Cryptography

Modern cryptography has developed the most during the World War I and World War II, because everybody was spying on everybody. We will tell this story and see why simple ciphers didn't work anymore. We will learn that shared secret key must be changed for every communication if one wants it to be secure. This is problematic when the demand for secure communication is skyrocketing, and the communicating parties can be on different continents. We will then discuss the famous RSA cryptosystem that allows parties to exchange secret keys such that no eavesdropper is able to decipher these secret keys in any reasonable time. After that, we will implement a few attacks against incorrectly implemented RSA!

Completed **Go to next item**

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