Senior Math Circles – Cryptography and Number Theory Week 1 Solutions

Dale Brydon

These are not necessarily full solutions, but should convey the idea of how to solve all the problems. Use at your own risk.

1. (a) VUFJIOBYZJIRT.
   (b) PERFECTSECRECY.

2. (a) 1.
   (b) 2.
   (c) $-37(50) + 23(18) \equiv (3)(2) + (-1)(2) \equiv 4 \pmod 8$.
   (d) 3. (The remainder of any number mod 10 is simply its last digit.)
   (e) $2 \equiv -1 \pmod 3$ and so $2^{2014} \equiv (-1)^{2014} \equiv 1 \pmod 3$.

3. We know that if k is divisible by 9, then
$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10^1 + a_0 \cdot 10^0 \equiv 0 \pmod 9.$$
   We also know that $10 \equiv 1 \pmod 9$. Hence,
$$\begin{aligned} 0 &\equiv a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10^1 + a_0 \cdot 10^0 \\ &\equiv a_n \cdot 1^n + a_{n-1} \cdot 1^{n-1} + \cdots + a_1 \cdot 1^1 + a_0 \cdot 1^0 \\ &\equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 9, \end{aligned}$$
   which shows the sum of the digits is also divisible by 9.

4. (a) Since the ciphertext is just the message plus the key, to get k from c and m we just subtract m from c. So $k = c - m$, i.e. $k_0 = c_0 - m_0,\ k_1 = c_1 - m_1, \cdots,\ k_n = c_n - m_n$.
   (b) COMPLETELYRANDOM.
   (c) We just saw that for every ciphertext-message pair, there is a key that encrypts the message to that ciphertext. So, given just a ciphertext, there is a key that would decrypt it to any possible plaintext. That is to say that any message of the appropriate length could possibly have produced the ciphertext. Further, by choosing a random key, it means that all messages are equally likely.

5. (a) The key used to encrypt c_2 can be computed as $k = c_2 - m_2$. Since the same key has been used for both messages we can find m_1 by computing $c_1 - k$.

   (b) Computing $k = c_2 - m_2$ and $m_1 = c_1 - k$, we see that $m_1 =$ "ATTACK".

   (c) Since $c_1 = m_1 + k$ and $c_2 = m_2 + k$, $c_2 - c_1 = m_2 - m_1$ and so does not depend on the key whatsoever. While the resulting string is still scrambled, it is far from totally random, as both c_1 and c_2 by themselves are.

   (d) The two words are "CRYPTOGRAPHY" and "SATISFACTION." While there are a few ways to solve this problem I will outline two. The first step in any approach is to subtract one ciphertext from the other, as noted in part (c). One option is then to use a computer to see which pairs of 12-letter words could produce this difference. There are only around 12000 12-letter English words and so with some small optimizations, possible pairs of words can be tested in under a second.

   The second method can be done by hand or with the aid of a computer. The key thing to note is that if, for example, "C" is the first letter of the first word, then we know that "S" must be the first letter of the second word. By trying out possible first 2- and 3-letter combinations, we can quickly see that there are only a few possibilities for the first few letters of each word. For example, with theses ciphertexts, there are only 62 possible combinations of 2-letter beginnings where both beginnings start 50 or more English words.