IV054 Coding, Cryptography and Cryptographic Protocols
2020 - Exercises IV.

1. *(4 points)* Decrypt the following cryptotexts:
   (a) `AAAAB AAAAA AAABA ABBBA ABBAB AAABA ABAAA ABBBB AABBB AABAA BAAAB`
   (b) ALERTED SHRILLNESS
   (c) `EPVQS CHXUL TAOAV DFLDY AAHSS OFLMS`
   Hint: FOUR SQUARE

2. *(2 points)* Consider the affine cryptosystem with parameters $a = 7$ and $b = 19$.
   (a) Encrypt the message `AFFINE`.
   (b) Decrypt the cryptotext `HTVPTI`.

3. *(3 points)* What is the number of possible keys and the unicity distance of an affine cipher if the following modulus is used:
   (a) 30
   (b) 31

4. (a) *(6 points)* Consider a secret key cryptosystem with $P = C = \{0, \ldots, n-1\}$, where n is a prime. Further assume that encryption functions are chosen uniformly. Decide whether the cryptosystem is perfectly secure, if the encryption function is given by:
      i. $c = ax \mod n$, with $a \in \{1, \ldots, n-1\}$;
      ii. $c = x + b \mod n$, with $b \in \{0, \ldots, n-1\}$;
      iii. $c = ax + b \mod n$, with $a \in \{1, \ldots, n-1\}$ and $b \in \{0, \ldots, n-1\}$.
   (b) *(2 points)* Consider a cryptosystem with $|P| = |C| = n$. What is the smallest number of encryption functions $|K|$ that can achieve perfect secrecy? Justify your answer.

5. *(4 points)* Alice needs to send three binary messages, w_1, w_2 and w_3, of length n, to Bob using one-time pad. However, they share only one key k of length n. She decides to encrypt the messages in the following way:

$$c_1 = w_1 \oplus w_2 \oplus w_3 \oplus k,$$
$$c_2 = w_2 \oplus w_3 \oplus k,$$
$$c_3 = w_3 \oplus k$$

   and sends the cryptotexts c_1, c_2, c_3 to Bob.
   (a) Show how Bob can recover all three messages.
   (b) Malicious Eve have intercepted all three cryptotexts. What information about the messages can Eve recover?

6. *(4 points)* Break the following cryptotext produced by the Vigenère cipher. Find the key length, the key and decipher the cryptotext. Explain your reasoning.

```
UACVL GVWUN CVETM QUCGT RPMAO UWYJM UHFMH FPTGV RGKEV IQBPR NEUIR HBBVW YRGJB EOEEC
YEZKJ MEXNG CQTPJ QNRLO PHLFK ITAIL SQUEW ZXJMH PAJNP SSYVA ILDJM NOMIT RWXNU WZMGP
GMEEY VHCET SIGIS EEVPC RYUXH XNFPP RGYDE ILHFX TTKLG WILCP PPRPG CFEMO MCRHK SPEYB
NUBPT NIPMI XTIWP NKYTR WAEOM NHFPC KSXXB GTNVH DTBUA HYDEO XGGSB VFHZT VWKGT AENYL
NKMOX HBSUY NHEMS NEPAT CYDVT GGDXN UFJDZ WEHVX RFXMY WVKXD KIDBH ICLGE MDATC DKZET
XTBRF XZFWM EXRBN UBPPI YULIT NBLXY VZGKS BNDYH HVRJX PNBMC DHVHJ BSVRZ JEAEE NRTBC
CLPAB XJKON GICYD ZIIXH XINMN HIMHM EGUOX OIVHG VHBFG LTRBY PLTLE DLPTN VKMIG GBHOT
YICKT HFEYN IGLGK IGGUB PTVGJ GIJUF BLSSI GGKGO XHLSK LGDAL ITETT VWVTN WBBVM AXIUV
```

More on next page >>>

OGTSC MUKMQ GHTSC YPNCE TZEEY JAYOI IFTNW WISOI UFCUB TGFZL ICXQI UULJW TZVLK LCKAD
ETNXS HLUVH BPTTR PEBPA ESBPC VVVTI GLZBL DRLCU IMOGH ZTWMP BSAIO AARFN GVTLA OXYOK
TWULB SICYG YMUWI LCPPP RZIUP HBCIG TGYXU NGZET NEHRX VAILI TDFSK SPXMH RFYIA DTNXO
YHJMW ATOCW ABSJW LLRXV BTNDF BZWVZ GKTAE SYTSR RCETX ROUEI MIGQP EAOUE IFRJB SWITW
ZVVVA HCVUS LPDJS QGAYT FLEHV SWMBK EBEZF KLGVR BMFUY WRVCG DHNFN SEFVA BSMHB NTTXE
XXTAE CLTTZ WJTCE EBLLD MEPMA ZEPPP RKLGB RKUTM TAEIP XMRIU CDQLM VXPHS TCMLV XJTTU
RJNTS YMPME ELJAP NTIFX MTNEY OTYEV UAUBB APKVI RAILW PLVSV GTXTM HVMAR FZKWI GGUBP
MNMVA AGIOY JERVJ XAWSU UCTFZ GKTAE SYDTF JVAEP OSFOI WXJBS PATNS ETEUX TAEOC EWFYN
WFBTJ HHIKL VAEEO OADTR RFBNZ TSUOI KMQGO YHVMS IEKWI CHDFV CEROK GGTCI CPVVQ GGTLI
ONSEZ RVXRX SUMZF EEVBO GAMMP CLVKM YTPSU NTZGG MHTTI UDCFR VBNNE ECYTF XJXTP EONTE
KLEXN MUSSD IDSPL IGGIN SETSF XBHOL