Aufgabe A

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):

1. Die 8 äußeren Zeichen jedes Quadrats wandern entgegen dem Uhrzeigersinn um die Anzahl Stellen, die sich aus der ersten Ziffer des Schlüssels ergibt.
2. 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.

2

|  |  |  |
| --- | --- | --- |
| 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 |

Abbildung 1: Beispiel für eine Verschlüsselung des Klartextes GUTENTAG mit dem  
Schlüssel 2725160298. Es ergibt sich der Geheimtext AVCVTGINI.

1. Verschlüsseln Sie den Klartext HAUSSCHUH mit dem Verfahren *Kolonne* und dem Schlüssel 3586129418. Verwenden Sie dazu die Abbildungen 3 und 4 im Material. [3 BE]
2. Entschlüsseln Sie den Geheimtext DOUENAMYR mit dem Verfahren *Kolonne* und dem Schlüssel 5631795473. Verwenden Sie dazu die Abbildungen 3 und 5. [3 BE]
3. Untersuchen Sie, wie sich die falsche Übertragung eines Geheimtextzeichens auf die damit entschlüsselte Nachricht auswirkt. [2 BE]
4. Entscheiden Sie jeweils begründet für die Schritte (I) und (II), ob es sich um ein monoalphabetisches Substitutionsverfahren, ein polyalphabetisches Substitutionsverfahren oder ein Transpositionsverfahren handelt. [2 BE]
5. Untersuchen Sie, wie viele verschiedene Quadrate durch Schritt (I) entstehen können. [2 BE]
6. Vergleichen Sie Schritt (II) des Verfahrens *Kolonne* mit dem Vigenère-Verfahren. [4 BE]
7. Entwickeln Sie ein mögliches Vorgehen zum Angreifen des Verfahrens *Kolonne* bei einer ausreichend langen Nachricht in einer bekannten Sprache. [5 BE]

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

1. Beurteilen Sie, ob sich die Sicherheit des Verfahrens im Vergleich zum Verfahren *Kolonne* erhöht. [3 BE]

In einer anderen Erweiterung *KolonnePremium* wird für jedes Klartextquadrat der Schlüssel verändert. Dazu sind die Positionen der zehn Schlüsselziffern von 0 bis 9 durchnummeriert. Der Wert, den die vorderste Schlüsselziffer hat, bestimmt die Position, an der die nächste Schlüsselziffer zu finden ist, die nun ganz an den Anfang des Schlüssels gesetzt wird. Dadurch werden einige Schlüsselziffern eine Position nach rechts verschoben. Der so veränderte Schlüssel wird nun für das nächste Quadrat des Klartextes verwendet. In Abbildung 2 sind die ersten Schritte einer solchen Schlüsselveränderung angegeben.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Schlüsselposition | | | | | | | | | |  |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1. Klartextblock wird mit | 3 | 5 | 7 | 6 | 1 | 2 | 9 | 4 | 3 | 8 | verschlüsselt. |
| 2. Klartextblock wird mit | 6 | 3 | 5 | 7 | 1 | 2 | 9 | 4 | 3 | 8 | verschlüsselt. |
| 3. Klartextblock wird mit |  |  |  |  |  |  |  |  |  |  | verschlüsselt. |
| 4. Klartextblock wird mit |  |  |  |  |  |  |  |  |  |  | verschlüsselt. |
| 5. Klartextblock wird mit |  |  |  |  |  |  |  |  |  |  | verschlüsselt. |
| 6. Klartextblock wird mit |  |  |  |  |  |  |  |  |  |  | verschlüsselt. |
| 7. Klartextblock wird mit |  |  |  |  |  |  |  |  |  |  | verschlüsselt. |
| 8. Klartextblock wird mit |  |  |  |  |  |  |  |  |  |  | verschlüsselt. |
| … | … | … | … | … | … | … | … | … | … | … | … |

Abbildung 2: Schlüsselbildung für das Verfahren KolonnePremium

1. Ergänzen Sie in Abbildung 2 die nächsten 6 Schlüssel. [2 BE]
2. Begründen Sie, dass sich die Sicherheit des Verfahrens *KolonnePremium* gegenüber dem Verfahren *Kolonne* bei einer guten Wahl des ersten Schlüssels erhöht, dies bei einer ungünstigen Wahl des ersten Schlüssels aber nicht zutrifft. [4 BE]

Material

zu Aufgabenteilen a) – b)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Abbildung 3: Hilfsmittel zur Durchführung von Caesar-Verschlüsselungen

zu Aufgabenteil a)

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

Abbildung 4: Aus dem Klartext HAUSSCHUH ergibt sich mit dem Schlüssel 3586129418  
der Geheimtext \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

zu Aufgabenteil b)

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

Abbildung 5: Aus dem Geheimtext DOUENAMYR ergibt sich mit dem Schlüssel 5631795473  
der Klartext \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.