Nápovědy – II.kolo

Soutěž 2007 - druhé kolo, pokračování příběhu Štěpána Schmidta

30.09.2007
http://crypto-world.info/news/index.php?prispevek=6052&sekce=s

Soutěž 2007 - nápověda č.3

Obecná nápověda pro zadávání slov, kterými se prokazuje, že řešitel úlohu druhého kola rozluštil...

II/1: Odkud?

II/2: (4)

II/3: Hrabě?

II/4: (3)

II/5: Mezi?

(vždy je správnou odpovědí jen jedno slovo, toto slovo je obsaženo v otevřeném textu a vždy se zadává bez diakritiky a velkými písmeny)

Soutěž 2007 - nápověda č.4

06.10.2007
http://crypto-world.info/news/index.php?prispevek=6083&sekce=s

Doplňte si ...

Prosím doplňte si v článku *Štěpán Schmidt odchází do Vídně*, který byl zveřejněn 30.9.2007, následující odstavce:

Úloha II/2 (text ze starého foliantu)

Klasická šifra odolná proti frekvenčnímu luštění

Beaufortova periodická šifra, délka klíče 6

úloha II/3

Jak jsem nakonec zjistil, byla použita homofonní šifra. Na rozdíl od jednoduché substituce, kde každý otevřený znak se převádí pomocí jednoho znaku šifrové abecedy, používají

homofonní šifry pro převod některých vybraných znaků (zpravidla těch nejfrekventovanějších) více šifrových znaků. Tím se výrazně ztížilo luštění, které je založeno právě na frekvenční analýze šifrového textu. V tomto případě mi při luštění pomohlo jednak to, že se mi podařilo odhadnout některá slova z otevřeného textu a také to, že ten, kdo sestavoval tabulku pro šifrování, použil homofony jen pro 6 frekventních znaků. Nejdříve jsem si myslel, že to byly pouze samohlásky, ale nakonec jsem zjistil, že to byly 4 samohlásky a dvě frekventní souhlásky. Navíc šifrová abeceda byla sestavena nevhodně, neboť se dalo odhadnout, které znaky rozšiřují šifrovou tabulku jednoduché záměny na homofony.

úloha II/4 (dopis baronu Ignáci von Kochovi)

Klasická šifra odolná proti frekvenčnímu luštění

Vigenére-Beaufortova varianta periodické šifry, délka klíče 7

úloha II/5

Abych si to ověřil, napsal jsem mu dopis. Samozřejmě zašifrovaný. Použil jsem klasickou periodickou Vigenérovu šifru. Klíč jsem zvolil takový, aby jej mohl příjemce snadno uhodnout. Při jeho volbě jsem však přece jen zaváhal, jeho délka se mi zdála příliš krátká.

Soutěž 2007 - nápověda č.10

27.10.2007
http://crypto-world.info/news/index.php?prispevek=6231&sekce=c

V pozůstalosti Štěpána Schmidta jsem našel zašifrovaný text pomocí homofonní šifry. Údajně pocházel z císařské kanceláře. Byl označen číslem II/3.

KS4YV PJ4L5 *RUC3 -AWPV UDBZY D51I- 5QWQK HE2H1 KXC-Y C-IJK FC2RQ VFHML 3SRVH WC-I4 UDR25 -HVB- HZ*J4 HVX2* CMXCM RJ4X* R2IMH PVXM1 33RUD JCWKX CMJLI *R3BK FHVSC 45Y5M IQWLW IY-C4 RUH-A 4B3HN V5JVH CBKX* J4CMX CMR21 X4P5J 4S3L4 RZXR4 Y-XMI LVR4C L1*13 L*R2C VIJH1 *RM5V B-CZF *C*XZ LIVSK Y*X21 4B2S4 PJ4ZU C4SLV S415F 3Y*U- BC-L- 5AZQ