1 Introduction

What is cryptography? Till the 1970’s, cryptography resembled an art, rather than a science, and it was concerned essentially just with the task of ’keeping messages secret’. Cryptography was a means to enable parties to maintain secrecy of the information they send to each other—even in the presence of an adversary. While providing data secrecy remains a central goal, the field of cryptography has grown vastly over the last three decades. It now encompasses much more than secret communication. It includes not only other goals of communication security, such as guaranteeing data integrity, data origin and authentication, and entity authentication, but many more fascinating goals. For example, it deals with the problems of electronic auctions, digital banking, and electronic elections.

As this radical change came about, the ’art’ of cryptography has been supplemented with a rich theory, which enables the rigorous study of cryptography as a science. In this course we shall focus on this science—modern cryptography.

Modern cryptography is a cornerstone of computer and communications security, with end products that are eminently practical. Its study touches on branches of mathematics that may have once been considered esoteric, and it brings together fields like number theory, computational complexity theory, and probability theory.

1.1 Cryptographic goals

Modern cryptography addresses a wide range of problems. The most basic and classical one is ensuring secrecy of communication across an insecure medium. To describe this, we first introduce two members of the cast of characters: The sender, Alice, and our receiver, Bob. Alice and Bob want to communicate with each other.

Ideally, we would like to imagine that our two parties, Alice and Bob, are provided with a dedicated, untappable, impenetrable pipe, into which Alice can whisper a message that only Bob will hear. Nobody else can look inside the pipe, or change what is in there. This pipe represents a perfect medium—available only to the sender and receiver, as though they were alone in the world. It is an “ideal” communication channel from the security point of view. See Fig.1.

Unfortunately, real life has no ideal channels to connect the pairs of parties that might like to communicate with each other. Instead, real parties communicate over public networks, like the Internet. The most basic goal of cryptography is to provide such parties with a means to imbue their communications with security properties akin to those provided by the ideal channel. We usually call the third member of our cast the adversary, Eve. An adversary models the source of all possible threats. We imagine the adversary as having access to the network and wanting to compromise the security of the parties’ communications in some way.

Not all aspects of an ideal channel can be emulated. Instead, cryptographers distill a few central security goals and try to achieve them.

- **Data secrecy**: Masking the content of a transmission so it is unintelligible to the adversary.
Figure 1: Basic settings

- **Data integrity**: Providing assurance of detection against the case that the message be modified on the way.

- **Data origin**: Ensuring that the receiver, upon receiving purported communication from the sender, be able to reliably verify that it really did originate with the sender (rather than from the adversary).

- **Entity authentication**: Ensuring that a party, upon establishing a connection with another entity, be able to reliably establish the identity of this other entity.

Cryptography has many other goals, some related to the ones above, some not. For example, it can be used for pseudorandom number generation, for exchanging key securely, for flipping a fair coin, and so on. In fact, cryptography is concerned with most problems that arise in the context of any distributed computation in the presence of internal or external attack.

### 1.2 Relations to other branches of IT security

- Information theory
- Security of communications
- Security of computation
- Authentication and authorization
- Trustworthy computing (trusted computing base)
- Trust management

### 2 Historic landscape

#### 2.1 Etymology

The word cryptography comes from the ancient Greek words κρυπτός γραφω meaning “hidden writing”. Until modern times, cryptography referred almost exclusively to encryption, which is the process of converting a message (the plaintext) into unintelligible gibberish (the ciphertext). Decryption is the reverse, and recovers the plaintext back from the unintelligible ciphertext. A cipher is a pair of algorithms, one for encryption, and one for decryption. The operation of a cipher is controlled both by a key—a piece of shared secret information, known only to the two communicants.
2.2 Classical ciphers

- **Transposition ciphers:** rearranges the order of letters in a message
  - **Scytale** (also transliterated as skytale)
    It is a tool used to ‘implement’ a transposition cipher. It consisted of a cylinder (the *scytale*) and a strip of paper (or leather, as in Fig. 2). This strip is wrapped around the cylinder at the certain angle, and the message is then written on the strip in direction longitudinal to the cylinder. The recipient uses a rod of the same diameter on which he wraps the paper at the same secret angle, which reveals the message. Such earliest form of ‘secret writing’ required little more than local pen and paper analogs. It also had the advantage of being fast and not prone to mistakes. Presumably, the ‘effectiveness’ of techniques similar to this in ancient time had quite a bit to do with the fact that most people were not able readers at those times. Essentially, what was sought was a kind of “shoulder browsing” security technique. Beyond that, it is clearly easily broken.

