Substitutionskryptering: Forskudt alfabet (Caesar Cipher)

Cæsarkryptering bruges i Romerriget, og her roteres alle bogstaver et antal positioner alfabetisk: BESKED >> CFTLFE. Før WWW blev den brugt i en række jokesgrupper I formen ROT 13:

Kan du finde pointerne? Hvorfor kaldes den ROT 13? Hvorfor foretrak man ROT 13?

Hvor sikker er Cæsarkryptering – hvor mange muligheder er der at gætte på?

Q: What do cats like to read?
A: Png-nybthrf!

Q: What kind of fun does a priest have?

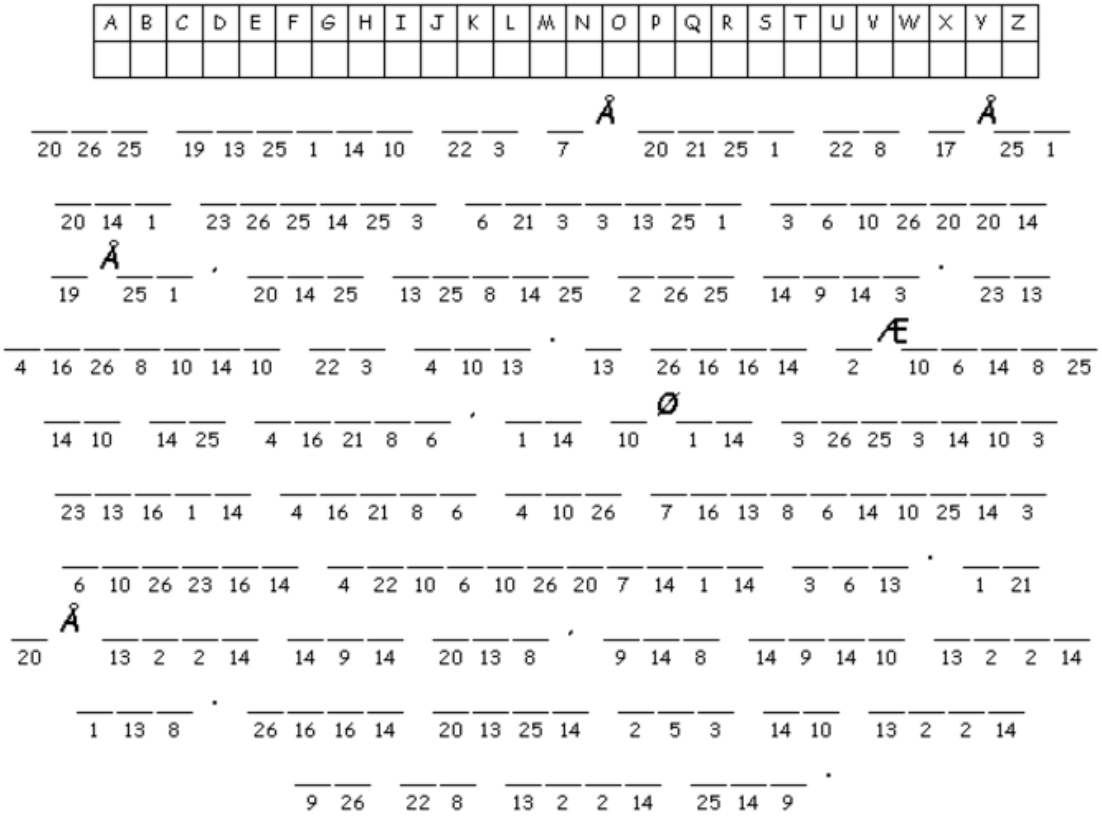
A: aha!

Q: Why did the tree get a computer?
A: Gb ybt ba

Substitutionskryptering: Blandet alfabet

Kryptogrammer er en udvidet cæsarkryptering, hvor alle bogstaver bytter plads.

Løs kryptogrammet og overvej: Om der er kryptografiske svagheder, så alle kombinationer ikke skal prøves? Hvor mange kombinationer der skal testes I et "Brute Force" angreb? (Gå eks. frem og se på kombinationsmuligheder med 1 bogstav I alfabetet, 2 bostaver, 3 bogstaver…)



Polyalfabetisk substitutionskryptering (Vigenere Cipher)

Blaise de Vigenère beskrev i 1586 en krypteringsteknik, hvor flere alfabeter kobles sammen via nøgleord . Det er en lignende teknik der blev brugt I tyskernes krypteringsmaskine "Enigma" under 2. verdenskrig. Tabellen er den enkleste form, hvor det er to alfabeter startende fra A der konbles.

