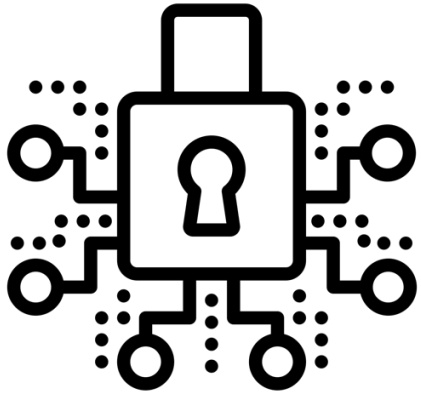

Crypto Challenge

Caesar-Chiffre

Hintergrund

Der Name Caesar-Chiffre stammt von dem gleichnamigen Feldherren Gaius Julius Caesar (100 v. Chr. – 44 v. Chr.). Caesar (manchmal im Deutschen auch Cäsar geschrieben) benutzte diese sehr einfache Form der Verschlüsselung, um militärische Nachrichten zu chiffrieren.

Beschreibung des Verfahrens

Es kann ein beliebiges Alphabet verwendet werden. Die hier genutzte Version benutzt die Großbuchstaben A-Z und die Zahlen 0-9. Das Alphabet wird zweimal, untereinander aufgeschrieben.

```
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 0 1 2 3 4 5 6 7 8 9
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 0 1 2 3 4 5 6 7 8 9
```

Nun wird das untere Alphabet um eine beliebige Anzahl Stellen verschoben. Diese Anzahl von Stellen ist der Wert des Schlüssels. Eine Verschiebung um 3 nach links, also mit dem Schlüssel 3, ergibt folgende Ansicht:

```
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 0 1 2 3 4 5 6 7 8 9
D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9 A B C
```

Ein A wird somit zu einem D, ein B zu einem E, ein C zu einem F, usw. Das Wort "Beispiel" würde somit unleserlich zu "Ehlvslho" chiffriert. Das obere Alphabet nennt man "Klartext-Alphabet" und das untere Alphabet nennt man "Geheimtext-Alphabet".

Vorgehen mit einer Chiffrierscheibe

Die Chiffrierscheibe wird so eingestellt, dass gleiche Buchstaben und Zahlen einander gegenüberliegen.

Verschlüsseln: Innere Scheibe gegen den Uhrzeigersinn um so viele Positionen gegen die Äußere verdrehen, wie die Verschiebezahl angibt. Die Buchstaben auf der äußeren Scheibe suchen und die entsprechenden Buchstaben auf der inneren Scheibe ablesen.

Entschlüsseln: Innere Scheibe im Uhrzeigersinn um so viele Positionen gegen die Äußere verdrehen, wie die Verschiebezahl angibt. Die Buchstaben auf der äußeren Scheibe suchen und die entsprechenden Buchstaben auf der inneren Scheibe ablesen.

Vigenère-Chiffre

Hintergrund

Die Vigenère-Chiffre stammt aus dem 16. Jahrhundert und wurde von dem französischen Kryptografen Blaise de Vigenère (* 15. April 1523 in Saint-Pourçain; † 1596)[1] entwickelt. Sie basiert auf der Verwendung der Caesar-Chiffre, allerdings mit wechselnden Alphabeten.

Beschreibung des Verfahrens

Es wird ein beliebig langer Schlüssel gewählt. Alle Zeichen des Schlüssels müssen demselben Alphabet angehören wie die Zeichen des zu verschlüsselnden Klartextes. Zur Demonstration seien dies wieder die Großbuchstaben A-Z und die Zahlen 0-9.

