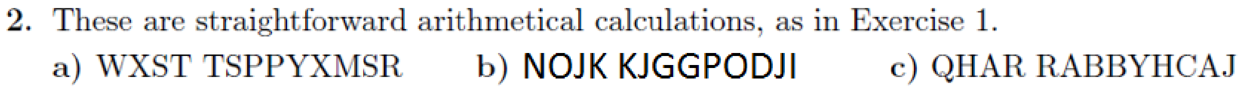
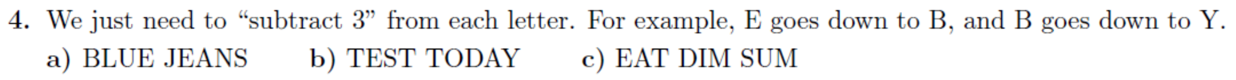
Training Problems #4 – Solutions

Exercises from Section 4.6 (page 304):



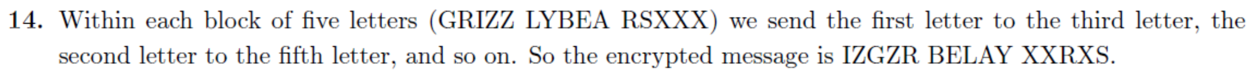
2. These are straightforward arithmetical calculations, as in Exercise 1.

a) WXST TSPPYXMSR b) NOJK KJGGPODJI c) QHAR RABBYHCAJ

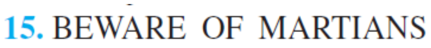


4. We just need to "subtract 3" from each letter. For example, E goes down to B, and B goes down to Y.

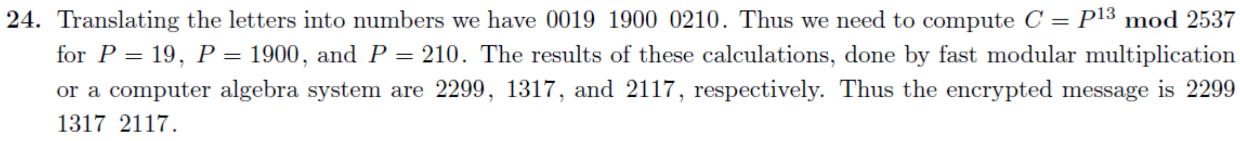
a) BLUE JEANS b) TEST TODAY c) EAT DIM SUM



14. Within each block of five letters (GRIZZ LYBEA RSXXX) we send the first letter to the third letter, the second letter to the fifth letter, and so on. So the encrypted message is IZGZR BELAY XXRXS.

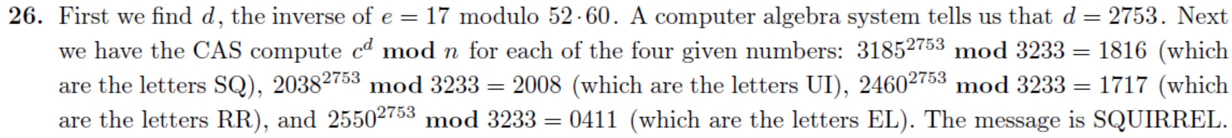


15. BEWARE OF MARTIANS



24. Translating the letters into numbers we have 0019 1900 0210. Thus we need to compute $C = P^{13}$ **mod** 2537 for $P = 19$, $P = 1900$, and $P = 210$. The results of these calculations, done by fast modular multiplication or a computer algebra system are 2299, 1317, and 2117, respectively. Thus the encrypted message is 2299 1317 2117.

26 - you can do it only for the first block, 3185, if you like.



26. First we find d, the inverse of $e = 17$ modulo $52 \cdot 60$. A computer algebra system tells us that $d = 2753$. Next we have the CAS compute c^d **mod** n for each of the four given numbers: 3185^{2753} **mod** $3233 = 1816$ (which are the letters SQ), 2038^{2753} **mod** $3233 = 2008$ (which are the letters UI), 2460^{2753} **mod** $3233 = 1717$ (which are the letters RR), and 2550^{2753} **mod** $3233 = 0411$ (which are the letters EL). The message is SQUIRREL.

i) Suppose that the ciphertext HKTGZX LXXWL FTDX HKTGZX MKXXL was produced by encrypting a plaintext message using a shift cipher. What is the original plaintext?

Answer: Shift key is 19. Decrypted text is:

ORANGE SEEDS MAKE ORANGE TREES

Instructor: Ali Sharifian