Sætning	`Listen very carefully`
Nøgle: 'Allo'	`AlloAl loAl loAlloAll`
Krypteret sætning	`LTDHEY GSRJ NORPQILWJ`

Dekrypter flg. sætning der også har nøglen "allo"

`I DSOLW DOY ESWS ZYZY ZYQE`

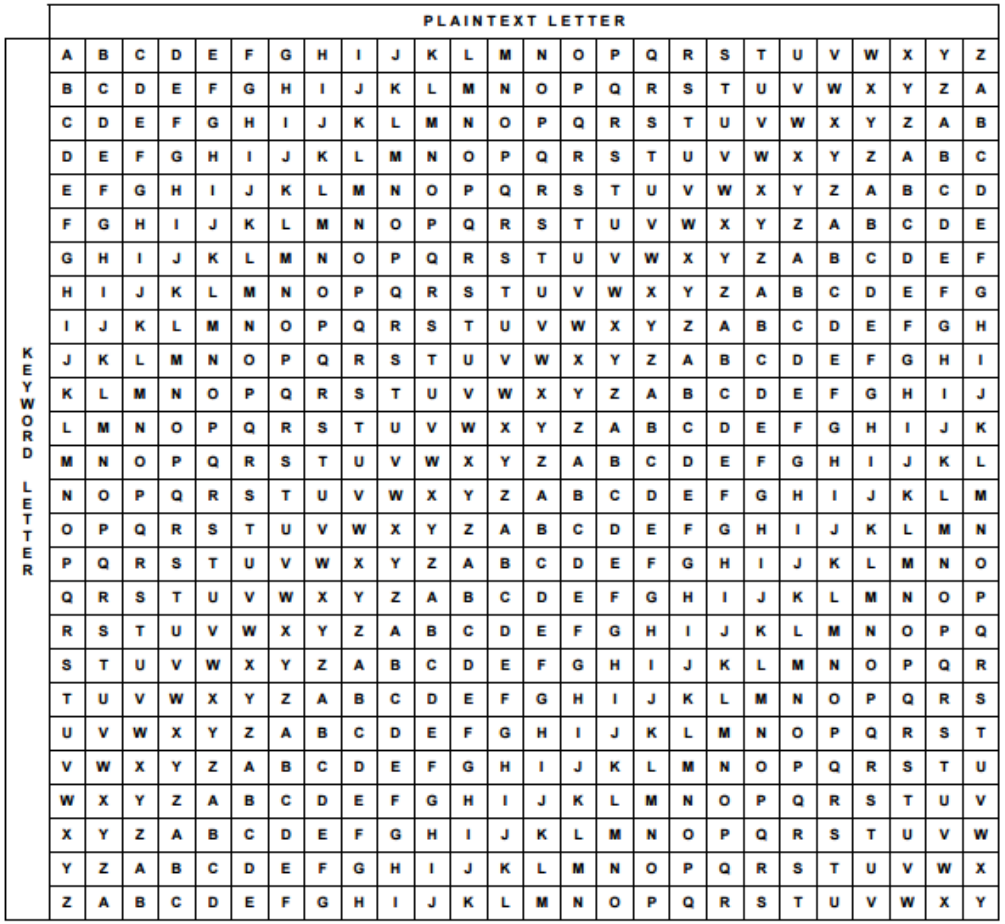
Se på den vigenere krypterede engelske tekst på flg. side:

En række gentagelse er mærket:

Hvilke hyppige engelsk ord er det mon?

>> Brug skemaet til at finde frem til nøglen.

>> Prøv at dekryptere første sætning



Polyalfabetisk substitutionskryptering (Vigenere Cipher)

UOLN TROK NELC JOK XE RJ EROY FJE. PKUI ANVIY ZO WVHL KNAZJEU, SECH EHQIGLEU **WNU** XAKPLV DAIZEEAD. YA WZHL WEGYP SRRAXALP. XUK PHZO IJ PHV UERN 1944 ! MLYH YWS YWPGANVZ SZJCV PHV JAQE TIEUDLHJ KF 1940-41. **KDE** LJIKAD EWTZKNJ DAMA IEBLZYTVZ UGKN KDE XARDWNJ CRVWT UAFVWTJ, EN FLEE XAKPLV, IAE-PO-DWN. FQR RER FBFVJSZRE YWS JARZKUJHY IADLYEU PHVER JPRVJGKD IE PHV WII **WNU** PHVER TWPRYIKU TF SAXA WRN OE PHV CRFQNU. KUI DODA FIKNKO HRRE XEVVJ UJ WN JQPVNIFNIKU IE SERLOEO AEZ MLJIKEOEO OW SAI, **WNU** LLRYEU WT FQR UESGKSRH GIAAK NEJARMAS FB TIWIEAD WEGYPIEC MVJ. TYA TZZE YWS KQREAD! **KDE** WNEV IEE KF **KDE** NKRCZ MRNCYENX POXATYAR KK VZYTFNY! Z DAMA FLHL TKNWEDVJCV EN PKUI ZEMKTZKN KK DLPY RJD JGICH IE XAKPLV. SE NELC WCTAPK JOKDIEC LVOS KDAE BUCH VZYTFNY! XKOU HUTG! AEZ LVP UJ WLC XEJAETD BCASJENX KF RHMZCHKU GFZ UGKN KDIJ CRVWT RJD EKBCA UEZEIPABENX. AIJANYKWVN.

Hvilke kryptografiske svagheder har Vigener Cipher?

Hvordan kunne systemet ovenfor forbedes væsentligt?

Hvor mange kombinationer prøves i et "Brute Force" angreb?