Station 1 – Skytale

Hintergrund

Bei der Skytale (σκυτάλη) handelt es sich um eine der ältesten Verschlüsselungsverfahren. Sie wird auf ca. 2500 Jahre geschätzt und den Spartanern im alten Griechenland angerechnet.

Laut dem Geschichtsschreiber Cornelius Nepos wurde um 478 v. Chr. der griechische Heerführer Pausanias (Παυσανίας) mit einer mittels Skytale verschlüsselten Nachricht zurückbeordert, als dieser sich mit dem Heer in Kleinasien aufhielt. Pausanias stand unter dem Verdacht einen Umsturz zu planen.

Auch im Peloponnesischen Krieg (431 v. Chr. bis 404 v. Chr.) spielte die Skytale eine Rolle. Der Historiker Plutarch beschreibt, dass der General Lysander (Λύσανδρος) Vorwarnungen vor dem Angriff der Perser in Form von mit Skytale verschlüsselter Botschaften erhielt. Einer von fünf Boten hatte geschunden den Marsch von Persien überlebt und überreichte Lysander seinen Gürtel. Lysander wickelte ihn um einen Stab und konnte die zufällig auf dem Gürtel verteilt scheinenden Buchstaben lesen. Dadurch konnten Vorbereitungen getroffen und der Angriff erfolgreich abgewehrt werden.

Prinzip

Ein Skytale beschreibt sowohl den Holzstab als auch das damit funktionierende Verschlüsselungsverfahren. Sowohl der Sender als auch der Empfänger haben einen Holzstab mit einer bestimmten Dicke.

Zum Verschlüsseln einer Botschaft wird ein Pergament oder Lederstreifen wendelförmig um den Stab gewickelt, so dass sich eine beschreibbare Fläche ergibt.

Quelle: Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Skytale.png

Wird der Steifen wieder abgewickelt, lässt sich der Zusammenhang der Buchstaben nicht mehr ohne viel Ausprobieren wiederherstellen, da die Buchstaben scheinbar willkürlich auf dem Streifen angeordnet sind.

Zum Entschlüsseln wird das Band wieder um einen Stab der gleichen Dicke gewickelt und die Buchstaben sind wieder in der richtigen Reihenfolge.

Als **geheimer Schlüssel** dieses Verfahrens dient der Holzstab bzw. dessen Umfang, der die Verschiebung beeinflusst. Es handelt sich um ein sogenanntes Transpositionsverfahren, bei dem die Buchstaben des Textes umsortiert werden. Bei der Skytale handelt es sich um ein symmetrisches Verschlüselungsverfahren, da zum ver- und entschlüsseln der gleiche Schlüssel genutzt wird. Dieser muss vorher zwischen den Teilnehmer*innen der Kommunikation über einen sicheren Weg ausgetauscht werden.

Die Sicherheit der Skytale war für damalige Verhältnisse sehr hoch. Nach dem Untergang der antiken Kulturen gab es erst im Mittelalter vergleichbar sichere Verschlüsselungsverfahren.

Beispiel

Am Stand siehst du ein Beispiel einer Botschaft. Einmal ist sie auf dem ursprünglichen Stab aufgewickelt, einmal ohne Stab und einmal auf einem Stab mit der falschen Größe aufgewickelt.

Du kannst leicht erkennen, dass die Nachricht ohne Stab oder mit dem falschen nicht so einfach zu entziffern ist.

Angriffe

Mathematisch gesehen, kann es unendlich viele Umfänge für einen Stab geben, da zwischen zwei Durchmessern, immer noch einer passt, der dazwischen liegt. Es spielt aber in der Praxis keine Rolle, ob ein Stab 4,005 oder 4,006 oder 4,007 Zentimeter Umfang hat. Die Buchstaben verschieben sich nur minimal und der Text bleibt bei geringer Abweichung lesbar. D.h. dass die Anzahl der möglichen Schlüssel in der Praxis doch beschränkt ist und ein Durchprobieren verschieden dicker Stäbe zu Erfolg führen wird. Das bloße Durchprobieren von möglichen Schlüsseln nennt man auch Brute-Force-Angriff.

Ausprobieren

Als Skytale eignen sich nicht nur klassische Holzstäbe. Auch Flaschen, Stifte oder Besenstiele sind geeignet, um eine Botschaft darum zu wickeln. Hauptsache du hast zweimal den gleichen Gegenstand zur Verfügung, damit deine Gesprächspartnerin oder dein Gesprächspartner die Nachricht auch entschlüsseln kann.

Finde die richtige Skytale

Wir haben mehrere Botschaften für euch mit unterschiedlichen Skytalen verschlüsselt. Kannst du sie entschlüsseln?

1. Nimm dir einen der bereitliegenden Papiersteifen und wickeln ihn nacheinander um die ausliegenden Stäbe. Bei den meisten wirst du nur Buchstabensalat sehen. Doch bei dem einem passendem Stab ergibt sich eine Botschaft.
2. Nimm nun einem anderen Streifen und versuche diesen mit dem gleichen Stab wie aus Aufgabe 1. Du wirst feststellen, dass diese Botschaft mit einem anderen Stab erstellt wurde und dass der Stab nicht funktioniert. Versuche nun die anderen Stäbe, bis du eine Botschaft lesen kannst.

Wie du gemerkt hast, ist der Durchmesser des Stabes für die Verschlüsselung ausschlaggebend. Je nachdem mit welchem Stab der Text verschlüsselt wurde, kann er auch nur mit diesem wieder gelesen werden.

Verschlüssele eine Botschaft für jemanden

Als zweiten Versuch kannst du ein eigene an jemanden verschlüsseln.

1. Nimm dir einen Stift, einen Streifen Papier und einen der ausliegenden Stäbe oder Gegenstände
2. Wickele deinen Papierstreifen um den Stab und befestige ihn mit Reißzwecken. Bei Dingen, die nicht aus Holz sind, hilft ein Streifen Tesafilm beim Fixieren.
3. Schreibe deine Botschaft Zeile für Zeile auf das Papier.
4. Wickele deinen Papierstreifen ab und gebe ihn an einen anderen Teilnehmer oder Teilnehmerin weiter.
5. Diese*r kann nun versuchen, den richtigen Stab zum Entschlüsseln zu finden.