1.-

FGVTCU FG EC FC EQFKIQ JCA WP GPKIOC

detras de ca da codigo hay un enigma

2.-

MFXYF ZS WJQTO IJXHTRZJXYT FHNJWYF QF MTWF ITX AJHJX FQ INF

hasta un reloj descomuesto acierta la hora dos veces al dia

3.-

NSYCM BOYVY CXEWO BYCOX DOBYC VYNOW KCOCS XFOXD YNOVR YWLBO

diosc reolo snume rosen teros lodem asesi nvent odelh ombre

4.-

UFQEA GZUHQ DEUPM PVQEG UFMPQ SGMPM XMVMD M

iteso unive rsida djesu itade guada lajar a

5.-

CRJDRKVDRKZTRJJFEVCRCWRSVKFTFEVCTLRCUZFJYRVJTIZKFVCLEZMVIJF

lasmatematicassonelalfabetoconelcualdioshaescritoeluniverso

6.-

MHQOQEQEXMSQZFQPQXMCGQZFQPQXMCGQZMPUQQEBQDMZMPMXMCGQTMOQOAEMECGQZMPUQBGQPQUYMSUZMD

Aveceseslagentedelaquentedelaquenadieesperanadalaquehacecosasquenadiepuedeimaginar

Código: <https://github.com/ElPala/SEGURIDAD_EN_REDES/blob/master/src/com/Palafox/CifradoCesar.java>

1.-

The ciphertxt below was encrypted using a substituttion ciper. Dexript the ciperhtext without knowledge of the key.

lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi bpr xjvn mkd ymibrut jx irhx wi bpr riirkvr jx ymbinlmtipw utn qmumbr dj w ipmhh but bj rhnvwdmbr dpr vjerykbi jx bpr qmbm mvvjudwko bj vy wkbrusurbmbwjk lmird jk xjubt trmui jx ibndt wb wi kjb mk rmit bmiq bj rashmwk rmvp yjerykb mkd wbi iwokwxwvmkvr mkd ijyr ynib urymwk nkrasshmwkrd bj ower m vjyshrbr rashmkmbwjk jkr cjnhd pmr bj lr fnmhwxwrd mkd wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwqwko ijnkdhrii ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd wkbrusurbmbwjk w jxxru yt bprjuwri wk bpr pjsr bpmb bpr riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb

Decodificado:

because the clactice of the basic colecests of data is the focu ast castelp of self is the essesce of catsubapshi lpu dalate to i shall tlp to elucitate the colecsts of the data accoltisv to cc istelcletatios baset os foltp peals of stutp it is sot as easp tasd to ekclais each colecst ast its sivsificasce ast soce cust lecais usekcclaiset to vile a cocclete ekclasatios ose koult hae to be jualifiet ast isscilet to such as ektest that he coult leach the state of eslivhteset cist cacable of lecovsidisv soustless soust ast shaceless shace i to sot teec cpself the fisal autholitp but cp ekceliesce kith data has left so toubt that the follokisv is the clocel acclicatios ast istelcletatios i offel cp theolies is the hoce that the essesce of odisakas dalate kill lecais istact

Código:

<https://github.com/ElPala/SEGURIDAD_EN_REDES/blob/master/src/com/Palafox/LetterFrequency.java>

2.-

We received th following ciphertext which was encoded with a shift cipher:

xultpaajcxitltlxaarpjhtiwtgxktghidhipxciwtvgtpilpitghlxiwiwtxgpadds

ifweallunitewewillcausetheriverstostainthegreatwaterswiththeiralood

2.1.-

Who wrote this messager?

Tecumseh's Speech to the Osages

1.- Libro Understanding Cryptography: A Textbook for Students and Practitioners: <http://swarm.cs.pub.ro/~mbarbulescu/cripto/Understanding%20Cryptography%20by%20Christof%20Paar%20.pdf>

2.- Las diferentes llaves que puede tener la maquina ENIGMA:

El Enigma básico es de 3 rotores, el cual tiene 26x26x26 = 17,576 estados posibles del rotor para cada uno de las 6 posiciones que puede tener la ruedas que dan 6x17,576 = 105,456 estados de la máquina.

Para cada uno de estos, el panel de conexión (con diez pares de letras conectadas) puede estar en 150,738,274,937,250 estados posibles.

26! / (6! 10! 2^10) = 150,738,274,937,250.