MATH 233 SPRING 2018
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.
- How many distinct, invertible affine ciphers are there for English? How is this related to $\phi(26)$? What does $\phi(26)$ represent?
- 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?
- 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?
- 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.)
- 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.)
- 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.)
- 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.)
- 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.)
- Same as above, but if the ciphertext had been `CKTNXKTU`.
- 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.)
- 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.)

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) $19 - 6 \cdot 3 = 1$).

- 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).

- 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.)
- Find a positive integer x less than 11 such that $5^{322} \equiv x \pmod{11}$

- Let ϕ be the usual Euler ϕ function. Find $\phi(12)$.

- 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.)

- How many integers n with $0 \leq n < 100$ are there with the property that $\gcd(100, n) = 1$? Explain your answer.

- Calculate $d = \gcd(341, 1043)$ and find integers x, y so that $d = 342x + 1043y$ (Bézout identity). Find all of the solutions of $341x = 1 \pmod{1043}$.

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).

- 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).

- 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)?

- 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 encprvts 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).