1 Verschlüsselung – der nächste Schritt

1.1 Ziel

Die SuS können anhand eines einfachen Models verstehen, wie moderne Kryptographie funktioniert. Insbesondere sind sie in der Lage die Grundprinzipien von AES (Kombination von Transposition und Substitution) zu verstehen.

1.2 Methodik und Ablauf

Mit Hilfe einer Einistiegsaufgabe, die das Vorwissen der SuS aufnimmt wird die Idee der Kombination von verschiedenen Verschlüsselungstechniken eingeführt. In diesem Fall ist es eine Kombination einer Caesar-Verschlüsselung mit einer einfachen Transposition. Die Aufgabe sollte in ca. 10 Minuten lösbar sein.

In einer anschliessenden Diskussion kann das Vorwissen fixiert und erweitert werden. Wichtige Fachbegriffe werden wiederholt und im neuen Kontext beschrieben.

Die SuS lösen dann selbständig die weiteren Aufgaben, in denen diese zentralen Themen vertieft werden.

Zum Abschluss der Lektion kann mit der angehängten Graphik die Verbindung zu AES gemacht werden.

Referenz: Anhaltspunkte für die Diskussion

- Wenn man verschiedene Verschlüsselungstechniken kombiniert, kann das zu stärkeren Verschlüsselungen führen.
- Welche Verschlüsselungsverfahren kennt ihr schon? Wie könnte man diese Kombinieren.
- Repetition von wichtigen Fachbegriffen: Plaintext, ciphertext, keyspace, ecryption, decryption, encoding, decoding. . .
- Ausblick auf die moderne Verschlüsselung z.B. AES (Anhand einer Graphik).

2 Aufgaben

Einstiegsaufgabe

Steffi die Super-Spionin hat zwei Nachrichten des Feindes abgefangen.

`BNW LWJNKJS RTWLJS ZR EJMS FS`

und

`WEMNH IIOUN RFRMA GEGZN RNEE*`

Offensichtlich testet der Felix der Feind ein neues Verschlüsselungsverfahren. Sie enthalten nämlich beide denselben Inhalt – auf zwei verschiedene Arten verschlüsselt. Welchen?

[Hinweis: die Leerzeichen können weiterhelfen.]

Am nächsten Tag fängt Steffi eine andere Nachricht ab. Diese scheint etwas komplizierter verschlüsselt zu sein. Was könnte diese wohl bedeuten?

`MNISSRHMJTF FJNPJJMYWIH MXTTSWSZJJP FJYJNSNSSPJ INJSRTHXHSS`

[Variante: ein kleines bisschen schwieriger] `MNISS RHMJT FFJNP JJMYW IHMXT TSWSZ JJPFJ YJNSN SSPJI NJSRT HXHSS`

Weiterführende Aufgaben

Exercise 1. Wählen Sie einen eigenen Text und verschlüsseln diesen mit dem obigen Verfahren.

Exercise 2. Erfinden Sie eine Abwandlung dieses Verfahrens (Kombination von Transposition und Caesar-Substiitution) und verschlüsseln Sie einen gewählten Text. Tauschen Sie einem Klassenkameraden/-kameradin Ihre Geheimtexte und versuchen Sie diese zu Entschlüsseln.

Exercise 3. Felix wählt 20 zufällige Zahlen zwischen 1 und 25. Er führt nun 20 Caesar-Verschlüsselungen auf eine Geheimbotschaft an.

Er behauptet, dass sein Schlüsselraum nun eine Grösse von 25^{20} hat. Stimmt das?

Exercise 4. Im oberen Beispiel wurde ein Caesar-Code mit einer Transpositionskodierung kombiniert. Spielt es eine Rolle, in welcher Reihenfolge dies geschieht?

Exercise 5. Felix wählt nun wieder 20 Zufallszahlen wie oben und Verschlüsselt eine Geheimbotschaft 20 mal mit einer Caesar-Verschlüsselung; nun führt er aber nach jedem Caesar-Schritt eine Transposition durch (immer dieselbe – in Zeilen Schreiben und nach Spalten lesen).

Ist das eine sicherere Verschlüsselungsmethode als beide Verfahren einfach je einmal anzuwenden?

Exercise 6. Verschlüsseln Sie einen Klartext, indem Sie eine zweifache Block-Transposition benutzen. Verwenden Sie, aber nicht für beide dieselben Blockgrössen. Gilt hier wie bei der Caesar-Verschlüsselung, dass das einfach eine andere Block-Transposition ist, oder ist dieses Verfahren sicherer.

Exercise 7. Nun macht Felix dieselben 20 loops, aber statt einer Caesar-Verschlüsselung verwendet er jedesmal einen Vigenère-Code (z.B. mit dem keyword `APFEL`). Ist dieses Verfahren sicherer als einmaliges Verschlüsseln mit Vigenère und Transponieren?

Exercise 8. Wie könnte man ein solches Verschlüsselungsverfahren (Cryptosystem) noch sicherer machen?

