Vogliamo analizzare il testo criptato conl metodo di Vigénère:

YILSUIOHLSIHYADVRCFUOPYVAIOHVWJOLEAVRIXGTDUEWTTYDSTONLWGVUFLOLU
YAURHSLGDCJGIRIAEGIHHJOMIDMUGIWJGMIDLUAZXSZIWSLUSYUGTDUJAGMYFLKA
PWNGGCSVGTILMZTYDWJIMHGYITAGTIHWUKSMSJOEYKLGBCDAZOWAGIHYVGBEM
KWLALWDGMULLONU

È una stringa di 203 caratteri.

Test di Kasiski.

YILSU**IOH**LSIHYADVRCFUOPYVA**IOH**VWJOLEAVRIXGTDUEWTTYDSTONLWGVUFLOLU
YAURHSLGDCJGIRIAEG**IH**HJOMIDMUGIWJGMIDLUAZXSZIWSLUSYUGTDUJAGMYFLK
APWNGGCSVGTILMZTYDWJIMHGYITAGT**IH**WUKSMSJOEYKLGBCDAZOWAGIHYVGBE
MKWLALWDGMULLONU

Nel test di Kasiski cerchiamo gruppi di almeno due lettere che si ripetano e ne calcoliamo la distanza, ragionando che se due gruppi di lettere sono a una distanza che è un multiplo della lunghezza della parola allora essere si ripetono.

I due blocchi IOH sono a distanza 20 (contando da I a I, esclusa la prima I).

Anche i blocchi VR sono a distanza 20

I blocchi IH sono a distanza 75

È probabile che la chiave abbia lunghezza 5.

Calcoliamo **l'indice di coincidenza.**

Contiamo la frequenza di ciascuna lettera nel testo criptato composto da 203 caratteri (contati con MS Word).

A=12; B=2;C=4;D=10;E=5;F=3;G=18;H=9;I=17;J=7;K=4;L=16;M=9;N=3;O=10;P=2;
Q=0; R=4; S=10; T=9; U=14; V=7; W=11; X=2; Y=11; Z=4;

La formula ci dà :

12x11+2x1+4x3+fino a+11x10+4x3=1004 che va diviso per 203x202 ottenendo

0.048, un valore che suggerisce una successione casuale di lettere.

Se ora spezziamo la stringa in 5 stringhe diverse prendendo i caratteri che appaiono a distanza 5 abbiamo come prima stringa

YIIVOIJVTTTGOUGIGOUGUZUTGKGGZJYTKOGZIBLGO

In cui

A=0;b=1;c=0;d=0;e=0;f=0;g=9; h=0;i=5;j=2;k=2;l=1;m=0;n=0;o=0;
p=0;q=0;r=0;s=0;t=5;u=4;v=2; w=0;x=0;y=2;z=3

Che dà un indice di coincidenza di 0.08 un valore doppio circa del valore casuale ottenuto da:

9x8+5x4+2x1+2x1+5x4+4x3+2x1+2x1+3x2=69 diviso per 41x40

Ora, per cercare di individuare la parola chiave, calcoliamo la quantità M_k al variare di k.

Otteniamo i seguenti valori, per k=0,1,etc:

0.02,0.02,0.04,0.02,0.03,0.03,**0.06**,0.02,0.03,0.01,0.01,0.02,0.01,0.02,0.02,0.04,0.03,
0.03,0.03,0.04,0.04,0.03,0.01,0.01,0.03,0.01

Il valore più alto è 0.06 in corrisposndenza della lettera G che quindi supponiamo sia la prima lettera della parola chiave.

Questo andrebbe ripetuto per ognuna delle altre quattro sottostringhe.

Infine la decriptazione ci dà:

SIRACCONTACHEILPRINCIPEDICONDEDORMIPROFONDAMENTELANOTTEAVANTILAGIORNATADIROCROIMAINPRIMO
LUOGOERAMOLTOAFFATICATOSECONDARIAMENTEAVEVAGIADATOTUTTELEDISPOSIZIONINECESSARIEESTABILIT
OCIOCHEDOVESSEFARELAMATTINA

Cioè:

Si racconta che il principe di Condé dormì profondamente la notte avanti la giornata di Rocroi: ma, in primo luogo, era molto affaticato; secondariamente aveva già dato tutte le disposizioni necessarie, e stabilito ciò che dovesse fare, la mattina.

(Alessandro Manzoni, I Promessi Sposi, Cap. II)