Seminar 6.4.2024

Solve in Cryptool (and also try it "by a hand" if you do not understand the cipher principle). Link for OS Windows version here https://www.cs.vsb.cz/ochodkova/courses/kpb/SetupCrypTool_1_4_30_en.exe It is possible to use also online version https://www.cryptool.org/en/cto/ . The software is also installed on computers here in the lab.

Write the all solutions in one document and submit via LMS (upload to LMS) as a **pdf file** by the end of seminar. Name the document with your login name and text "sem3"!). It is not a team task, you will each solve it separately.

1. **Substitution.** Encrypt and then decrypt the plaintext P below using a generalized Caesar cipher (Shift cipher) with a key K of 'X'. What is the ciphertext, when the alphabet is English alphabet without space (i.e. remove spaces)? (Cryptool - Encrypt/Decrypt – Symmetric (classic) – Caesar)
   P = THE ONRUSH OF A CONQUERING FORCE IS LIKE THE BURSTING OF PENT UP WATERS INTO A CHASM A THOUSAND FATHOMS DEEP

2. **Substitution.** Encrypt and then decrypt the plaintext P below using a general monoalphabetic substitution cipher with a given key K = "JULIUSCAESAR". What is the ciphertext, when the alphabet is English alphabet without space (i.e. remove spaces)?
   P = THE ONRUSH OF A CONQUERING FORCE IS LIKE THE BURSTING OF PENT UP WATERS INTO A CHASM A THOUSAND FATHOMS DEEP

3. **Substitution.** Encrypt and then decrypt the plaintext P below using a Playfair cipher with a given key K = "MONDAY". What is the ciphertext, when the alphabet is English alphabet without space (i.e. remove spaces)?
   P = THE ONRUSH OF A CONQUERING FORCE IS LIKE THE BURSTING OF PENT UP WATERS INTO A CHASM A THOUSAND FATHOMS DEEP

4. **Substitution.** Encrypt and then decrypt by a hand (i.e. manually) and then in Cryptool the plaintext P below using a Hill cipher with a given key matrix K = {{15, 20, 2}, {8, 17, 9}, {4, 1, 22}}. What is the ciphertext, when the alphabet is English alphabet without space (i.e. remove spaces)?
   P = CRYPTOGRAPHY

5. **Substitution.** Encrypt and decrypt by a hand (i.e. manually) and then in Cryptool, the text below using a Vigenère cipher with a key K of "KEY". What is the ciphertext, when the alphabet is English alphabet without space (i.e. remove spaces)?
   P = THIS TERMINAL IS NO MORE IT HAS CEASED TO BE ITS EXPIRED AND GONE TO MEET ITS MAKER THIS IS A LATE TERMINAL ITS A STIFF BEREFT OF LIFE IT RESTS IN PEACE IF YOU HADNT NAILED IT TO THE BENCH IT WOULD BE PUSHING UP THE DAISIES THIS IS AN XTERMINAL

6. **Product Cipher.** Encrypt and decrypt by a hand (i.e. manually) and then in Cryptool, the text below using an ADFGVX cipher with a substitution key K_S of "MONDAY" and transposition key K_T = (3,4,2,1)
   P = THIS TERMINAL IS NO MORE IT HAS CEASED TO BE ITS EXPIRED AND GONE TO MEET ITS MAKER THIS IS A LATE TERMINAL ITS A STIFF BEREFT OF LIFE IT RESTS IN PEACE IF YOU HADNT NAILED IT TO THE BENCH IT WOULD BE PUSHING UP THE DAISIES THIS IS AN XTERMINAL

7. **Transposition.** Encrypt and then decrypt the plaintext P below using a Rail Fence cipher a key K=5. What is the ciphertext, when the alphabet is English alphabet without space (i.e. remove spaces)?
   P = THE ONRUSH OF A CONQUERING FORCE IS LIKE THE BURSTING OF PENT UP WATERS INTO A

CHASM A THOUSAND FATHOMS DEEP

8. **Transposition.** Let A = {A, B, …, Y, Z} be the English alphabet (without space). Let P (the plaintext) and C (the ciphertext) be sets of all strings over A. The key K = (3 12 7 1 5 9 10 6 11 4 8 2) is chosen to be a permutation on A. Do it "by a hand, i.e. manually" and then in Cryptool.
    a) Encrypt an English message P=CRYPTOGRAPHY. What is the ciphertext?
    b) What way we can obtain a plaintext from the ciphertext from the previous step, i.e. how shall decryption proceed? What is the decryption key?