![Figure 2: A scytale](image)

- **Substitution ciphers:** systematically replace letters or groups of letters with other letters or groups of letters.
  - **Shift ciphers (Caesar cipher).**
    This is one of the simplest and most widely known enciphering techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by the letter down the alphabet that follows it by some fixed number of positions (the *shift*). The method is named after Julius Caesar, who used it to communicate with his generals, with a fixed shift of three positions. As illustrated in Fig.3), this process would replaced an ‘A’ by a ‘D’, a ‘B’ by a ‘E’, and so on. For example, the message *meet at dawn*, would be enciphered (ignoring spaces) as follows:

<table>
<thead>
<tr>
<th>Plain:</th>
<th>meetatatdawn</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cipher:</td>
<td>PHHWEWGEZQ</td>
</tr>
</tbody>
</table>

![Figure 3: Caesar cipher](image)
As in the case of the scytale, the goal of Caesar cipher was likely a form “shoulder browsing” resistance. Beyond that, the fixed shift creates clear troubles, as enciphering is a fixed method: there is no secret key. Thus anyone learning how Caesar cipher works would be able to decipher effortlessly. Even in the case where the shift is random, acting as a secret key $k \in [0, 25]$, cryptanalysis by exhaustive enumeration of the 26 possibilities is trivial. This is an example of brute-force attack, or exhaustive search.

Incidentally, many conventional operative systems include a command-line utility caesar that performs Caesar enciphering, or a close variant, rot-13, that performs shift enciphering with a fixed shift of -13.

- **The mono-alphabetic substitution cipher**

  The idea of the mono-alphabetic substitution cipher is to map each plaintext character to a different ciphertext character in an arbitrary manner. The mapping must be one-to-one in order to enable decryption. If we are working with the English alphabet, the size of the key space is $26! \approx 2^{88}$.

![Figure 4: The distribution of letters in a typical sample of English language text](image)

Large key space does not necessarily imply security, however. Indeed, it is trivial to attack the mono-alphabetic substitution cipher by utilizing statistical patterns of the English language as shown in Fig.4. (A similar attack is possible in the case of any other language.) By graphing the frequencies of the letters as they occur in the ciphertext, and by knowing the expected distribution of letters in the original language of the plaintext, the one-to-one correspondence is easily learned. This is known as frequency analysis. Such frequency analysis relies on two properties of the mono-alphabetic substitution cipher:

1. The mapping of each letter is fixed.
2. The probability distribution of individual letters in the English language (or any other language) is known.

- **The Vigenère (poly-alphabetic substitution) cipher**

  The Vigenère cipher works as a sort of ‘parallel composition’ of multiple shift ciphers. A secret word is chosen as the key, and then the plaintext is encrypted by “adding” (modulo 26) each plaintext character to the next character of the key, wrapping around in the key when necessary. For example, an encryption of the message **attack at dawn** using the key **sesame** would works as follows:
Plaintext: attackatdawn  
Key: SESAMESESAME  
Ciphertext: TYKBPTYWBJS

The idea behind the Vigenère cipher is to disguise plaintext letter frequencies, with the goal of interfering with a straightforward application of frequency analysis. The primary weakness is the repeated use of its key, as caused by the ‘wrapping around’ rule. If a cryptanalyst correctly guesses the key’s length, then the ciphertext can be treated as interwoven Caesar ciphers, which individually are easily broken.

3 Discussion

3.1 Kerckhoffs’ principle

In the late 19th century, Auguste Kerckhoffs investigate the use of ciphers for military purposes. In the process, he proposed several design principles to serve as ‘best practices’ in the ‘art’ of developing military ciphers. One of the most important of these principles (now known simply as Kerckhoffs’ principle) is the following:

*The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.*

In other words, in a well-designed encryption scheme, only the key shared by the communicating parties needs to be secret; there should be no secrecy in the algorithm.