Als Beispiel wird nun der Satz „DIES IST EIN GEHEIMER TEXT" mit dem Schlüssel „KEY" verschlüsselt. Als Erstes wird der Schlüssel unter den Klartext gesetzt und so oft wiederholt, bis er der Länge des Klartextes entspricht.

```
DIES IST EIN GEHEIMER TEXT   (Klartext)
KEYK EYK EYK EYKEYKEY KEYK   (Schlüssel)
```

Nun kommt die Caesar-Chiffre zum Einsatz. Der erste Buchstabe des Klartextes D wird durch die Caesar-Chiffre mit dem ersten Buchstaben des Schlüssels K verschlüsselt. Das bedeutet, dass für die Caesar-Verschlüsselung das Alphabet um den Schlüssel K nach links verschoben wird. Da K der elfte Buchstabe im Alphabet ist, bedeutet dies eine Verschiebung um zehn Zeichen, womit sich diese Abbildung ergibt:

```
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 0 1 2 3 4 5 6 7 8 9
K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J
```

A würde also auf K abgebildet, B auf L, C auf M und dementsprechend das D (von „DIES IST EIN GEHEIMER TEXT") auf das N. Somit ist der erste Buchstabe des Geheimtextes das N. Anschließend wird der zweite Buchstabe des Klartextes I durch die Caesar-Chiffre mit dem zweiten Buchstaben des Schlüssels E verschlüsselt. E ist der fünfte Buchstabe im Alphabet, was eine Verschiebung der Ausgangsabbildung um vier Zeichen nach links bedeutet:

```
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 0 1 2 3 4 5 6 7 8 9
E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9 A B C D
```

Demnach wird das I auf das M abgebildet und der bis dahin berechnete Geheimtext ist NM. Nach diesem Schema wird der gesamte Text zeichenweise verschlüsselt, sodass sich am Ende der Geheimtext: „NM22 MG3 I6X K2RI6WIF 3IL3" ergibt.

RSA-Algorithmus

Hintergrund

RSA (Rivest–Shamir–Adleman) ist ein asymmetrisches kryptographisches Verfahren, das zum Verschlüsseln von Nachrichten verwendet wird. Es verwendet ein Schlüsselpaar, bestehend aus einem privaten Schlüssel, der zum **Entschlüsseln** von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man Daten **verschlüsselt**. Der private Schlüssel wird geheim gehalten und kann nicht mit realistischem Aufwand aus dem öffentlichen Schlüssel berechnet werden.

Die Sicherheit von RSA basiert darauf, dass es zwar einfach ist, das Produkt n zweier großer Primzahlen p und q zu berechnen. Es ist jedoch sehr schwer, nur aus dem Produkt n die beiden Primzahlen zu bestimmen, die das Produkt ergeben. Dieses Zerlegen nennt man auch die Primfaktorzerlegung von n.

Schlüsselerzeugung

1. Wähle zufällige Primzahlen p und q, $p \neq q$
2. Berechne $n = p * q$
3. Wähle e mit $0 < e < \varphi(n)$ und $ggT(e,\ \varphi(n)) = 1$
4. Berechne $d \equiv e^{-1}\ mod\ \varphi(n)$
5. Erhalte $K_{pub} = (n,\ e),\ \ K_{priv} = (p, q, d)$

Verschlüsselung

Für m aus $\mathbb{Z}_n$: Berechne c $\equiv m^e\ mod\ n$

Entschlüsselung

Berechne m $\equiv c^d\ mod\ n$, sodass $m \in \mathbb{Z}_n$

Modulo-Rechnung

Modulo ist eine Rechenoperation (wie z. B. Addition oder Multiplikation). Sie wird für zahlreiche Verschlüsselungsverfahren benötigt.

Mit Modulo, mod, wird der Rest der ganzzahligen Division bezeichnet.

Beispiel-Rechnungen:

$18\ mod\ 5 = 3$, da $18 : 5 = 3$ (Rest 3)

$10\ mod\ 4 = 2$, da $10 : 4 = 2$ (Rest 2)

$14\ mod\ 7 = 0$, da $14 : 7 = 2$ (Rest 0)

Crypto Challenge

Caesar-Challenge

Ciphertext: SUZ5FDFH
Key: 13
Alphabet: A-Z0-9
Tools: Chiffrierscheibe

Ziel: Entschlüssle den Ciphertext und ermittle den Klartext!

Vigenère-Challenge

Ciphertext: ZXE1WAA
Key: S3CR3T
Alphabet: A-Z0-9
Tools: Vigenère-Quadrat

Ziel: Entschlüssle den Ciphertext und ermittle den Klartext!

