MATH 233 SPRING 2017
SOLUTIONS TO MIDTERM PRACTICE

Classical ciphers

- An affine-like cipher given by $c \equiv \alpha x + \beta \pmod{26}$ (where c is the cipher and x is plaintext) encrypts the plaintext *bad* as DBH. Find another three-letter plaintext that is encrypted as DBH by this cipher.
  Solution. Since `a` encrypts as `B`, we see that $\beta = 1$. Since `b` encrypts as `D`, we see that $\alpha = 2$. Thus, adding 13 to any of the letters gives a plaintext that encodes the same way. So we can replace `a` with `n`, `b` with `o`, and `d` with `q`. So, for example `onq` encrypts the same way as `bad`; as does `oad`.

- Alice and Bob are sending messages using an affine cipher. You gain access to the plain text `if` and its corresponding ciphertext `IZ`. You then intercept the ciphertext `XAP`. What was the corresponding plaintext?
  Solution. If the cipher is written as $x \mapsto \alpha x + \beta \pmod{26}$, then we must have $8\alpha + \beta = 8$ and $5\alpha + \beta = 25$, so subtracting gives $3\alpha \equiv -17 \pmod{26}$, so $\alpha = 3$. That means that $\beta = 10$. That means that to *decrypt* we send x to $9x + 14$. We see then that `XAP` would decrypt as `not`.

- Alice and Bob are sending messages using an affine cipher, and you intercept the ciphertext `LQHUH`. You gain access to the *decryption* machine, and when you input the ciphertext `AB` the machine outputs `ch`. What is the plaintext corresponding to the intercepted ciphertext?
  Solution. Since *decryption* takes `AB` to `ch`, we must decrypt by sending x to $5x + 2$. Thus, `LQHUH` decrypts to `felyl`

- Suppose that we know a cipher is either an affine cipher or a 2×2 Hill block cipher or a Vignère cipher with a keyword of length 2. It encrypts *aarons* as $BESSOW$. (You do not have to find the key, just give a convincing explanation of why it must be one of the ciphers or why it must not be either of the others.)
  Solution It cannot be a 2×2 Hill block because if it were, then `aa` would be encrypted as `AA`. It cannot be affine because `a` encrypts in two different ways. Thus, it must be Vignère. In fact, it is not too hard to see that it is Vignère with keyword `be`.

- Suppose that we know a cipher is either an affine cipher or a 2×2 Hill block cipher or a Vignère cipher with a keyword of length 2. It encrypts `abba` as as `BBBA`. (You do not have to find the key, just give a convincing explanation of why it must be one of the ciphers or why it must not be either of the others.)
  Solution It cannot be affine because it encrypts `a` differently on the first and last letters. If it was Vignère, it would have to be keyword `ba`, but that does not work, so it must be a Hill block cipher. In fact, one can check that the matrix is $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ since that sends $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ to $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ to $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

- Suppose that we know a cipher is either an affine cipher or a Vignère cipher with a keyword of length 2. It encrypts *back* as $EBHF$. (You do not have to find the key, just give a convincing explanation of why it must be one of the ciphers or why it must not be the other.)
  Solution This cannot be a Vignère cipher with a keyword of length 2 because the only possibility would be `db` and that does not work on the last letter, clearly. So it must be affine. We see easily that in fact it is affine with $\alpha = 3$, $\beta = 1$.

- Suppose that we know that Alice and Bob are using either an *affine* cipher or a *Vigenère* cipher with key size 2. The plaintext aqua is decrypted as XVRG. Which sort of cipher is being used? (You do not need to find the key; just give a convincing explanation.)
  Solution. If it was encrypted with a *Vigenère* cipher with key size 2, the only possible keyword would be xg since the first a goes to X and the fourth letter, also an a, goes to G. But then q would go to W, not to V. So it must be a Hill cipher with key size 2.

- Suppose that we know that Alice and Bob are using either a *Vigenère* cipher with key size 2 or a *Hill* cipher with a 2 × 2 key matrix. The plaintext aardvark is decrypted as AAXRVQLM. Which sort of cipher is being used? (You do not need to find the key; just give a convincing explanation.)
  Solution If it was a *Vigenère* cipher with key size 2, then the keyword would have to be aa, but that does not work for the other letters, so it must have been encrypted with a Hill cipher.

- Same as above, but if the ciphertext had been CKTNXKTU.
  Solution. Any Hill cipher of size 2 must send aa to AA, since it is linear and aa corresponds to the zero vector. So this must be *Vigenère*. We can see that the key word must be *ck*.

- Suppose that we have an alphabet with two letters b and a. The frequency of b is .9 and the frequency of a is .1. We see the ciphertext

  $$ABABABABAA$$

  What was the likely keyword? Explain your answer. (You may assume the keyword length is not longer than 3.)
  Solution. We get many more incidences with a shift of two than with a shift of 1 or 3, so it should be a keyword of length 2. Based on frequencies, it is probably ba.

- Suppose that we devise an encryption scheme as follows. First we take our plaintext and encrypt it using a Vignère cipher with keyword ai. Then we take the output of that and encrypt it *again*, this time using a Vignère cipher with keyword *epa*. The cipher we obtain in this way is equivalent to a single Vignère cipher. What is the keyword for this single Vignère cipher? (Hint: You might begin by trying to figure out what the length is. Another hint: The beginning of this keyword is a word that is especially relevant this week.)
  Solution. We see that the cipher we obtain this way will repeat after six letters since six is the smallest number divisible by three and two. Now all we have to do is see what happens to aaaaaa. It encrypts under the first Vignère as aiaiai. The second Vignère then encrypts this as exampi. (exam, then everyone's favorite mathematical constant.)

