The exercises serve two goals. Firstly, they are preparations for the KU examination. Secondly, they are meant as a help to understand the VO lectures. The **Method** is at least as important as the final result. Use the Student Tick System – `https://stics.iaik.tugraz.at/` to tick the tasks you solved before each class.

1 The Vernam Scheme

We are using the the Vernam scheme.

1. Decrypt the following ciphertext.

ciphertext	1|0|1|1|0|0|1|0|0|1|0|1|0|1|1|0|1|1|0|0
key	1|0|0|0|1|0|0|1|0|1|1|1|0|1|1|0|0|0|1|0
plaintext	| | | | | | | | | | | | | | | | | | | |

2. You are given a ciphertext of length n. What is the complexity of finding the correct plaintext without knowing the corresponding key?

3. Derive the relationship between plaintext and ciphertext for two encryptions with the same key. Is the Vernam cipher still secure if we use the same key twice?

2 Vigenère Cipher 1

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

We are using the the Vigenère cipher.

1. Encrypt the following plaintext: `noonecanreadthismessage` with the key `vigenere`.

2. Decrypt the following ciphertext: `LLCLWVZIUGPWLMQF` assuming the key used for encryption was `sec`.

3 Vigenère Cipher 2

We encrypt with double Vigenère using for the first encryption the key $k_1 =$ `cipher` and for the second encryption the key $k_2 =$ `key`

1. Encrypt the plaintext: `message`.

2. Show that this is equivalent to simple Vigenère encryption, and find the key for the single Vigenère encryption that is equivalent to double Vigenère encryption with the above keys k_1 and k_2.

4 Affine Ciphers

We used an affine cipher $c = a \cdot p + b \bmod 26$ for encryption, where c is the ciphertext, p is the plaintext, and (a, b) is the key.

1. Explain how decryption works. What can you say about the key (a, b)?
2. The key (19,7) was used for encryption. Give the decryption key and find the plaintext for the following ciphertext: `encmessage`.

5 Basic Cryptanalysis 1

In this example we will perform a known plaintext attack. This is an attack where the adversary knows a plaintext and the according ciphertext. The aim of the adversary is to find out which cipher and which key has been used for the encryption. Note that the adversary in general knows the used cipher (Kerckhoffs' principle).

plaintext: `myplaintext`
ciphertext: `OPNATWPKCMM`

1. Which cipher has been used for encryption (Transposition, Caesar, Vigenère)?
2. Determine the key used for encryption.
3. Verify your result for the following ciphertext: `AFSVHHVYCRHFTVAIDSA`.

6 Basic Cryptanalysis 2

Given the following ciphertext encrypted using the Vigenère cipher. Determine the key (use the method you have learned in the lecture). Hint: the period of the used key is 2.

MI|XA|BU|DO|VU|DC|YH|CS|YO|PI|EH|NN
RY|BC|QB|DJ|VU|SH|DY|HN|PI|BU|BY|VC
KV|VY|PL|OK|EY|XW|IU|XU|VS|CC|CQ|OH
OY|NU|PY|GG|YL|OQ|YL|NM