message. For example, each time ‘a’ occurs in the plaintext message, it is replaced with ‘m’. Here is an example. Suppose the plaintext is ‘attack at noon’. Then, let us obtain the ciphertext. So, the ciphertext letter corresponding to the plaintext letter ‘a’ is ‘m’. We can see that from this table.

So, the ciphertext letter corresponding to the plaintext letter ‘a’ is ‘m’. So, we have replaced the first letter of the plaintext with ‘m’. Then, the next plaintext letter is ‘t’. The ciphertext

letter corresponding to ‘t’ is ‘u’. So, we replace ‘t’ with ‘u’. Then, the next letter is again ‘t’. So, again, we replace it with the same ciphertext letter, that is, ‘u’. Then, the next letter is ‘a’; we replace it with ‘m’. Then, the next letter is ‘c’. We can see from the table that it is to be replaced with ‘b’, which is the corresponding ciphertext letter, and so on and so forth. So, if we continue this process, then we see that the ciphertext is this. So, this is the monoalphabetic cipher. So, what's the key in the monoalphabetic cipher?

The key is the string of ciphertext letters for the 26 alphabets. This is to be kept secret. So, this is the key, which is to be kept secret in the monoalphabetic cipher. What is the number of possible keys? So, the number of possible keys is the number of permutations of the 26 alphabets, that is, 26!.

That comes out to be around 4×10^{26}. So, suppose an intruder who doesn’t know the key wants to break the cipher; then a brute force approach they might use is to try out all possible keys, but the number of possible keys is of the order of 10^{26}, so this is a very time-consuming process, so it’s difficult to break the monoalphabetic cipher by brute force. But, it’s possible to break this cipher efficiently by a process known as frequency analysis. The frequency analysis was discovered long ago in the first millennium, that is, around 700 AD or around that time. So, it was discovered by the Arabs, and we now discuss this process of frequency analysis briefly.

So, this table shows the frequencies of different letters in typical English text. The letter ‘e’ appears in 12.7% of the text, then ‘t’ appears in 9.1% of the text, and ‘a’ appears 8.2% of the time, and so on. So, we see that, as expected, ‘e’, ‘t’, ‘a’, and ‘o’, ‘i’, and so on, these appear very frequently in English text, whereas letters like ‘x’, ‘q’, and ‘z’ appear very rarely in English text. So, this fact is used to try to break the cipher. If the message, which is sent from the sender to the receiver, is sufficiently long, then the intruder can measure the frequencies of different letters in the ciphertext.

And this is used to form guesses. For example, if ‘p’ is the most frequent letter in the ciphertext, then assuming that the plaintext is similar to ordinary English text. So, hence, ‘p’, which is the most frequent letter in the ciphertext, is most probably the substitute for one of these frequently occurring letters, that is, either ‘e’, ‘t’, or ‘a’. Then, we first replace all occurrences of ‘p’ with ‘e’. If that doesn't work out, then we replace all occurrences of ‘p’ with ‘t’. If that also doesn't work out, then we replace all occurrences of ‘p’ with ‘a’. We also use the following fact. Several two or three-letter sequences of letters, for example, “in”, “it”, “the”, “ion”, “ing”, and so on, appear frequently in English text. This fact is used.

After some replacements of ciphertext letters with plaintext guesses have been made, then more guesses can often be made. Here's an example. Suppose after we have substituted for ‘e’ and ‘t’. Suppose the pattern “tke” appears frequently; then it means that ‘k’ is probably the substitute for ‘h’. So, this ‘k’ should be replaced with ‘h’ throughout. So, this is how it proceeds. So, after we have been able to replace a few letters of the ciphertext with the corresponding plaintext letters, then we start getting patterns; we start getting strings like these, from which other plaintext letters can also be guessed. And then we continue this process; we repeat this process, so we replace all occurrences of ‘k’ with ‘h’ in this example, and then after having replaced ‘k’ with ‘h’, we might be able to guess some more words, and so on.

So, we repeat this process. So, see this website for a complete example of the use of frequency analysis to transform a ciphertext message into a plaintext message. So, we have only provided an overview, but for details, you can see this example. So, this frequency analysis technique can be used to try to break a monoalphabetic cipher. It involves a lot of trial and error because we have to make guesses and then make some replacements of ciphertext to plaintext.

If that doesn't work out, then we try some other letters, and so on and so forth. So, it involves a lot of trial and error, but in several cases, we can break the cipher and guess the plaintext corresponding to some ciphertext. So, for these reasons, the monoalphabetic cipher is also not considered secure. Another type of symmetric key cipher is the polyalphabetic cipher. This uses multiple monoalphabetic ciphers.

Each letter in the plaintext is replaced with the corresponding letter from one of these ciphers. And which cipher is used depends on the position of the letter in the plaintext. An example will make this clearer. Suppose in the polyalphabetic cipher we use two monoalphabetic ciphers. The first monoalphabetic cipher is a Caesar cipher with $k = 5$, and the second one is a Caesar cipher with $k = 19$.

These two ciphers are shown in this figure here. We see that the first, the second row is a Caesar cipher with $k = 5$. So, for example, instead of ‘a’, we have the letter that is 5 letters to the right, that is ‘f’. Instead of ‘b’, we have ‘g’, and so on and so forth. Similarly, the third row is a Caesar cipher with $k = 19$. These two ciphers are used in the following repeating pattern: C_1, C_2, C_2, C_1, C_2.

So, suppose, for example, that the plaintext is ‘attack at noon’, then the ciphertext is obtained as follows. So, this is the plaintext. This is to be transformed by applying the

repeating pattern that is provided there: C_1, C_2, C_2, C_1, C_2. So, we transform ‘a’ using the cipher C_1. We transform this ‘t’ using the cipher C_2.

Then, we transform this ‘t’ using the cipher C_2. And then C_1, C_2. ‘a’ is transformed using C_1, and ‘c’ is transformed using C_2. Since it is a repeating pattern, we again repeat the same pattern. So, ‘k’ is transformed using C_1, then C_2, C_2, C_1, C_2, C_1, and so on and so forth.

So, to transform ‘a’, ‘a’ has to be transformed using the cipher C_1. So, we see from the table that instead of ‘a’, we should write ‘f’. Then, ‘t’ is to be replaced using the cipher C_2. So, instead of ‘t’, we have ‘m’. This ‘t’ is also to be transformed using the cipher C_2. So, we have ‘m’ again. Then, ‘a’ is to be transformed using the cipher C_1.

So, we get ‘f’. Then, ‘c’ is to be transformed using the cipher C_2, so we get ‘v’, and so on and so forth. So, we see that the cipher that is to be used for a particular letter depends on the repeating pattern. And the ciphertext letter depends on the position of the plaintext letter in the plaintext. So, the ciphertext in this example is this.

So, you can verify that this is indeed the ciphertext. Polyalphabetic cipher cannot be broken using frequency analysis, which we discussed on the previous slide. However, several polyalphabetic ciphers have been broken using other techniques. An example is, Vigenère cipher, which was considered secure for a long time, but then it was broken using cryptanalysis, which is more sophisticated than frequency analysis. So, for these reasons, many polyalphabetic ciphers have also been broken, and hence, they are not secure anymore.

We will continue our discussion of cryptography in the next lecture. Thank you.