

# Vigenere'i šifri murdmise näide.

Ahto Buldas

## Ülesanne

Murda Vigenere'i šifri abil moodustatud krüptogramm, mille avatekst on eeldatavasti inglisekeelne:

CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQRBW  
RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK  
LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX  
VRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHR  
ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT  
AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEIBBI  
PEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHP  
WQAI IWXNRMGWOI I FKEE

(Ülesanne on võetud raamatust: Douglas R. Stinson. Cryptography: Theory and Practice. 1995.)

## Kassiski test

Sõne CHR kordub viies kohas: positsioonidel 1, 166, 236, 276 ja 286

CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQRBW  
RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK  
LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX  
VRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHR  
ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT  
AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQECCI  
PEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHP  
WQAI IWXNRMGWOI IIFKEE

Positsioonide vahed on: 165, 235, 275 ja 285.

Et  $\text{süt}(165, 235, 275, 285) = 1$ , siis võib oletada, et võtmepikkus  $m = 5$ .

## Osasõned

$Y_1$ :CVABWEBQBUAWWQRWWXANTBDPXXRDWBFAXCWMNJJFAIACNRNCATBWKDMCDCQQXWK  
 $Y_2$ :HOEITESEWOOEGMFTIFUDSTNSNVTNDPASNHESBGSEGEMRDRSHEAIEORTHNHOANOE  
 $Y_3$ :RARANOBQRASAJNVRAPT CXUGRJRUQTHLVGRLJHNGYNQRRGINRYQPVEEBRVRHIRIE  
 $Y_4$ :EHAXXPQEVKXHMKGZKSEMMIMEEVLWYXJBLZEIWMLPRJVELMRQEEKWMHTRCPIMI  
 $Y_5$ :EMTXBHRXXXBMGXLLKMGXAGLLPHTGTHFLBKKRGXHBTLMXGWHVBEAAXHKZLWWGF

Kontrolli mõttes arvutame kokkulangevuse indeksid:

$$I_c(Y_1) = 0.063, I_c(Y_2) = 0.068, I_c(Y_3) = 0.061, I_c(Y_4) = 0.072 .$$

Tulemus annab kinnitust, et oletus  $m = 5$  peab paika.

## Võtmete vahede leidmine

Arvutame omavahelise kokkulangevuse indeksid

$$I_C^g(X_i, X_j) = \sum_{h=0}^{25} f_h \cdot f'_{h-g} \approx \sum_{h=0}^{25} p_h \cdot p_{h+(k_i-k_j)-g}$$

kõigi paaride  $i \neq j$  ja kõigi nihkeväärtuste  $g = 0, 1, \dots, 25$  korral.

Kui  $g = k_i - k_j$ , siis  $(k_i - k_j) - g = 0$  ja seega

$$I_C^g(X_i, X_j) = \sum_{h=0}^{25} p_h \cdot p_h \approx 0.065 \ .$$

$i, j$	$I_C^g(X_i, X_j), \text{ kus } g = 0, 1, \dots, 25$									
1,2  $g = 9$	0.029	0.028	0.028	0.034	0.040	0.038	0.026	0.026	0.052	
	0.069	0.045	0.026	0.038	0.043	0.038	0.044	0.038	0.029	
	0.042	0.041	0.034	0.037	0.052	0.046	0.042	0.037		
1,3	0.040	0.034	0.040	0.034	0.028	0.054	0.049	0.034	0.030	
	0.056	0.051	0.046	0.040	0.041	0.036	0.038	0.033	0.027	
	0.038	0.037	0.032	0.037	0.055	0.030	0.025	0.037		
1,4	0.034	0.043	0.026	0.027	0.039	0.050	0.040	0.033	0.030	
	0.034	0.039	0.045	0.044	0.034	0.039	0.046	0.045	0.038	
	0.056	0.047	0.033	0.027	0.040	0.038	0.040	0.035		
1,5  $g = 16$	0.043	0.033	0.028	0.046	0.043	0.045	0.039	0.032	0.027	
	0.031	0.036	0.041	0.042	0.024	0.020	0.048	0.070	0.044	
	0.029	0.039	0.044	0.043	0.047	0.034	0.026	0.046		
2,3  $g = 13$	0.046	0.049	0.041	0.032	0.036	0.035	0.037	0.030	0.025	
	0.040	0.035	0.030	0.041	0.068	0.041	0.033	0.038	0.045	
	0.033	0.033	0.028	0.034	0.046	0.053	0.042	0.030		

