MATC16 Cryptography and Coding Theory
Gábor Pete
University of Toronto Scarborough
gpete at utsc dot utoronto dot ca

Solutions for Assignment 1

The solutions below are sometimes sketchy, skipping computational details.

Problem 1. What is $49^{-1} \pmod{50}$? And $\pmod{700}$? And $\pmod{701}$? **(3 pts)**

Solution. $49 = -1 \pmod{50}$, and $1^{-1} \equiv 1$, hence $49^{-1} \equiv (-1)^{-1} \equiv -1 \pmod{50}$. Since $\gcd(49, 700) = 7$, the inverse $\pmod{700}$ does not exist. Finally, the extended Euclidean algorithm for $49x + 701y = 1$ gives $x \equiv 49^{-1} \equiv 186 \pmod{701}$.

Problem 2. Show that if $\gcd(a, n) = 1$ and $a \mid mn$, then $a \mid m$. **(2 pts)**

Solution. Since $\gcd(a, n) = 1$, the prime factors of a and n are all different. But $a \mid mn$ means that all the prime factors of a can be found in the factorization of mn, with at least as large exponents as in a. All these factors must come from m, so $a \mid m$.

Another proof. Since $\gcd(a, n) = 1$, there exist x, y with $ax + ny = 1$. Then $max + mny = m$. Since both terms on the left are divisible by a, the right side must be divisible, too.

Note that $a \nmid n$ and $a \mid mn$ together do not imply that $a \mid m$. For instance, $6 \mid 12$ and $6 \nmid 4$, but $6 \nmid 3$.

Problem 3. Find all integer solutions (x, y) to $1234x + 5678y = 910$. (Do not forget to argue that those you have found are all the ones.) **(4 pts)**

Solution. By the extended Euclidean algorithm, $\gcd(1234, 5678) = 2$ and for $1234x' + 5678y' = 2$ we get a solution $(x'_0, y'_0) = (704, -153)$. Then $(x_0, y_0) = 455 \cdot (x'_0, y'_0) = (320320, -69615)$ is a solution to the original equation. Now, if (x_1, y_1) is another solution, then $1234(x_0 - x_1) + 5678(y_0 - y_1) = 0$, so $617(x_0 - x_1) = 2839(y_1 - y_0)$. By divisibility, this means that $y_1 - y_0 = 617k$ and $x_0 - x_1 = 2839\ell$, and then obviously $k = \ell$. So, all solutions must be of the form $(x_1, y_1) = (x_0 - 2839k, y_0 + 617k)$, $k \in \mathbb{Z}$, and all of these are obviously solutions.

Another way of saying the same thing is that by a Corollary we had on class, any solution x_0 must be $\equiv 455 \cdot 704$ or $\equiv 455 \cdot (704 + 2839) \pmod{5678}$, which gives two infinite families for x_0 with step-size 5678 each, or one family with step-size 2839, as you wish. Then the corresponding y_0 can be found from the original equation.

Problem 4. Suppose a language has only 3 letters, a, b, c, with frequencies .7, .2, .1, and not much dependence between neighbouring letters in a typical text. The ciphertext "ABACABCBBB" is encrypted with Vigenère (mod 3). You are told that the keyword length is 1,2, or 3. What is the most probable keyword? **(2 pts)**

Solution (3pts). If you displace the ciphertext by 1,2,3 letters, you find 2,4,2 coincidences between the letters, respectively. Hence 2 looks like the length of the keyword. At the odd places we see AAACB, so the letters A,B,C should correspond to a, b, c, which means a shift of 0, or code-letter **a**. At the even places we see BCBBB, so A,B,C should correspond to c, a, b, which means a shift of 1, or code-letter **b**. Hence the codeword should be 01 or **ab**, meaning the same.

Problem 5. Alice regularly sends quotations from her favorite Zen master Shunryu Suzuki to Bob, always encrypted with a Hill cipher, using the same 3×3 matrix (mod 26). Eve has been following the messages for a while, and since "BKJDBC" and "SSFUSY" are the two most frequent segments in the ciphertexts, she guesses that the first stands for "Buddha" and the second for "Suzuki".

