Häufigkeitsanalyse mit Vigenère verhindern

Blaise de Vigenère

1. Wie wir festgestellt haben, sind monoalphabetische Substitutionsverfahren bei steigender Textlänge anfällig gegenüber einer Häufigkeitsanalyse. Überlege, wie man eine Häufigkeitsanalyse erschweren könnte!
2. Der französische Kaufmann *Blaise de Vigenère* hat das Problem im 16. Jh. gelöst. Versuche anhand einer Demonstration die Idee des Verfahrens nachzuvollziehen:
   a. Öffne das Programm „Krypto“ und gibt einen Satz in das Klartext-Feld ein!
   b. Wähle im Menü Demos den Menüpunkt Vigenère-Verschlüsselung aus!
   c. Klicke nun wiederholt auf den Knopf „Buchstaben verschlüsseln“!
   d. Beschreibe die Vorgehensweise des Verfahrens!
3. Vereinbare mit deinem Partner ein Geheimwort und sendet euch mit dem Vigenère-Verfahren verschlüssle E-Mails zu!
4. Überprüfe dein Postfach! Die E-Mail mit dem Betreff „Haben Sie Erkenntnisse über diese Person?“ ist offenbar nicht an dich gerichtet und nur aus versehen falsch adressiert worden. Aber ein Verschlüsselter Text birgt (fast) immer ein Geheimnis … Schade nur, dass du das Schlüsselwort nicht kennst!
   a. Öffne das Programm *Cryptool*, kopiere den Inhalt der E-Mail in ein neues Dokument und wähle das Menü *Analyse >> Symmetrische Verschlüsselung (klassisch) >> Chyphertext Only >> Vigenère*!
   b. Überlege: Wie lässt sich eine mit dem Vigenère-Verfahren verschlüsselte Chiffre auch ohne Kenntnis des Schlüssels knacken, wenn die Länge des Schlüsselwortes bekannt ist?
   c. Welche Bedingung müsste erfüllt sein, um einen solchen Angriff unmöglich zu machen?
5. Recherchiere: Was besagt das *Kerckhoffs’sche Prinzip*?

Häufigkeitsanalyse mit Vigenère verhindern

Blaise de Vigenère

1. Wie wir festgestellt haben, sind monoalphabetische Substitutionsverfahren bei steigender Textlänge anfällig gegenüber einer Häufigkeitsanalyse. Überlege, wie man eine Häufigkeitsanalyse erschweren könnte!
2. Der französische Kaufmann *Blaise de Vigenère* hat das Problem im 16. Jh. gelöst. Versuche anhand einer Demonstration die Idee des Verfahrens nachzuvollziehen:
   a. Öffne das Programm „Krypto“ und gibt einen Satz in das Klartext-Feld ein!
   b. Wähle im Menü Demos den Menüpunkt Vigenère-Verschlüsselung aus!
   c. Klicke nun wiederholt auf den Knopf „Buchstaben verschlüsseln“!
   d. Beschreibe die Vorgehensweise des Verfahrens!
3. Vereinbare mit deinem Partner ein Geheimwort und sendet euch mit dem Vigenère-Verfahren verschlüssle E-Mails zu!
4. Überprüfe dein Postfach! Die E-Mail mit dem Betreff „Haben Sie Erkenntnisse über diese Person?“ ist offenbar nicht an dich gerichtet und nur aus versehen falsch adressiert worden. Aber ein Verschlüsselter Text birgt (fast) immer ein Geheimnis … Schade nur, dass du das Schlüsselwort nicht kennst!
   a. Öffne das Programm *Cryptool*, kopiere den Inhalt der E-Mail in ein neues Dokument und wähle das Menü *Analyse >> Symmetrische Verschlüsselung (klassisch) >> Chyphertext Only >> Vigenère*!
   b. Überlege: Wie lässt sich eine mit dem Vigenère-Verfahren verschlüsselte Chiffre auch ohne Kenntnis des Schlüssels knacken, wenn die Länge des Schlüsselwortes bekannt ist?
   c. Welche Bedingung müsste erfüllt sein, um einen solchen Angriff unmöglich zu machen?
5. Recherchiere: Was besagt das *Kerckhoffs’sche Prinzip*?

E-Mail (nur?) für Dich – eine Unterrichtsreihe des Projekts *Informatik im Kontext*