$i, j$	$I_C^g(X_i, X_j), \text{ kus } g = 0, 1, \dots, 25$								
2,4	0.046	0.035	0.044	0.045	0.034	0.031	0.041	0.046	0.040
	0.048	0.045	0.034	0.024	0.028	0.042	0.040	0.027	0.035
	0.050	0.035	0.033	0.040	0.057	0.043	0.029	0.028	
2,5	0.033	0.033	0.037	0.047	0.027	0.018	0.044	0.081	0.051
	0.030	0.031	0.045	0.039	0.037	0.028	0.027	0.031	0.040
	0.040	0.038	0.041	0.046	0.045	0.043	0.035	0.031	
3,4	0.039	0.036	0.041	0.034	0.037	0.061	0.035	0.041	0.030
	0.059	0.035	0.036	0.034	0.054	0.031	0.033	0.036	0.037
	0.036	0.029	0.046	0.033	0.052	0.033	0.035	0.031	
3,5	0.036	0.034	0.034	0.036	0.030	0.044	0.044	0.050	0.026
	0.041	0.052	0.051	0.036	0.032	0.033	0.034	0.052	0.032
	0.027	0.031	0.072	0.036	0.035	0.033	0.043	0.027	
4,5	0.052	0.039	0.033	0.039	0.042	0.043	0.037	0.049	0.029
	0.028	0.037	0.061	0.033	0.034	0.032	0.053	0.034	0.027
	0.039	0.043	0.034	0.027	0.030	0.039	0.048	0.036	

## Lahendame võrrandisüsteemi

$$\begin{cases} k_1 - k_2 \equiv 9 \pmod{26} \\ k_1 - k_5 \equiv 16 \pmod{26} \\ k_2 - k_3 \equiv 13 \pmod{26} \\ k_2 - k_5 \equiv 7 \pmod{26} \\ k_3 - k_5 \equiv 20 \pmod{26} \\ k_4 - k_5 \equiv 11 \pmod{26} \end{cases}$$

Saame, et võti on tõenäoliselt kujul:

$$k_1, k_1 + 17, k_1 + 4, k_1 + 21, k_1 + 10 ,$$

kus liitmine toimub mooduliga 26.

Jääb üle ära arvata  $k_1$ . Seda võib juba teha proovimise teel, või isegi sagedusanalüüsi kasutades.

## Lahendus

Võti tuleb JANET ja avatekst:

THEALMONDTREEWASINTENTATIVEBLOSSOMTHEDAYSW  
ERELONGEROFTENENDINGWITHMAGNIFICENTEVENING  
SOF CORRUGATEDPINKSKIESTHEHUNTINGSEASONWASO  
VERWITHHOUNDSANDGUNSPUTAWAYFORSIXMONTHSTHE  
VINEYARDSWEREBUSYAGAINASTHEWELLORGANIZEDFA  
RMERSTREATEDTHEIRVINESANDTHEMORELACKADAISI  
CALNEIGHBORSHURRIEDTODO THEPRUNINGTHEYSHOUL  
DHAVEDONEINNOVEMBER

## Iseseisev töö

Murra järgmine inglisekeelse avatekstiga Vigenere'i šifriga krüpteeritud sõnum:

ZHQQCAQDGF'TUQGMERGWERRROHSQDROKTTHONYIAXSFK  
IZJTAGOUVTAWRKHVQUYBRSELBXHKQBBGWTTHRQDRQVO  
YHSGETXHTUHSKRUODNFUYFKEWHYELNMQYAUDQUIRBOG  
WHUQKF'KEWHYUVNAWRMQDAPLKVEXHCFHDEWADWWUWHXL  
KQOYAQEEZHQQYAXFUQAXOYRLNPWHQUI SKTWHYKRUODN  
EWOBBOGGOZWHMYEFRTDBAXOTTHRQVTAITTHKQBS