Lösungen

Einstiegsaufgabe. Beim ersten Code handelt es sich um eine Caesar Verschlüsselung mit $key = 5$. Die Dekodierung liefert `WIR GREIFEN MORGEN UM ZEHN AN.`

Die zweite ist eine Transpositionschiffre (der Stern ist ein Füllzeichen):

```
WEMNH
IIOUN
RFRMA
GEGZN
RNEE*
```

Wenn man diese von oben nach unten Spaltenweise liest, erhält man dieselbe Botschaft.

Wenn man nun den verschlüsselten Text in Zeilen schreibt und mit dem selben Caesar Schlüssel entschlüsselt, erhält man den Klartext spaltenweise:

```
HAHAD IESEI DIOTE NKOEN NENIM MERNO CHNIC HTUNS ERENC ODEKN ACKEN
```

Oder: "Ha Ha diese Idioten können immer noch nicht unseren Code knacken."

Solution of Exercise 1: Seien Sie kreativ!

Solution of Exercise 2: Seien Sie kreativ!

Solution of Exercise 3: Eine Caesar Verschlüsselung kann nur auf eine von $25 = 26 - 1$ Arten geschehen. Jede Kombination von Caesar Schlüsseln, führt wieder zu einem anderen Caesar Schlüssel.

Solution of Exercise 4: Es spielt keine Rolle, ob zuerst transponiert oder verschoben wird. Die Verschlüsselte Botschaft bleibt gleich.

Solution of Exercise 5: Dieses Verfahren ist äquivalent zu einer einmaligen Caesar Verschlüsselung kombiniert mit 20-facher Transposition. Insofern ist dieses Verfahren ein bisschen sicherer, als das vorherige, aber nur weil nicht mehr so klar ist, wie die Transpositionen zustande kamen.

Fall natürlich der Text aus genau 25 Buchstaben besteht, dann erhält man zweifacher Transposition gerade wieder den Klartext. In diesem Fall würde es Sinn machen ein anderes Transpositionsverfahren zu benutzen.

Solution of Exercise 6: Im Allgemeinen sollte diese Verfahren sicherer sein. Es kommt aber sehr darauf an, wie man die Blocks wählt und wie der Klartext strukturiert ist.

Solution of Exercise 7: Bei der Vigenère Verschlüsselung werden Buchstaben an verschiedenen Positionen anders kodiert. Entsprechend führt eine Transposition dazu, dass Buchstaben mehrfach mit verschiedenen Verschiebungen kodiert werden. DIes führt zu einem ziemlich sicheren Verschlüsselungsverfahren.

Solution of Exercise 8: Je länger und komplexer das Schlüsselwort bei der Vigenère Verschlüsselung ist, desto sichere wird die Verschlüsselung, da Mustererkennung schwieriger wird. Durch die Transposition wird es auch schwierig nach zweier- und dreier-Blöcke im Text zu suchen, was die statistische Analyse erschwert.

Falls natürlich der Schlüssel beim Vigenère Verfahren gleich lange oder länger wie die Botschaft ist, kommen wir dem einzig wirklich sicheren Verschlüsselungsverfahren – dem One-Time-Pad – näher.

