# Crypto Lab Assignment

- Submit online and bring a hard copy to the class.

- Due date: 5:30 PM, Oct, 31

- Usual file naming rules apply.

## Task 1 (5 point)

Prepare the two English texts. One is prepared by the instructor (War&Peace\_Tolstoy.txt). For the other, go to [www.nytimes.com](http://www.nytimes.com) and pick any article of your interest. Create a text file of the New York Times article by copy-paste.

- Provide a histogram showing in the graphical form the relative frequency of letters in two prepared texts.

- Provide a digram and a trigram of the textual listings in two prepared texts. For a digram and a trigram, go to Analysis \ Tools for Analysis \ N-gram.

- Provide the screen shots to answer the questions.

- Provide the link of the New York Times article.

- Do the three distributions above depend significantly on the type of text?

## Task 2 (5 point)

Take a small subset of the two texts (e.g., their first 200 letters) prepared in Task 1 and recompute the frequency distribution of single letters, digrams, and trigrams. Determine how good is the match between frequency distributions for short texts and long texts of the same type. Summarize your observations.

## Task 3 (5 points)

Encrypt the “War&Peace\_Tolstoy.txt” file using the following four classical ciphers available in CrypTool: Caesar, Vigenere, and Hill, and Substitution. Compute the frequency distribution of single letters, digrams, and trigrams for the four obtained ciphertexts. What are the characteristic features of the obtained distributions?

## Task 4 (5 points)

- Sign the “War&Peace\_Tolstoy.txt” file using MD5 and RSA.

- Verify the signature.

- Attach the screen shots.

## Task 5 (5 points)

Find three ciphertexts of *the same* message encrypted using one of the following four classical ciphers available in CrypTool: Caesar, Vigenere, Hill, and Substitution. Do your best to match each ciphertext with a cipher that could have been used to obtain the given ciphertext.

For Vigenere, you need to try different key sizes for cracking. If Vigenere is used, list the ley.

For Hill, you need to conduct known-plaintext attack. If Hill is used, obtain the key by setting the value of the first alphabet character equal to 1, and list the key.

For Substitution, you have to figure out whether the alphabet has one-to-one mapping.

All attacks must be documented. Provide the necessary screen shots.

Brute-force attacks do not count.

Ciphertext 1

Naan Cniybian'f qenjvat ebbz jnf tenqhnyyl svyyvat. Gur uvturfg

Crgrefohet fbpvrgl jnf nffrzoyrq gurer: crbcyr qvssrevat jvqryl va ntr

naq punenpgre ohg nyvxr va gur fbpvny pvepyr gb juvpu gurl orybatrq.

Cevapr Infvyv'f qnhtugre, gur ornhgvshy Uryrar, pnzr gb gnxr ure sngure

gb gur nzonffnqbe'f ragregnvazrag; fur jber n onyy qerff naq ure onqtr

nf znvq bs ubabe. Gur lbhgushy yvggyr Cevaprff Obyxbafxnln, xabja nf yn

srzzr yn cyhf frqhvfnagr qr Crgrefobhet, jnf nyfb gurer. Fur unq orra

zneevrq qhevat gur cerivbhf jvagre, naq orvat certanag qvq abg tb gb

nal ynetr tngurevatf, ohg bayl gb fznyy erprcgvbaf. Cevapr Infvyv'f fba,

Uvccbylgr, unq pbzr jvgu Zbegrzneg, jubz ur vagebqhprq. Gur Noor Zbevb

naq znal bguref unq nyfb pbzr.

Ciphertext 2

Prnc Tpzlqzce's fvpaipk gsoo apw gtesyanpn jinpxrg. Vlt liiltwt

Riiirufjvg usrmevc les cwhimdpth tjigi: pgsepe fmujetmck wkhtpy kr pke

crs ghcvpgtgv qyt cpxoe kr ile usrman gxvcni is wjmrl tjin fensckef.

Tgmnei Keskpx'w dcyvltgv, ile dipytkjjp Hgptre, eebi tq xpoe jig javltv

tq xwi aofpwschdv's griirvexrmgri; whg adve c fppl fvtws crs let fphgg

eh qakh dj hqrdv. Tji nsuvluyl nmixlg Tgmneihw Bqpzsnuopca, mrdan cw ae

fgqbi lc tays uisyiuecxe fi Eitgvhfowvv, aau eawo vltve. Ult laf ftin

oegvigh syrkrv xhg tgivksjw wkriir, crs fekrv trgkcenv hxh nqx vs tq

ecc lcvvi gcxwirkrvw, bwx drla xd wmcpa veeiexiqrh. Trkrri Vcwxpi'u wdr,

Hkteslaxt, laf gdqe ymil Mqviimcvi, ahqq wi ipxgsdwgth. Tji Pfbg Qdviq

ech mcrn stjigw hch ppsq gdqe.

Ciphertext 3

Arae Cmvvodae's beujwak eibu jof eeuqkapyu sglhixg. Vuk uogjrmt

Renelszuxt ubkvoga jof yfqrgbtex tjele: jripxe xipscecak jwquyu ix nkr

unh ctavngggr vuz apvur cn xuk fmpuap puewya gq wvvmh zuky xefovtgd.

Fecage Pnwivv'c qqhmhzel, tje vruuzipur Ukyaai, pmze gq gcxw ukr zaxukr

no buk nqoifqahoz'f cnxelgcixzenx; sfr qozr u oilh dhrmf ynh ukr vahtg

nw zain on uuasr. Nuk lkuzhlur yetvya Pdixpqfq Owygovfincn, oaswb nw yw

sczme fa tyqf qexhofynxe xe Jenelszbcea, jof yyoo bukey. Sfe bah omeh

zarlvod tuxixg vuk pdepvyhy jwnxel, ard rrcak pdraaenx qyd dob tq gq

ary havtg tctjelixtu, ocg qnpy pb azalh eypqpfvyaw. Pdixpq Ikfgye'f qov,

Uopbotype, bah paze jwtj Zornrgavg, yuum hr cnxeiqkpqd. Juk Afom Zoecb

inh zaac obukem ugq qyob kbue.

T

*(This Ciphertext 3 includes ‘T’ at the bottom.)*