DHBW
Duale Hochschule
Baden-Württemberg
CAS
Center for Advanced Studies

IT-Security Cryptography and Secure Communications

Excercise: **Classical Encryption Techniques**
Lecturer: *Prof. Dr. Michael Eichberg*
Version: 2023-10-10

Playfair Cipher

Decrypt the ciphertext: `XGAWMGAZ`. The password is `MONARCHY` (as used in the slides.)

Vigenère Cipher

Let's assume that you got one plaintext / ciphertext pair.

P: `secret`
C: `HSFGSW`

1. Can you recover the key?
2. What type of attack were you able to perform?

Rail-fence Cipher

Encrypt the message: "i love crypto" with the key/depth 3.

Row Transposition Cipher

You received the following message:

YSFRITTUNCOSPJU

Additionally, you were able to extract the key except of one value: 4153.

1. How many possible decryptions are possible?
2. Can you decrypt the text?
3. What is the key?

Steganography

Uncover the text hiden in the spam message.