3 Weiterführende Ressourcen für Lehrpersonen

3.1 Ressourcen zu AES

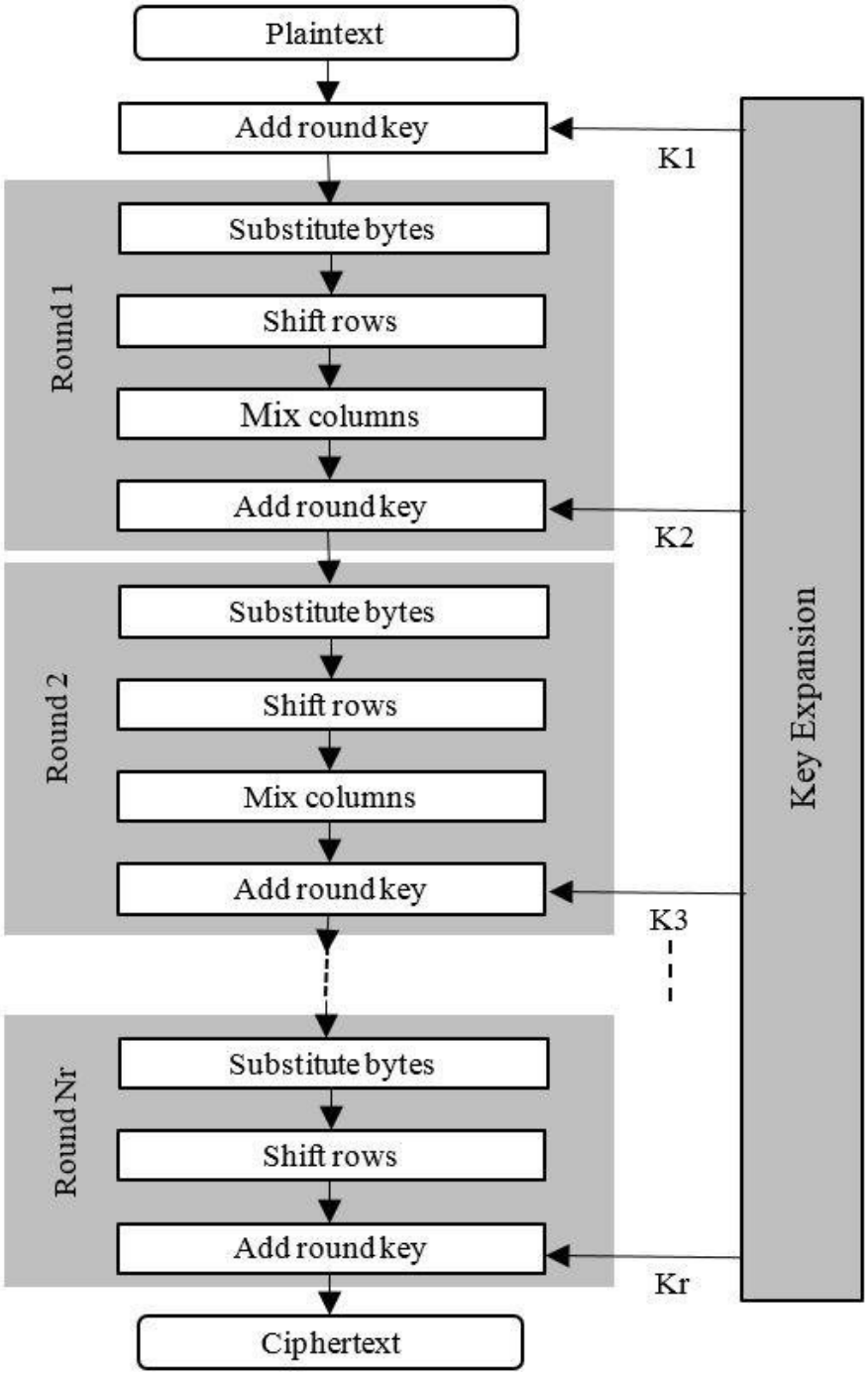
Falls man mit den SuS tatsächlich verwendete Verfahren anschauen möchte, dann bietet es sich an, AES auf einem einfachen Level als Kombination von Substitutionen und Transpositionen anzuschauen. Es gibt auch ein sehr gutes Video von Computerphile dazu:

https://www.youtube.com/watch?v=O4xNJsjtN6E

Die nachfolgende Graphik kann man zur Veranschaulichung verwenden:

Quelle: A Survey on the Cryptographic Encryption Algorithms - Scientific Figure on ResearchGate. Available from: `https://www.researchgate.net/figure/Advanced-Encryption-Standard-AES-Algorithm_fig5_321587376` *[accessed 26 Nov, 2021]*

Graphik zu AES



3.2 Kommentare zur Einstiegaufgabe

Die SuS sollen hier bemerken, dass die neue Botschaft eine Kombination der Codes aus den beiden vorherigen ist. Da sowohl Schlüssel sowie die Transposition gleich bleiben, sollte diese Aufgabe lösbar sein. Sie ist aber sicherlich nicht eine einfache oder übermässig kurze Aufgabe. Man wird da ein bisschen 'eintauchen' müssen.

3.3 Kommentare zu einzelnen Aufgaben

1. Diese Aufgabe hat keinen expliziten Lösungsschlüssel. Die SuS sollen hier kreativ sein.

2. Diese Aufgabe hat keinen expliziten Lösungsschlüssel. Die SuS sollen hier kreativ sein.

3. Die SuS sollen hier bemerken, dass mehrfache Verschiebungen von Buchstaben wieder zu einer (veränderten) Verschiebung führen.

4. Hier könnte man weitere Beispiele von transitiven oder nicht-transitiven Operationen zeigen (z.B. Multiplikation, Addition vs. Spiegelungen und Translationen)

5. Dies soll die SuS ein bisschen darauf bringen, dass es sicherer ist, wenn nicht alle Buchstaben mit der gleichen Verschiebung kodiert werden. Im nächsten Beispiel wird das dann anhand des Beispiels der Vigenère Verschlüsselung gemacht.

6. Hier geht es darum zu erkennen, dass eine zweifache Ausführung einer solchen Transposition durhchaus komplexer sein kann, als eine einfache.

   Selbstverständlich führt das alles zu einer Permutation der Buchstaben, aber nicht jede Permutation von Buchstaben kann als Block-Transposition entstehen. Wenn man dieses Verfahren weiterführt kommt man bald in die Nähe von $n!$ in den Zeichen für die Komplexität – was doch ziemlich sicher ist.

7. Dieses Verfahren kann man als einfaches Analogon zu einem modernen Verschlüsselungsverfahren wie AES betrachten. Dort werden ebenso in zahlreichen

’loops’ Bits (statt Buchstaben) substituiert und transponiert. Also ähnlich wie dieses Beispiel es mit Buchstaben macht.

8. Das One-Time-Pad kann hier oder an anderer Stelle erklärt werden. Grundlegende Voraussetzungen für die Sicherheit des One-Time-Pads sind:

   Der Schlüssel

   - muss mindestens so lang sein wie die Nachricht,
   - muss gleichverteilt zufällig gewählt werden,
   - muss geheim bleiben und
   - darf nicht wiederverwendet werden, auch nicht teilweise.