ECE 8372 / CS 8352 CRYPTOGRAPHY & DATA SECURITY

Homework #1
23 Jan 2020

Professor Jim Dunham
Due: 30 Jan 2020

Read Text: Chapter 1.

1. Substitution Cipher.

   VKOEPK SPNRUIV UF PKNHPYZ APTUIV FUVIUMUWPID PIY APNRMJK HMMHWDF OI OJN WORRJIUDUHF, OJN AHPKDA, PIY OJN WKURPDH. FHP KHTHK NUFH UF PWWHKHNPDUIV. DAH IJREHN OM KPNVH SUKYMUNHF UF VNOSUIV. YPIVHNOJF AHPD SPTHF PNH EHWORUIV RONH WORROI. HGDNHRH FDONR HTHIDF PNH UIWNHPFUIV UI RPIZ PNHPF. RONH FHTHNH YNOJVADF PNH OWWJNNUIV UI ODAHNF.

2. Substitution Cipher.

   XV FGV QI HPV RNBJ QA F HGFIBJQGHFHOQI GVSQUNHOQI, XPVGV TGOSVGUVBB RFGB LVRQZV FI VBBVIHOFU ZQLOUOHK QJHOQI. OH XOUU IQH PFJJVI QSVGIODPH, LNH BVUA-TGOSOID SVPORUVB FIT RPFIDVB HQ QNG HGFIBJQGHFHOQI OIAGFBHGNRHNGV FGV RQZOID BQQIVG HPFI KQN ZODPH HPOIW.

3. Columnar Transposition Cipher (72 characters):

   ARRMN SRTML CROWN RSTVI ERRNL EEOUI ENREI EPSYH HOETL CLYRI GTTCT OAEAG SOEFE ANDHO TE

4. Columnar Transposition Cipher (88 characters):

   UWUHT AOEWO EOTOE ADTLU HZBIO NIERE EMSEH LAHLN WONAL SFSNC MRTOY ONMPS NHLLT XANWO NMAHB EIMEL PEETI BSR

5. The following enciphered message has been intercepted. Your only information about the cipher system is that it is either a substitution cipher or a transposition cipher. Can you crack the code?

   FUDNW BDCYX IQGNF UDKLL WKQKS DCGAK LOXXF YKQQE KSDFU
   KFVDF DCSGL DNFUD AUKSB GXLXO FUDLK FGXLK QOXXF YKQQQ
   DKEWD FUDEK SDAWQ SGLKF DNKND KNXLF UKFYD EGLNG LFUDB
   CDJGX WNAKQ DLVKC TDKCK LVGNF UDAXL AQWNG XLXOK QQFUD
   JKCGX WNBQK TXOON FUDAX LFDNF GNUDQ VGLKL KSDCG AKLAG
   FTAUX NDLFU CDDFX OXWCT DKCNY DOXCD UKLVW NWKQQ TKFIK
   CSIDK FUDCN GFDNX CVXSD VNFKV GWSNH

Here are URLs for some web tools which may help you solve these ciphers:

- http://wreckstorm.com/richkni/php/crypta/index.php
- http://substitution.webmasters.sk
- http://www.hanginghyena.com/solvers_a/transposition-cipher-solver