Modular arithmetic

- Does 20 have a square root mod 57? If so, how many does it have (Some facts: (a) 57 factors as $3 \cdot 19$, (b) 20 is equivalent to 1 mod 19 and 2 mod 3, (c) $19 - 6 \cdot 3 = 1$).
  Solution. Since 2 is not a square mod 3, there are no square roots of 20 modulo 57.

- Does 39 have a square root mod 57? If so, how many does it have? (39 is equivalent to 1 mod 19 and 0 mod 3).
  Solution. There must be two since 1 has two square-roots modulo 19 and 0 has one square root modulo 3. In fact, we see that 39 must square to 39. The other square root is -39 which is 18.

- Does $x^2 \equiv 8 \mod 13$ have a solution? Show your work. (Do it by checking all possibilities only if you have to – there is a better method that would work on larger primes.)
  Solution. A necessary criteria for a to have a square root is that $a^{(p-1)/2} \equiv 1 \pmod{p}$. Since $p = 13$ in this case we need to calculate $8^6 \equiv -1$ which shows that 8 has no square root modulo 13.

- Find a positive integer x less than 11 such that $5^{322} \equiv x \pmod{11}$
  Solution. Since $\phi(11) = 10$, we obtain that 5^{320} is 1 modulo 11, by Fermat's little theorem (or Euler's theorem). So we obtain 5^2 modulo 11 which is 3 modulo 11.

- Let ϕ be the usual Euler ϕ function. Find $\phi(12)$.
  Solution. Since $\phi(4) = 2$ and $\phi(3) = 2$, we obtain 4. We might also note that these correspond exactly to 1, 5, 7, and 11.

- True or false and explain: $a^{\phi(12)+1} \equiv a \pmod{12}$ for all positive integers a. (Hint: It is enough to check things modulo 3 and 4 by the Chinese remainder theorem.)
  Solution. When we check modulo 4, we see that in fact 2^5 is 0 modulo 4 not 2 modulo 4, so this must be false. (It actually works fine modulo 3.)

- How many integers n with $0 \leq n < 100$ are there with the property that $\gcd(100, n) = 1$? Explain your answer.
  Solution. This is just $\phi(100)$ which is $20 \cdot 2$ (from $(5^2 - 5) \cdot (2^2 - 2)$), so 40.

- Calculate $d = \gcd(341, 1043)$ and find integers x, y so that $d = 342x + 1043y$ (Bézout identity).
  Find all of the solutions of $341x = 1 \pmod{1043}$. **Solution.** We use the Euclidean algorithm.
  $$1043 = 342 \cdot (3) + 17$$
  $$342 = 17 \cdot (20) + 2$$
  $$17 = 2 \cdot (8) + 1$$
  Unwinding this gives
  $$1 = 17 - 2 \cdot (8) = 17 - (342 - 17 \cdot 20) \cdot 8$$
  $$= 17 \cdot 161 - 342 \cdot 8 \qquad = (1043 - 342 \cdot 3) \cdot 161 - 342 \cdot 8) = 1043 - 491 \cdot 342$$
  The inverse of $342 \equiv -491 \equiv 552 \pmod{1043}$ which solves the congruence equation. There is only one solution.

Odds and ends

- Suppose the function f is defined by
  $$f(00) = 0; \quad f(01) = 1; \quad f(10) = 1; \quad f(11) = 0.$$
  True or false and explain: we have $f(a \oplus b) = f(a) \oplus f(b)$ for all a, b (where a and b are each two bits).
  Solution. Yes, this is **true**. We first note that since $f(00) = 0$, we have $f(00 \oplus b) = f(00) \oplus f(b)$ for all b. Then, checking through $f(a \oplus b)$ where a, b range over 01, 10, and 11, we see that $f(a \oplus b) = f(a) \oplus f(b)$ for all a, b.

- Suppose the function f is defined by

  $$f(00) = 1; \quad f(01) = 0; \quad f(10) = 1; \quad f(11) = 0.$$

  True or false and explain: we have $f(a \oplus b) = f(a) \oplus f(b)$ for all a, b (where a and b are each two bits).

  Solution. This is **false**. For example $f(10 \oplus 11) = f(01) = 0$ but $f(10) \oplus f(11) = 1 \oplus 0 = 1$. There are several other examples too.

- In an attempt to increase security, Bob decides to double encrypt his message by using one affine cipher to encrypt, then another affine cipher to encrypt a second time. First, he encrpyts by sending x to $3x + 1$. For the second cipher he encyrpts by sending x to $5x + 11$. This turns out to be exactly the same as doing a single affine cipher encryption of $x \mapsto \alpha x + \beta$ for what α and β (each between 0 and 25)?

  Solution. Let us write the first encryption as f and the second as g. Then

  $$g(f(x)) = g(3x + 1) = 5(3x + 1) + 11 = 15x + 16$$

- In an attempt to increase security, Alice decides to double encrypt her message by using a one Vignenère cipher to encrypt, then another Vignenère cipher to encrypt a second time. For the first cipher she encrpyts with keyword *cat*. For the second cipher, she encpryts with keyword *dog*. This is the same as doing a single Vignenère cipher encryption with what three-letter word (note, the three letters you get might not be real English word).

  Solution. Since c corresponds to 2, a corresponds to zero, t corresponds to 19, and d corresponds to 3, o corresponds to 14, g corresponds to 6, we see that key word corresponds to 5 then 13 then 25 so the key word is foz.