Vigenère knacken

Die Länge des Schlüsselworts bestimmen

Die polyalphabetische Verschlüsselung nach dem Vigenère-Verfahren hat eine Schwäche: In jeder Sprache gibt es einige kurze Wörter und Buchstabenkombinationen, die recht häufig auftreten. Werden diese mit denselben Buchstaben des Geheimworts verschlüsselt, so wiederholen sich auch dieselben Zeichen im Geheimtext. Über die Analyse des Auftretens solcher Wiederholungen (im Folgenden **Parallelstellen** genannt) lässt sich ein mit dem Vigenère-Verfahren verschlüsselter Text knacken:

1. Finde weitere Parallelstellen in unten stehendem Geheimtext und ergänze die Liste!
2. Berechne jeweils den Abstand zwischen den Parallelstellen!
3. Berechne den größten gemeinsamen Teiler der Abstände der Parallelstellen!
   Der so berechnete Wert ist sehr wahrscheinlich die Länge des Schlüsselworts.

**PWTMYTBADKDGPWPFYWFGUESOTLUPNVYWAPKCSOO
JWWASTLSUZUSJMJBBRSTIMGPYSXOJWWASMMZQLC
HJQWGYDHKOJWWASTMFPADWIPVKLHONZWPDPWRAA
GQPRKNJCNPKGPJJLTHYOWOHPGYJWCUEKUZLGAOW
KHOGPESMZMRWPBKVFVZTQNLAGSFSMVWTDPWRAAG
QPRKNJCNPTGTKEOMSGVLYVCHKBVKLOFOBLGNCIV
XWPLYBZAAEOOWKEWEODZKZOGPWGOMSWMPWTIFFL
CTUTYGUOSLZSILYOHEWEODSRVVYHSFAVVHHWGIP
TGHYHCWJVLERGJWKPDHGJWTUTQNBXGZEUKTWIAZ
PPMOGPWGJQWGYDHKNJCNPSOVWTZPFOMNQUQFGOW
PYTQNBAIVOSXNSNZNVHMSPAHCXBWVDTFJRWFLAS
XAGPHYHCWJVLEOANWKUPTXIYGUFFSQLLHZRKZFG
PYTXIYGUOWKVAEOEAOBBCVOSXVWKUMSGVLYVCHK
BOGYOSTSGGUYSTAAPKYWIPLBBRSRIKULYJUVWKU
PFHMDKLMWMMFRLCGUVKQSWAGVVWYNVLZSILYROM
KKJSBAZSWMOWKHMILSCKZAIRPWZHMGPYSXLWTNC
IVXWPIPNOMZGUSSXIMUIPYUUEGUKICMDEOPFMZM
RWPGOMYGOZSXBOKLGWKTWHYLUKVEWZDAGVEKUOS
YBWPZDHKTDGUFBJEWNJSSLZSILYYUMFPAPAGVKV
LWZKV**

Parallelstelle:	**Abstand:**
OJWWAS	**28, 21**
T..	

Vermutete Länge des Schlüsselworts: ☐

Vigenère knacken

Das Schlüsselwort bestimmen

Überlege: Wie lässt sich bei bekannter Länge des Schlüsselworts (für diesen Text 7) das Schlüsselwort selbst aus dem Geheimtext herausfinden?

Hinweis: Die Verschlüsselung erfolgt für die verschiedenen Buchstaben nach dem Cäsar-Verfahren, das wir bereits geknackt haben …

1234567 1234567 1234567 1234567 1234567

PWTMYTB ADKDGPW PFYWFGU ESOTLUP NVYWAPK
CSOOJWW ASTLSUZ USJMJBB RSTIMGP YSXOJWW
ASMMZQL CHJQWGY DHKOJWW ASTMFPA DWIPVKL
HONZWPD PWRAAGQ PRKNJCN PKGPJJL THYOWOH
PGYJWCU EKUZLGA OWKHOGP ESMZMRW PBKVFVZ
TQNLAGS FSMVWTD PWRAAGQ PRKNJCN PTGTKEO
MSGVLYV CHKBVKL OFOBLGN CIVXWPL YBZAAEO
OWKEWEO DZKZOGP WGOMSWM PWTIFFL CTUTYGU
OSLZSIL YOHEWEO DSRVVYH SFAVVHH WGIPTGH
YHCWJVL ERGJWKP DHGJWTU TQNBXGZ EUKTWIA
ZPPMOGP WGJQWGY DHKNJCN PSOVWTZ PFOMNQU
QFGOWPY TQNBAIV OSXNSNZ NVHMSPA HCXBWVD
TFJRWFL ASXAGPH YHCWJVL EOANWKU PTXIYGU
FFSQLLH ZRKZFGP YTXIYGU OWKVAEO EAOBBCV
OSXVWKU MSGVLYV CHKBOGY OSTSGGU YSTAAPK
YWIPLBB RSRIKUL YJUVWKU PFHMDKL MWMMFRL
CGUVKQS WAGVVWY NVLZSIL YROMKKJ SBAZSWM
OWKHMIL SCKZAIR PWZHMGP YSXLWTN CIVXWPI
PNOMZGU SSXIMUI PYUUEGU KICMDEO PFMZMRW
PGOMYGO ZSXBOKL GWKTWHY LUKVEWZ DAGVEKU
OSYBWPZ DHKTDGU FBJEWNJ SSLZSIL YYUMFPA
PAGVKVL WZKV

Vigenère knacken

Das Schlüsselwort bestimmen

1. Führe mit einem Partner eine Häufigkeitsanalyse für alle mit dem ___. Buchstaben des Schlüsselworts verschlüsselten Zeichen durch und trage die Anzahl der Zeichen in die entsprechende Spalte ein, um so dass häufigste Zeichen zu bestimmen, das sehr wahrscheinlich dem Klartextzeichen **E** entspricht! Damit wäre der Abstand zum Klartextalphabet ermittelt, der Buchstabe 5 Positionen vor dem häufigsten Geheimtextzeichen steht dann für das **A** und ist der Buchstabe des Geheimworts.
2. Tauscht euch mit Paaren aus, die die Häufigkeitsanalyse für die anderen Buchstaben des Schlüsselworts durchgeführt haben, um so gemeinsam das Schlüsselwort zu bestimmen!
3. Ob eure Analyse richtig ist könnt ihr überprüfen, in dem ihr den Geheimtext in *Krypto 1.5* öffnet und mit dem von euch bestimmten Schlüsselwort entschlüsseln lasst!

Geheim-textzeichen	1. Buchstabe	2. Buchstabe	3. Buchstabe	4. Buchstabe	5. Buchstabe	6. Buchstabe	7. Buchstabe
A	𝍸						
B							
C	𝍸 III						
D	𝍸 III						
E	𝍸 II						
F	III						
G	I						
H	II						
I							
J							
K	I						
L	I						
M	III						
N	III						
O	𝍸 𝍸						
P	𝍸 𝍸 𝍸 𝍸						
Q	I						
R	II						
S	𝍸						
T	𝍸						
U	I						
V							
W	𝍸						
X							
Y	𝍸 𝍸 II						
Z	III						
Häufigster Buchstabe:	**P**						
Buchstabe im Schlüsselwort:	**L**						

Schlüsselwort: L ...