One-time Pad

RSA Cryptosystem

Secure Communication

The Germans invented a rotor cipher machine Enigma and used it during the World War I

Enigma machine with four rotors (source: Wikipedia).

During the World War II, the allies led by Alan Turing built a computer that broke the Enigma codes. It tried all possible combinations of the rotors, and then tried to decipher the ciphertexts intercepted by the counterintelligence. If what was on the output was looking like English plaintext, that meant that the cipher was decoded. Otherwise, it looked like just a random sequence of bits.

After the World War, it became clear that to be a superpower, countries need to be able to launch and aim nuclear missiles, and also to defend against them. The US launched radars that try to detect unrecognized flying objects and alarm about the potential threat. This alarm went through one of the first computer networks to the control center where the top army officers could make some decisions and react quickly, thanks to the quick information flow through the computer networks. Then, the universities were the first who understood the potential of computer networks, and they appeared in the classrooms. Finally, thanks to various start-up companies, we got things that we cannot imagine our life today without: cash machines, money transfers, e-mail, online commerce, messengers. All these inventions rely on *secure communication*.

A typical setting in secure communication is the following. Two parties, traditionally called Alice and Bob, want to exchange some information. Alice and Bob are just placeholders for the parties that need to exchange some information: in practical applications, these could be a secret agent and a center, or a person and an online store, or two computers. There is also Eve who is stepping on the wire and listening to everything they say to each other. This does *not* depend on the channel of communication: if they are standing right next to each other, someone could be eavesdropping; if they are talking over the phone or Internet, somebody could be listening to the line. Thus, we assume that everything that Alice sends to Bob is known to Eve. The only thing they can keep in secret is something that they keep to themselves and do not tell to anyone.

Thus, Alice wishes to send a message to Bob through a public channel that is listened by Eve. Alice wants Bob to be able to read the message, but does not want Eve to understand anything. To achieve this, instead of sending the original message, called a *plaintext*, Alice somehow encodes her message and sends the resulting *ciphertext* to Bob. For this scheme to be secure, one needs to ensure that Bob can easily decode the ciphertext, whereas it is difficult for Eve to decode. Below, we discuss various ways to achieve this, called *ciphers*, and discuss their advantages and disadvantages.

✓ **Completed** **Go to next item**

Like **Dislike** **Report an issue**