DHBW
Duale Hochschule
Baden-Württemberg
CAS
Center for Advanced Studies

# IT-Security Cryptography and Secure Communications

| | |
|---|---|
| **Exercise:** | **Classical Encryption Techniques** |
| **Lecturer:** | Prof. Dr. Michael Eichberg |
| **Version:** | 2023-10-27 |

## Playfair Cipher

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

### Solution

```
w(i/j)nXnerX => winner
```

## Vigenère Cipher

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

| | |
|---|---|
| **P:** | `secret` |
| **C:** | `HSFGSW` |

1. Can you recover the key?

   ### Solution

   The key is: PODPOD.

2. What type of attack were you able to perform?

   ### Solution

   A plaintext attack.

## Rail-fence Cipher

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

Solution

```
P = I L O V E C R Y P T O
    1 2 3 1 2 3 1 2 3 1 2

C = I V R T L E Y O O C P
```

## 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?

   Solution

   5: 24153, 42153, 41253, 41523, 41532

2. Can you decrypt the text?

   Solution

   We have five colums (len of key) and therefore three rows.

   Split up in 5 segments of three letter. YSF RIT TUN COS PJU

   Write them down in a table:

   ```
   y r t c p   => looks like "crypt"
   s i u o j
   f t n s u
   ```

   P = `crypto is just fun` (space added for readability.)

3. What is the key?

   Solution

   ```
   K = 42153
   ```

## Steganography

Uncover the text hiden in the spam message.

Solution

```
Success
```