Aufgabe 2

Die ADFGVX-Verschlüsselung ist ein mehrstufiges Verschlüsselungsverfahren. In der ersten Stufe werden Buchstaben und Ziffern aus dem Klartext entsprechend einer Schlüsselmatrix ersetzt. Die Buchstaben am Rand der Schlüsselmatrix sind immer ADFGVX, die Buchstaben und Ziffern innerhalb der Matrix können beliebig angeordnet sein. Eine beispielhafte Schlüsselmatrix ist im Material in Abbildung 2.1 zu finden. Jedes Klartextzeichen im Inneren der Matrix wird durch die am Rand der Schlüsselmatrix stehenden Zeichenpaare ersetzt (zuerst Zeilen-, dann Spaltenbuchstabe). Leer- und Satzzeichen werden weggelassen.

Beispielsweise wird entsprechend der im Material gegebenen Schlüsselmatrix das Klartextzeichen S durch GA und das Klartextzeichen 1 durch VG ersetzt.

Damit wird der Klartext `KOMM UM 9 UHR` zum Geheimtext `DXFFAVAVGFAVXXGFAFFX`.

a) Ein Klartext lautet `13 UHR AM SEE`. Der Schlüssel ist die im Material gegebene Matrix (Abb. 2.1). Bestimmen Sie für diesen Klartext den Geheimtext der ersten Stufe der Verschlüsselung.

Nennen Sie die wesentlichen Eigenschaften von monoalphabetischen und polyalphabetischen Verschlüsselungsverfahren und entscheiden Sie, zu welcher dieser beiden Arten von Verfahren die erste Stufe der ADFGVX-Verschlüsselung gehört.

Vergleichen Sie dieses Verfahren mit der Caesar-Verschlüsselung hinsichtlich der Möglichkeit, bei bekanntem Verfahren, aber ohne Kenntnis des Schlüssels vom Geheimtext auf den Klartext zu schließen. (11 BE)

Bei der zweiten Stufe der ADFGVX-Verschlüsselung wird der Geheimtext der ersten Stufe zeilenweise in eine neue Matrix (s. Abb. 2.2) eingetragen. Die Breite dieser Matrix ergibt sich aus einem Schlüsselwort (hier im Beispiel `NACHRICHT`). Das Schlüsselwort wird über die Matrix geschrieben. Die Buchstaben dieses Schlüsselwortes werden dann in alphabetischer Reihenfolge nummeriert.

Nachdem der Geheimtext der ersten Stufe in die Matrix eingetragen wurde, wird diese nun spaltenweise ausgelesen. Dabei entspricht die Reihenfolge der ausgelesenen Spalten der alphabetischen Nummerierung der Schlüsselwortbuchstaben.

Aus dem Geheimtext der ersten Stufe `DXFFAVAVGFAVXXGFAFFX` entsteht durch die Anwendung der zweiten Verschlüsselungsstufe (Schlüsselwort `NACHRICHT` entsprechend Abbildung 2.2) der endgültige Geheimtext `XAXFVAFFXVAVGDFFAXGF`.

b) Bestimmen sie aus dem Geheimtext `FDXXGAXDXDFXVDFAGGGVFGDADX` den Klartext. Es wurde für die zweite Stufe das Schlüsselwort `ROSE` gewählt. Für die erste Stufe der Verschlüsselung wurde erneut die im Material angegebene Schlüsselmatrix (s. Abb. 2.1) verwendet.

Analysieren Sie die Auswirkungen eines falschen oder fehlenden Geheimtextbuchstabens auf die korrekte Entschlüsselung. (10 BE)

c) Analysieren Sie, inwiefern das ADFGVX-Verfahren mithilfe einer Häufigkeitsanalyse angegriffen werden kann.

Fritz behauptet, dass sich die Sicherheit des gesamten Verschlüsselungsverfahrens bezüglich des Angriffs mit einer Häufigkeitsanalyse durch das Vertauschen der beiden Verschlüsselungsstufen erhöhen würde. Es würde zunächst der Klartext in die Matrix eingetragen und spaltenweise ausgelesen werden. Das Ersetzen der Buchstaben gemäß der Schlüsselmatrix würde im zweiten Schritt erfolgen.

Georg hat eine andere Idee: Er schlägt vor, die zweite Stufe der Verschlüsselung durch das Vigenère-Verfahren zu ersetzen, um den Angriff auf die Verschlüsselung mithilfe einer Häufigkeitsanalyse zu erschweren. Georg meint damit, dass auf den Geheimtext der ersten Stufe der ADFGVX-Verschlüsselung eine Vigenère-Verschlüsselung angewendet werden soll.

Beurteilen Sie jeweils, ob die Vorschläge einen Gewinn hinsichtlich der Sicherheit erzielen. (9 BE)