

Practice Sheet 1

Due Date: Mar 8, 2011

Q1: Given the Ciphertext;

“Nsgre fhpprffshy cebivfba bs QFY fghqrag cnpxntr, RIB fghqrag cnpxntr vf orvat vagebqhprq va beqre gb snpvvyngnr fghqragf jvgu zbovyvgl nf jryy va nqqvgvba jvgu ybj pbfg uvtu fcrrq vagrearg. Ol ninvyvat guvf snpvvyvgl, fghqragf jvyv or noyr gb npprff vagrearg naljurer veerfcrpgvir bs gurve ybpanyvgl. Va guvf ertneq, UD AHFG erdhverf lbhe srrqonpx nobhg gur cebcbfrq fghqrag cnpxntr juvpu jvyv or ng qvfpbhagrq engrf. UD AHFG jvyv sbezhyngnr n srnfvoyr naq pbfg rssrpgvir cyna juvpu jvyv or onfrq ba lbhe srrqonpx. Cynrfr pyvpx urer gb fryrpg sebz tvira bcgvbaf ol 18 Sro, 2011. Ybbxvat sbejneq sbe lbhe inyhnoyr srrqonpx ng gur rneyvrfg.”

It is known that the above ciphertext is encrypted using ROT-13 Cipher, Perform the Cryptanalysis:

Q2: Given the Message and K=6, Encrypt the following Message using Railfence Cipher:

M = “A Quick Brown Fox Jumps Over all the Lazy Dogs”

Q3: The Key for Transposition Cipher is “CRYPTOGRAPHY”, Encrypt the following Message;

M = “A Quick Brown Fox Jumps Over all the Lazy Dogs”

Q4: Given Ciphertext is;

“Xofolavd Umffcbc mk Eobjafe , a um citualomjaf aji umjeloltcjl Uaxpte mk Jalomjaf Tjohcveold mk Euocjuce aji Lcurjmfmbd JTEL, oe icioualci lm aihajuojb njmzfcibc aji citualojb elticjle oj euocjuc, aji lcurjmfmbd. Lrc umffcbc rae umxc a fmjb zad oj lrc roelmvd. Lrc epovol mk lrc ojeloltlomj rae jml urajbci mhcv lrc ec dcave. Rcvl lrc ktjiaxcjlaft ptpmecs oe lm uraffcjbcs elticjle lm vcafogc lrcov robrcel pmlcjloaf. Lrc umffcbc pvmhoice aj cjhovmjxcjl zrcvc ojlcffcul aji avl, uravaulcv aji vceofocjuc avc jtvltvci aji urcvoerci. Mtv elticjle qcumxc cyucffcl zvolcve aji umxxtjoualmve. Lrcd avc aqfc lm vcaemj uvoulouaffd oj lrc zmvfi mk Cjbojccvoj, Xalrcxaloue, Qteojcee aji Euocjuc zolr lrc aqofold lm vcaur mtl lm aff ldpce mk fcavjcve. Zc aox lm pvmituc bvaitalce zrm vcepmji zolr tjicvelajiojb aji umxpaeomj lm lrc umxpfcyold mk lrc rtaxj umjiolomje.”

It is also known that it is encrypted using the Simple Substitution Cipher, perform Cryptanalysis?