(a) What is the key matrix used by Alice? **(1.5 pts)**

(b) What does the ciphertext "WNA TAU CEL LUC SLS SPE SYK NSY NSZ OSR THO TWK VCQ WNU NOW IDP AHI ANP EZH AHI" mean? (This is a bit long to do by hand, so if you get bored, then either use a computer program (Mathematica, Maple, Matlab, C) to do the matrix multiplications, or just decode the first few words.) **(1.5 pts)**

Solution. $buddha = (1, 20, 3, 3, 7, 0)$ maps to $(1, 10, 9, 3, 1, 2)$ and $suz = (18, 20, 25)$ maps to $(18, 18, 5)$. These give the following equation for the key matrix M:

$$\begin{pmatrix} 1 & 20 & 3 \\ 3 & 7 & 0 \\ 18 & 20 & 25 \end{pmatrix} M = \begin{pmatrix} 1 & 10 & 9 \\ 3 & 1 & 2 \\ 18 & 18 & 5 \end{pmatrix} \pmod{26}.$$

The determinant of the first matrix is -1523, which is relative prime to 26, so can invert, so can solve this equation, giving

$$M = \begin{pmatrix} 1 & 2 & 4 \\ 0 & 3 & 6 \\ 0 & 0 & 5 \end{pmatrix} \pmod{26}.$$

The inverse of this is the decrypting matrix:

$$M^{-1} = \begin{pmatrix} 1 & 8 & 0 \\ 0 & 9 & 10 \\ 0 & 0 & 21 \end{pmatrix} \pmod{26}.$$

Then WNA= $(22, 13, 0)$ multiplied by M^{-1} is $(22, 7, 0)$ (mod 26), and so on, giving the plaintext "What we call 'I' is just a swinging door that moves when we inhale and exhale."

Problem 6. An LFSR sequence generated by a length 3 recurrence starts 001110. What is the next element of the sequence? **(2 pts)**

Solution. We have a recursion $x_{n+3} = c_0x_n + c_1x_{n+1} + c_2x_{n+2} \pmod 2$, which maps 001 to 1, 011 to 1, and 111 to 0. Hence

$$\begin{pmatrix}0 & 0 & 1\\ 0 & 1 & 1\\ 1 & 1 & 1\end{pmatrix}\begin{pmatrix}c_0\\ c_1\\ c_2\end{pmatrix} = \begin{pmatrix}1\\ 1\\ 0\end{pmatrix} \pmod 2 .$$

This has the unique solution $(c_0, c_1, c_2) = (1, 0, 1) \pmod 2$, hence the recursion is $x_{n+3} = x_n + x_{n+2}$, and the next element is 1+0=1.

Problem 7. Consider an Enigma machine with 3 rotors with known wirings and with a plugboard with 6 pairs of plugs. (See Section 2.12 in the book.)

(a) In the computation of the size of the keyspace, the book has a factor 100391791500 corresponding to the 6 pairs of plugs. Why is this the correct number? **(2 pts)**

(b) Does Enigma have Shannon's diffusion and confusion properties? **(2 pts)**

Solution (a). There are 12 numbers to choose what to connect with the plugs, this can be done in $\binom{26}{12}$ ways. Then out of this 12, we can choose the first pair to connect in $\binom{12}{2}$ ways, then the next pair in $\binom{10}{2}$ ways, and so on. But in reality there's no distinguished "first", "second" and so on plug, only in our counting above, so we have to divide by 6!. Altogether,

$$\frac{\binom{26}{12}\binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}\binom{4}{2}\binom{2}{2}}{6!} = 100391791500.$$

Another way to count is to first choose the first pair out of the 26 to connect, then the second pair out of the remaining 24, and so on, and finally divide by the same 6! as above:

$$\frac{\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}\binom{16}{2}}{6!} = 100391791500.$$

Solution (b). It does have confusion, since each letter is encrypted using the entire key: we are composing several permutations which are determined by the initial setting of the rotors and by the setting of the plugboard (and by the position of the letter that tells how much the rotors have moved since the initial setting).

It does not have diffusion, since the k^{th} letter of the ciphertext depends only on the k^{th} letter of the plaintext (and on the key, of course).

(Max possible score: **20 pts**)