T-79.159 Cryptography and Data Security
2005 / Homework 1

1. The following ciphertext about President J.F.Kennedy was created using simple substitution:

   ```
   RGJJG MVKTO TZPGT STBGP CATJW PGOCM GJS
   ```

   What is the corresponding plaintext?

2. This ciphertext is generated using a Vigenère cipher. Use Kasiski's method to find the period.

   ```
   APWVC  DKPAK  BCECY  WXBBK  CYVSE  FVTLV  MXGRG
   KKGFD  LRLZK  TFVKH  SAGUK  YEXSR  SIQTW  JXVFL
   LALUI  KYABZ  XGRKL  BAFSG  CCMJT  ZDGST  AHBJM
   MLGEZ  RPZIJ  XPVGU  OJXHL  PUMVM  CKYEX  SRSIQ
   KCWMC  KFLQJ  FWJRH  SWLOX  YPVKM  HYCTA  WEJVQ
   DPAVV  KFLKG  FDLRL  ZKIWT  IBXSG  RTPLL  AMHFR
   OMEMV  ZQZGK  MSDFH  ATXSE  ELVWK  OCJFQ  FLHRJ
   SMVMV  IMBOZ  HIKRO  MUNIE  RYG
   ```

3. At the course homepage in "Articles" section you find a paper about mobile security systems and a GSM specification of network security functions. Using this material investigate what type of cryptographic functions are used in the GSM security system.

4. The attached page contains some ciphertext which has been obtained by encrypting the letters of some English text. The punctuation and spaces remain untouched. What is the plaintext about? Which encryption method has been used?

