D_KRYPTOGRAFIE_SYM_ANNEX

Aufgabe-1 Cryptool-Applikation installieren: Mit CrypTool1, einem Open-Source-Projekt und somit freier Lern-Software erhalten wir ein Tool in die Hand, dass die Konzepte der Kryptographie und der Kryptoanalyse erfahrbar machen lässt. Installieren Sie nun CrypTool1 auf ihrem Notebook, bei Sicherheitsbedenken als virtuelle Applikation.
CRYPTOOL1 kann man hier herunterladen: https://www.cryptool.org/de/ct1/

Aufgabe-2 Rotationschiffre: Schon der römische Feldherr und spätere Kaiser Julius Cäsar kannte den folgenden Verschlüsselungstrick und nutzte ihn bei seinen geheimen Botschaften: Ersetze jeden Buchstaben durch den, der eine bestimmte Anzahl Stellen später im Alphabet folgt! Somit konnte Cäsar effektiv geheime Botschaften übermitteln, wie z.B. diese Zitate:
GHU DQJULII HUIROJW CXU WHHCHLW GLH ZXHUIHO VLQG JHIDOOHQ LFK NDP VDK XQG VLHJWH WHLOH XQG KHUUVFKH
Benutzen Sie nun Ihr CrypTool1 und finden Sie heraus, um welche Zitate es sich handelt! Die Rotationschiffre ist übrigens ein klassisches, symmetrisches Verfahren. Nun aber nicht einfach drauflos probieren. Machen Sie etwas Kryptoanalyse mit einem ASCII-Histogramm. (Tipp: Häufigkeitsanalyse der im Text enthaltenen Buchstaben)

Aufgabe-3 Vigenèreverschlüsselung: Um etwas warm zu laufen, verschlüsseln wir, diesmal ohne Cryptool, das Wort **BEEF** mit dem Schlüsselwort **AFFE**.
Wer will, kann sich hier noch an einer Entschlüsselung des Geheimtexts **WRKXQT** mit dem Schlüsselwort **SECRET** versuchen.

Nun wirds spannender: Wir versuchen den Vigenère-Code zu knacken und bedienen uns einem Analysewerkzeug im Cryptool1. Abgefangen haben wir die folgende Vigenère-Chiffre:

USP JHYRH ZZB GTV CJ WQK OCLGQVFQK GAYKGVFGX NS ISBVB MYBC MWCC NS JOEVB GTV KRQFV AGK XCUSP VFLVBLLBE ESSEILUBCLBXZU SENSWFGVRCES SER CZBCE ILUOLBPYISL CCSZG VZJ

Neugierig wie wir sind, möchten wir gerne wissen, welcher Text hinter dieser Chiffre steckt. Da uns aber das Schlüsselwort fehlt, müssen wir tief in unsere Trickkiste greifen. (Tipp: Im CrypTool1/Hilfe/Index/Vigenère-Verschlüsselungsverfahren findet man weitere Informationen zum Vigenère-Analyseverfahren.)

Zu guter Letzt versuchen wir, ob das Analysetool auch Resultate liefert, wenn das Passwort wesentlich länger ist. Nehmen sie den entschlüsselten Text von vorhin und verschlüsseln sie ihn erneut, diesmal aber mit diesem Schlüssel:

LoremipsumdolorsitametconsectetueradipiscingelitAeneancommodoligulaegetdolorAeneanmassaCumsociisnatoquepenatibusetmagnisdisparturientmontesnasceturridiculusmusDonecquamfelisultriciesnecpellentesqueeupretiumquissemNullaconsequatmassaquisenimDonecpedejustofringillavelaliquetnecvulputateegetarcuInenimjustorhoncusutimperdietavenenatisvitaejustoNullamdictumfeliseupedemollispretiumIntegertinciduntCrasdapibusVivamuselementumsempernisiAeneanvulputateeleifendtellusAeneanleoligulaporttitoreuconsequatvitaeeleifendacenimAliquamloremantedapibusinviver

raquisfeugiatatellusPhasellusviverranullautmetusvariuslaoreetQuisque rutrumAeneanimperdietEtiamultriciesnisivelaugueCurabiturullamcorperu ltriciesnisiNamegetduiEtiamrhoncusMaecenastempustellusegetcondimentu mrhoncussemquamsemperliberositametadipiscingsemnequesedipsumNamquamn uncblanditvelluctuspulvinarhendreritidloremMaecenasnecodioetantetinc idunttempusDonecvitaesapienutliberovenenatisfaucibusNullamquisanteEt iamsitametorciegeterosfaucibustinciduntDuisleoSedfringillamaurissita metnibhDonecsodalessagittismagnaSedconsequatleoegetbibendumsodalesau guevelitcursusnunc

Funktionieren nun die Vigenère-Analysetools immer noch?

Aufgabe-4 XOR-Stromchiffre: Verschlüsseln sie die Dezimalzahl **`4711`** von Hand als XOR-Stromchiffre. Der binäre Schlüssel lautet: **`1000'1101`**. Zur Kontrolle entschlüsseln sie die erhaltene Chiffre wieder.
(Hinweis: Sie müssen die Dezimalzahl zuerst in eine 16-Bit Binärzahl umwandeln. Führende Nullen dabei nicht weglassen. Sollte der Schlüssel für die Verschlüsselung zu kurz sein, wird dieser mehrmals wiederholt. Der Datenstrom soll in dieser Aufgabe mit der Übertragung des MSB's, also von links nach rechts beginnen.)

Aufgabe AES (Advanced Encryption Standard): Öffnen sie nun in der Cryptool-Onlineversion die folgende Visualisierung AES-Rijndael-Animation und studieren sie diese: https://www.cryptool.org/de/cto/aes-animation

Aufgabe-5 Wie sicher ist mein Passwort? Da Cryptool ja bereits geöffnet ist, kann es auch nicht schaden, mal sein Lieblingspasswort auf seine Sicherheit zu überprüfen. Crypttol bietet dazu einen Passwort-Qualitätsmesser an: Einzelverfahren/Tools/Passwort-Qualitätsmesser