Caesar-Challenge ohne bekannten Schlüssel

Ciphertext: KDOORZHOW
Alphabet: A-Z0-9
Tools: Chiffrierscheibe

Ziel: Finde den passenden Schlüssel und entschlüssle die geheime Nachricht!

Für die Profis

Crypto Challenge

Caesar-Challenge

Ciphertext: 26I79XY9
Key: 13
Alphabet: A-Z0-9
Tools: Chiffrierscheibe

Ziel: Entschlüssle den Ciphertext und ermittle den Klartext! Der resultierende Klartext ist der Ciphertext der nächsten Challenge.

Vigenère-Challenge

Ciphertext: Lösung der Caesar-Challenge
Key: S3CR3T
Alphabet: A-Z0-9
Tools: Vigenère-Quadrat

Ziel: Entschlüssle den Ciphertext und ermittle den Klartext! Der resultierende Klartext ist der Ciphertext der nächsten Challenge.

RSA-Challenge

Ciphertext: 120 57 78
Öffentlicher Schlüssel: n=143 und e=23

Ziel: Aus den gegebenen Informationen den privaten Schlüssel berechnen, um den Ciphertext zu entschlüsseln.

Hinweise:

- Die Lösung der Vigenère-Challenge ist ASCII-kodiert (hexadezimal). Dekodiere diese für einen Hinweis.
- Wenn die geheimen Primfaktoren p und q bekannt sind, so kann d berechnet und die Entschlüsselungsfunktion ausgeführt werden.
- $\varphi(n) = (\mathrm{p} - 1) * (\mathrm{q} - 1)$
- Das Ergebnis der Entschlüsselung ist wieder ASCII-kodiert (dezimal) und muss dekodiert werden.

Lösungen für die Profi Challenge

Caesar-Challenge

Klartext: PT5UWKLW
Ciphertext: 26I79XY9
Key: 13
Alphabet: A-Z0-9

```
Ciphertext: 26I79XY9
Klartext:   PT5UWKLW
```

Vigenère-Challenge

Klartext: 703D3133
Ciphertext: PT5UWKLW
Key: S3CR3T
Alphabet: A-Z0-9

```
Ciphertext: PT5UWKLW
Key:        S3CR3TS3
Klartext:   703D3133
```

RSA-Challenge

Lösung von Vignère-Challenge ASCII-dekodiert: $p = 13$
Gegeben: $n = 143$ und $e = 23$
Berechne mit $p = 13$ das q → $n = p * q \implies 143 = 13 * q \implies \frac{143}{13} = q = 11$

Berechne $\varphi(n) = (\mathrm{p} - 1) * (\mathrm{q} - 1) = 12 * 10 = 120$

Berechne $d \equiv e^{-1}\ mod\ \varphi(n) \implies d \equiv 23^{-1}\ mod\ 120 \implies d \equiv 47$

Führe auf dem Ciphertext 120 57 78 die RSA-Entschlüsselung aus →
Das Klartextergebnis 87 73 78 ergibt ASCII-dekodiert **WIN**

```
Klartext: 70 3D 31 33
           p  =  1  3
```

$\mathbf{m} \equiv \boldsymbol{c^d\ mod\ n}$
$120^{47}\ mod\ 143 \equiv 87$
$57^{47}\ mod\ 143 \equiv 73$
$78^{47}\ mod\ 143 \equiv 78$

Lösungen für die Basic Challenge

Caesar-Challenge

Klartext: FHMS2024
Ciphertext: SUZ5FDFH
Key: 13
Alphabet: A-Z0-9

```
Ciphertext: SUZ5FDFH
Klartext:   FHMS2024
```

Vigenère-Challenge

Klartext: H4CK3RS
Ciphertext: ZXE1WAA
Key: S3CR3T
Alphabet: A-Z0-9

```
Ciphertext: ZXE1WAA
Key:        S3CR3TS
Klartext:   H4CK3RS
```

Caesar-Challenge ohne bekannten Schlüssel

Klartext: HALLOWELT
KEY: 3 (durch erraten, bruteforce)
Ciphertext: KDOORZHOW
Alphabet: A-Z0-9