RIRELBAR SNZVYVNE JVGU GUR JBEYQ JVQR JRO XABJF GUNG VG VF HAQRETBVAT N NQVPNY ZRGNZBECUBFVF NAQ CEBIVQVAT ZNEIRYYBHF BCCBEGHAVGVRF SBE JRO QRIRYBCREF NAQ OHFVARFFRF GUR JBEYQ BIRE. FVZCYL CHG, KZY VF N ZRGUBQ BS CHGGVAT FGEHPGHERQ QNGN VA N GRKG SVYR. GUVF VF N FBSGJNER NPEBALZ SBE RKGRAFVOYR ZNEXHC YNATHNTR. GUR JRO VF ORPBZVAT ZHPU ZBER GUNA N FGNGVP YVOENEL. HFREF NER NPPRFFVAT GUR JRO SBE "JRO CNTRF" GUNG PNA'G OR FRRA. GUR CNTRF NER TRARENGRQ QLANZVPNYYL SEBZ VASBEZNGVBA NINVYNOYR GB GUR JRO FREIRE. GUNG VASBEZNGVBA PNA PBZR SEBZ QNGN ONFRF BA GUR JRO FREIRE, SEBZ GUR FVGR BJARE'F RAGRECEVFR QNGN ONFRF NAQ SEBZ BGURE JRO FVGRF. "FGEHPGHERQ QNGN" ERSREF GB FCERNQFURRGF, NQQERFF OBBXF, PBASVTHENGVBA CNENZRGREF, SVANAPVNY GENAFNPGVBAF, GRPUAVPNY QENJVATF, RGP. KZY VF N FRG BS EHYRF SBE QRFVTAVAT GRKG SBEZNGF SBE FHPU QNGN, VA N JNL GUNG CEBQHPRF SVYRF GUNG NER RNFL GB TRARENGR NAQ ERNQ (OL N PBZCHGRE), GUNG NER HANZOVTHBHF, NAQ GUNG NIBVQ PBZZBA CVGSNYYF, FHPU NF YNPX BS RKGRAFVOVYVGL, YNPX BS FHCCBEG SBE VAGREANGVBANYVFNGVBA/YBPNYVFNGVBA, NAQ CYNGSBEZ-QRCRAQRAPL. QRIRYBCZRAG BS KZY FGNEGRQ VA 1996 NAQ VG VF N J3P FGNAQNEQ FVAPR SROEHNEL 1998, JUVPU ZNL FRRZ YVXR VASNAG GRPUABYBTL. OHG QRYVIVAT VAGB GRPUABYBTVPNY SVYRF ZNXRF VG BOIVBHF GUNG KZY VF ABG NF ARJ NF VG NCCRNEF GB OR. ORSBER KZY GURER JNF FTZY (FGNAQNEQ TRARENYVFRQ ZNEXHC YNATHNTR), QRIRYBCRQ VA GUR RNEYL '8OF, NA VFB FGNAQNEQ FVAPR 1986 NAQ JVQRYL HFRQ SBE YNETR QBPHZRAGNGVBA CEBWRPGF. UGZY TREZVANGRQ VA 1990. GUR QRFVTAREF BS KZY GBBX CNEGF BS FTZY, THVQRQ OL GUR RKCREVRAPR JVGU UGZY NAQ PNZR HC JVGU N CBJRESHY NAQ FVZCYRE ZRGUBQ. FB GUR OVEGU BS KZY JNF NA RIBYHGVBANEL BAR. HFNTR BS FTZY VF YNETRYL SBE GRPUAVPNY QBPHZRAGNGVBA OHG KZY VF SBE GRKG SVYRF. KZY VF N ZRGN-YNATHNTR CRESRPGYL FHVGRQ GB GUR ERFCRPGVIR CHECBFR, SBE ZNEXVAT HC VASBEZNGVBA BS NAL XVAQ. VA UGZY C C266 YNCGBC OE SEVRAQYL PBZCHGRE FUBC OE $1438 V VA A K KZ ZY Y CEBQHPG ZBQRY C 266 YNCGBC/ZBQRY QRNYRE SEVRAQYL PBZCHGRE FUBC/QRNYRE CEVPR $1438/CEVPR CEBQHPG BJA GNTF, FB GURL QRFPEVOR RKNPGYL JUNG LBH ARRQ GB XABJ. LBH PNA QB QNGN CEBPRFFVAT BE QBPHZRAG CEBPRFFVAT BE OBGU NG GUR FNZR GVZR VA KZY. NCCYVPNGVBAF VA VAQHFGEVRF JVGU YBAT-YNFGVAT QNGN, RT VA GUR CUNEZNPRHGVPNYF VAQHFGEL, JURER GUR QBPHZRAGNGVBA BS QEHT BE ZRQVPNZRAG UNF GB OR NINVYNOYR SEBZ GUR SVEFG YNOBENGBEL GRFGVAT GB GUR ZNEXRG YNHAPU. VA GUR NIVNGVBA VAQHFGEL JUVPU UNF GB FGBER NAQ ZNVAGNVA VGF QBPHZRAGNGVBA BS NVEPENSG SBE QRPNQRF; SBE JRO CHOYVPNGVBA ORVAT N ZRQVHZ BS CERFRAGNGVBA JUVPU UNF GB OR NOYR GB SHAPGVBA VAQRCRAQRAGYL SEBZ GUR OEBJFRE NAQ UNEQJNER RAIVEBAZRAG HFRQ. QNGN RKPUNATR VAFGRNQ BS ZHYGVCYR QNGN RAGEL; TBVAT ORLBAQ QRCNEGZRAG NAQ PBZCNAL OBEQREF NAQ ORGJRRA PBBCRENGVAT PBZCNEAVRF; VA GUR VAGENBE VAGREARG. KZY VF NOYR GB TRARENGR RYRZRAGF JUVPU NER GNVYBE-ZNQR GB CNEGVPHYNE VASBEZNGVBA GLCRF. BAR TBBQ RKNZCYR VF NA FTZY QBPHZRAG JUVPU VF FGEHPGHERQ NPPBEQVAT GB GUR CNGGREA BS GUR QGQ, QRCRAQRAG BA GUR VAQHFGEL. HFHNYYL, RFFRAGVNY VASBEZNGVBA VF YBFG VA JRO CHOYVFUVAT FVAPR UGZY QBRF ABG CEBIVQR FHSSVPVRAG ZBQRF BS RKCERFFVBA. KZY ZNXRF GUVF VASBEZNGVBA "JRO-PNCNOYR." GUR SHGHER BS GUR JRO VF VA KZY. GUR QRPVFVIR SNPGBE VF GUNG KZY PNA OR GNVYBERQ GB GUR ARRQF BS HFREF NAQ GUR NCCYVPNGVBA CHECBFR. KZY VF ABG N FBYHGVBA OHG ENGURE N GBBY GB QRIRYBC FBYHGVBAF. &AOF.