# Criptografia y Seguridad, Tarea 1

Fecha de Entrega: Lunes 18 de febrero de 2013

1. ¿Cuántas transformaciones afines distintas hay para el alfabeto español de 27 letras? Justifique su respuesta.
2. ¿Cuántas transformaciones afines distintas hay para el alfabeto griego de 24 letras? Justifique su respuesta.
3. Utilice la transformación afin $3x + 5\ (mod\ 26)$ para cifrar el siguiente texto. Ignore los acentos y signos de puntuación:

   Siempre tengo un plan de emergencia cuando tomo algún riesgo: si todo lo demás falla, voy a morir una muerte horrible y dolorosa. En efecto, no es un buen plan de emergencia, pero es un plan.

   (Walter Slovotsky, en *El camino a casa* de Joel Rosenberg)
4. El siguiente texto fue cifrado con una transformación afín sobre el alfabeto español de 27 letras. La primer palabra es "cuando". Diga cuál fue la transformación de cifrado, y decifre el mensaje. (Sugerencia: encuentre la función inversa, que también es una transformación afín.)

   `JEBZN HAQZY BCGKH WIHTB CBJQS AHNHR HLHWG FRQLB SBLEQ RQBZV EJCHL HWQKQ VLRHL QYBSR QWWGZ HRHCB JQZNH EYRBW BNBVW`
5. Decifre el siguiente texto, que utiliza el alfabeto estándar. De ser posible, describa la construcción del alfabeto de cifrado:

   `PADTYR AT PZDGODVDT YEJCMOD OEVGDJ L YMDQGDHDJ VDT BAETRJ PRHR ORJ YE TEWVRT IDGD UAMETEJ TR JDBET TDYD DOQATDJ IEGJRTDJ JE IGEQATVDT IRG UAE OD PMETPMD TR JE OEKDTVD L OR VGMVAGD EJ IRG EJVR UAMETEJ IAEYET ETVETYEG OD GECAVDPMRT LD JDBET UAE TR EJ TEPEJDGMD L IAEYET JM DJM OR YEJEDT YEVEPVDG DO PZDGODVDT IRG JM HMJHR ORJ UAE TR IAEYET TR`

JDBGMDT OD YMCEGETPMD ETVGE OD KEGYDYEGD GEJIAEJVD L ORJ TAEKRJ YMDQGDHDJ L OEVGDJ UAE EO PZDGODVDT IGRYAPMGMD YEPODGDTYR UAE ZD YEGGRVDYR D ORJ CMORJRCRJ DAQAJVR YE HRGQDT ATD PROEPPMRT YE IDGDYRFDJ

6. Decifre el siguiente texto, que utiliza el alfabeto estándar. De ser posible, describa la construcción del alfabeto de cifrado:

BLKLI VOXLM GIZIR LHLBF MKILW FXGLZ XZYZW LZYHL IYLVM
VITRZ VOVXG IRXZW RIVXG ZNVMG VBOZF GRORA LXLMX ZHRFM
XRVMG LKLIX RVMGL WVVUR XRVMX RZVHG LBXLN KFVHG LWVUF
VIGVN VGZOV HGLBX LMHXR VMGVX LMHGZ MGVNV MGVBK FVWLH
LKLIG ZIUZX RONVM GVOLH NZHVC GIVNZ WLHXZ NYRLH ZNYRV
MGZOV HVHGL HHLMS VXSLH JFVKZ IGRVM WLWVO ZRIIV UFGZY
OVKIL KLHRX RLMWV JFVMR MTFMH VIKFV WVXIV ZIFMH VINHK
VIUVX GLJFV VOIVW FXVEF VHGIZ GLMGZ GVLIZ ZOZMZ WZ