**Workshop – HistoCrypt 2018**

**(Automated) Cryptanalysis of Classical Ciphers with CrypTool 2**

Nils Kopal, Armin Krauss, and Bernhard Esslinger

2018-06-20



**Solutions**

**Task 1:**

In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence

**Task 2:**

Qksec Tevsec Mkockb uxygx li rsc myqxywox Tevsec Mkockb, gkc k Bywkx zyvsdsmskx kxn wsvsdkbi qoxobkv gry zvkion k mbsdsmkv byvo sx dro ofoxdc drkd von dy dro nowsco yp dro Bywkx Bozelvsm kxn dro bsco yp dro Bywkx Owzsbo. Ro sc kvcy uxygx kc kx kedryb yp Vkdsx zbyco.

**Task 3:**

In cryptography, a cipher is an algorithm for performing encryption or decryption - a series of well-defined steps that can be followed as a procedure. An alternative, less common term is encipherment. To encipher or encode is to convert information into cipher or code. In common parlance, "cipher" is synonymous with "code," as they are both a set of steps that encrypt a message; however, the concepts are distinct in cryptography, especially classical cryptography.

**Task 4:**

Substitution of single letters separately - simple substitution - can be demonstrated by writing out the alphabet in some order to represent the substitution. Uhis is termed a substitution alphabet. Uhe cipher alphabet may be shifted or reversed (creating the Maesar and Ktbash ciphers, respectively) or scrambled in a more complex fashion, in which case it is called a mixed alphabet or deranged alphabet. Uraditionally, mixed alphabets may be created by first writing out a keyword, removing repeated letters in it, then writing all the remaining letters in the alphabet in the usual order.

**Task 5:**

wLENJOWLcNVE OL aLENJOROWE UK JVY NLcaJUaY cPZ KJIZE OX JYaVPUMIYK XOL KYaILY aOQQIPUacJUOP UP JVY NLYKYPaY OX JVULZ NcLJUYK acRRYZ cZHYLKcLUYK.

**Task 6:**

WILLIAM FREDERICK FRIEDMAN WAS A US ARMY CRYPTOGRAPHER WHO RAN THE RESEARCH DIVISION OF THE ARMYS SIGNAL INTELLIGENCE SERVICE IN THE THIRTIES

**Task 7:**