Kerckhoffs’ principle is universally embraced by the cryptographic community. Among others, the advantages of an “open cryptographic design”, whereby algorithm specifications are made public, include:

- Published designs undergo public scrutiny, so that at the bugs and weakness are more likely to be discovered, which result in a stronger final design.
- It is better for security flaws to be revealed by “ethical hackers” rather than having these flaws be known only to malicious parties.
- If the security of the system relies on the secrecy of the algorithm, then reverse engineering of the code poses a serious threat to security. (Notice that demanding secrecy for the key poses much less of a problem from this perspective, since the key should not be part of the code, and would not be vulnerable to reverse engineering.)
- If the security of the system relies on the secrecy of the algorithm, then there is no protection against insider attacks, even after the breach is discovered and the insider is apprehended. With an open design, instead, it suffices to change the shared secret key.
- Public designs enable the establishment of standards.

3.2 Toward modern cryptography

Let us now look back to the particular examples described in Sec. 2.2, and ask: what are these people trying to do?

*Make it difficult for somebody to understand the message.*
So we need to elaborate on three things:

- **Difficulty.** We will see two approaches to formalizing the notion of ‘difficulty’: mathematical impossibility, and computational hardness.

- **Somebody.** Of course we are designing for communication in the presence of an attacker (or adversary). The important part is qualifying the capability that are assumed of the attacker. The more ‘powers’ we endow to the attacker, the stronger the definition, the more difficult it will be to achieve, the more useful it will be in applications.

  Important directions along which we will refine the idea of adversarial power are:
  
  - the amount of *computation* that the adversary is assumed to be able to perform while mounting her attack;
  - the *type of interaction* that the adversary is assumed to be able to engage in the context of the communication;
  - the additional *side/a-priori knowledge* that the adversary is assumed to have about the subject of the communication.

- **Understand the message.** Also in this case, we will look at two main ways the capture the notion of what it means for the attacker to ‘understand’ the message. Looking ahead, the first approach (the *information-theoretic* approach) will formalize knowledge in terms of probability distributions, whereas the second approach (the *computational indistinguishability* approach) will look at knowledge (or lack thereof) in terms the attacker’s (in)ability to distinguish between clearly distinct alternatives.

It is important to keep in mind that we the are several reasonable ways to model the attacker. Here are some basic types of attacks against encryption schemes, in order of severity:

- **Ciphertext-only attack:** The adversary just observes a ciphertext (or multiple ciphertexts) and attempts to determine the underlying plaintext (or plaintexts).

- **Known-plaintext attack:** The adversary learns one or more pairs of plaintexts/ciphertexts encrypted under the same key. The aim of the adversary is then to determine the plaintext that was encrypted in some other ciphertext (for which she does not know the corresponding plaintext).

- **Chosen-plaintext attack:** The adversary has the ability to obtain the encryption of plaintexts of her choice. It then attempts to determine the plaintext that was encrypted in some other ciphertext.

- **Chosen-ciphertext attack:** The adversary is even given the capability to obtain the decryption of ciphertexts of her choice. The adversary’s aim, once again, is to determine the plaintext that was encrypted in some other ciphertext (whose decryption the adversary is unable to obtain directly).

4 Modern cryptography

As the field of cryptography has advanced, the dividing lines for what is and what is not cryptography have become blurred. Cryptography today might be summed up as the study of techniques and applications that depend on the existence of difficult problems. Cryptanalysis is the study of how
to compromise (defeat) cryptographic mechanisms, and cryptology is the discipline of cryptography and cryptanalysis combined.

The modern cryptographic approach is characterized by its adherence to three basic principles: *Formulation of exact definitions; Reliance on precise assumptions; Rigorous proofs of security.* Our discussion in Sec. 3.2 was clearly inspired by the first principle, as it was geared towards stressing the importance of isolating and specifying precisely the defining traits of the task at hand. In the next few lectures, we will turn more formally to those aims, and define notions of data secrecy for the shared-key setting. The other two principles will then play a crucial role in assessing whether certain concrete construction achieves our formal definitions.

References

