|  |  |  |
| --- | --- | --- |
| **Zentralabitur 2024** | **Informatik** | **Material für Prüflinge** |
| **Block 2: Aufgabe A** | **gA** | **Prüfungszeit: 250 min** |

**Name:** **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Klasse:** **\_\_\_\_\_\_\_**

Inhaltsverzeichnis

[Aufgabe A (25 BE) 3](#_Toc162335682)

# Aufgabe A (25 BE)

Beim Verschlüsselungsverfahren Kolonne wird der zu verschlüsselnde Klartext in Blöcke zu je neun Zeichen unterteilt, die dann jeweils in 3x3-Quadraten zeilenweise angeordnet werden (siehe linkes Quadrat in Abbildung 1). Dabei werden nicht verwendete Stellen des letzten Quadrats mit dem Zeichen **X** aufgefüllt. Als Schlüssel wird eine Zahlenfolge aus 10 Ziffern verwendet. Mit jedem dieser Quadrate geschehen nun die folgenden zwei Prozesse, um die jeweiligen Ergebnisquadrate zu erhalten (siehe rechtes Quadrat in Abb. 1):

(I) Die 8 äußeren Zeichen jedes Quadrats werden entgegen dem Uhrzeigersinn um so viele Stellen weiterbewegt, wie die erste Ziffer des Schlüssels angibt.

(II) Die hinteren 9 Ziffern des Schlüssels werden zeilenweise in die Felder des Quadrats eingetragen. Jedes Zeichen des Quadrats wird nun um die angegebene Anzahl gemäß dem Caesar-Verfahren weitergeschoben.

Für jedes Ergebnisquadrat wird der Geheimtext zeilenweise ausgelesen.

#### Abbildung 1:

Beispiel für eine Verschlüsselung des Klartextes **GUTENTAG** mit dem Schlüssel **2725160298**.  
Es ergibt sich der Geheimtext **AVCVTGINI**.

|  |  |  |
| --- | --- | --- |
| **G** | **U** | **T** |
| **E** | **N** | **T** |
| **A** | **G** | **X** |

|  |  |  |
| --- | --- | --- |
| **T**  **7** | **T**  **2** | **X**  **5** |
| **U**  **1** | **N**  **6** | **G**  **0** |
| **G**  **2** | **E**  **9** | **A**  **8** |

|  |  |  |
| --- | --- | --- |
| **A** | **V** | **C** |
| **V** | **T** | **G** |
| **I** | **N** | **I** |

**2**

a) Verschlüsseln Sie den Klartext **HAUSSCHUH** mit dem Verfahren *Kolonne* mit dem Schlüssel **3586129418**. Verwenden Sie dazu die Abbildungen 2 und 3 im Material.  
**[3 BE]**

b) Entschlüsseln Sie den Geheimtext **DOUENAMYR** mit dem Verfahren *Kolonne* mit dem Schlüssel **5631795473**. Verwenden Sie dazu die Abbildungen 2 und 4.  
**[4 BE]**

c) c) Entscheiden Sie jeweils begründet für die Schritte (I) und (II), ob es sich um ein monoalphabetisches Substitutionsverfahren, ein polyalphabetisches Substitutionsverfahren oder ein Transpositionsverfahren handelt.  
**[3 BE]**

d) Untersuchen Sie, wie viele verschiedene Quadrate durch Schritt (I) entstehen können.  
**[3 BE]**

e) Begründen Sie, dass es sich beim Schritt (II) des Verfahrens *Kolonne* um eine spezielle Art des Vigenère-Verfahrens handelt.  
**[4 BE]**

f) Für einen mit dem Vigenère-Verfahren verschlüsselten deutschen Text ist bekannt, dass dieser mit einem Schlüssel der Länge 3 verschlüsselt wurde.

Erläutern Sie, inwiefern in diesem Fall Häufigkeitsanalysen eingesetzt werden können, um zu versuchen, den Klartext zu rekonstruieren.  
**[4 BE]**

Es wird eine Erweiterung des Verfahrens Kolonne angeboten: Im Verfahren KolonnePlus werden für jedes Quadrat des Klartextes die Schritte in der Reihenfolge (I)-(I)-(II)-(II) durchgeführt. Dabei bleibt der Schlüssel unverändert.

g) Beurteilen Sie, ob sich die Sicherheit des Verfahrens im Vergleich zum Verfahren *Kolonne* erhöht.  
**[4 BE]**

#### Gesamtergebnis

|  |  |  |
| --- | --- | --- |
| **Aufgabe A** | **Mögliche Punkte** | **Erreichte Punkte** |
| **a)** | **3 BE** |  |
| **b)** | **4 BE** |  |
| **c)** | **3 BE** |  |
| **d)** | **3 BE** |  |
| **e)** | **4 BE** |  |
| **f)** | **4 BE** |  |
| **g)** | **4 BE** |  |