Exam 2 Solution

Date and time: April 11, 2018, 3:20 to 4:40 pm.

Instructions: The exam is **closed book** and consists of **4 problems + 1 bonus problem**. Make sure you write your name and NetID on the paper. Show all your work, you will not receive full credit if your answer lacks the necessary explanations. Cheating $\implies 0$.

Problem I: *(25 points)* The Vigenère cipher is a private key encrypting method that is based on shift ciphers. The method consists of repeatedly using a series of shift ciphers based on the letters of a private keyword. For example, to encrypt the word HELLO using the private keyword TO, we first replace HELLO and TO by their corresponding elements in $\mathbb{Z}_{26}$, given by $7\ 4\ 11\ 11\ 14$ and $19\ 14$, respectively. Then, we use the keyword TO repeatedly to perform the following shifts

$$\begin{array}{cccccccc} & 7 & 4 & 11 & 11 & 14 & & \\ + & 19 & 14 & 19 & 14 & 19 & & \\ \hline \equiv & 0 & 18 & 4 & 25 & 7 & (\textbf{mod}\ 26). & \end{array}$$

As a result, we would obtain the ciphertext ASEZH. The conversion table from letters to their corresponding elements in $\mathbb{Z}_{26}$ is provided below.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

1. *(10 pts)* Someone sent you the message AFS PKS TZEWM encrypted with the private keyword CRYPTO. Decrypt the message to obtain the original text.

2. *(10 pts)* You found a file named RXGRFTHT APHWG TLPA on one of the computers in Rutgers. Decrypt the name of the file knowing that the name is encrypted using a Viginère cipher with a private keyword formed of two consecutive letters.

3. *(5 pts)* When using a Viginère cipher, is it better to use a long or a short private keyword? Justify your answer.

Solution:

1. First, we replace AFS PKS TZEWM and CRYPTO by their corresponding elements in $\mathbb{Z}_{26}$, given by $0\ 5\ 18\ \ 15\ 10\ 18\ \ 19\ 25\ 4\ 22\ 12$ and $2\ 17\ 24\ 15\ 19\ 14$, respectively. Then, we repeatedly use the keyword CRYPTO to perform the following shifts

$$\begin{array}{cccccccccccc} & 0 & 5 & 18 & 15 & 10 & 18 & 19 & 25 & 4 & 22 & 12 & \\ - & 2 & 17 & 24 & 15 & 19 & 14 & 2 & 17 & 24 & 15 & 19 & \\ \hline \equiv & -2 & -12 & -6 & 0 & -9 & 4 & 17 & 8 & -20 & 7 & -7 & (\textbf{mod}\ 26). \\ \equiv & 24 & 14 & 20 & 0 & 17 & 4 & 17 & 8 & 6 & 7 & 19 & (\textbf{mod}\ 26). \end{array}$$

   Therefore, the original message is YOU ARE RIGHT.

2. Since the private keyword is not available, we need to use our knowledge of the English alphabet to try to break the cipher. The most common letter in the English alphabet is known to be the letter E. The most common letter in the name of the file is T, which appears in positions 6, 8, and 14. So we assume that the shift based encryption maps the letter E to the letter T.

   We are given the information that the private keyword is formed of two consecutive letters. Based on the assumption that the letter T ($\equiv 19$) is initially E ($\equiv 4$), we can can determine that one of the two letters of the keyword corresponds to $19 - 4 \pmod{26} \equiv 15 \pmod{26}$ in $\mathbb{Z}_{26}$, therefore the letter is P.

   Furthermore, since the letter T appears at the three even positions 6, 8, and 14, then we can infer that P is the second letter of the private keyword. Hence, the first letter is O since we are given the information that the private keyword is formed of two consecutive letters. Now similar to part 1, to decrypt the name of the file, we replace the words by their corresponding elements in $\mathbb{Z}_{26}$ and perform the following shifts

	17	23	6	17	5	19	7	19	0	15	7	22	6	19	11	15	0	
$-$	14	15	14	15	14	15	14	15	14	15	14	15	14	15	14	15	14	
$\equiv$	3	8	-8	2	-9	4	-7	4	-14	0	-7	7	-8	4	-3	0	-14	(**mod** 26).
$\equiv$	3	8	18	2	17	4	19	4	12	0	19	7	18	4	23	0	12	(**mod** 26).

   Therefore, the name of the file is DISCRETE MATHS EXAM.

3. It is better to use a long private keyword because it is more difficult to guess (or determine) longer keywords. So breaking the cipher would be harder when the keyword is long. In fact, if we use a random private keyword that is as long as the message, then the Vigenère cipher method is equivalent to the Shannon one-time pad scheme which is known to achieve perfect secrecy. Note that in the latter case, perfect privacy comes at the cost of privately sharing a keyword that is as large as the message itself.

Problem II: *(30 points)* The odds that a certain event will occur can be any non-negative real number. Assume that the odds of getting an A on this course can be calculated as the square of the time you spent to study divided by 36.

1. *(5 pts)* Give the function $f(t)$ that expresses the odds of getting an A as a function of the time t, $t \geq 0$, spent to study. What is the domain and codomain of f?

2. *(10 pts)* Given the odds of getting an A, is it possible to uniquely determine the amount of time spent to study? Justify your answer. If your answer is yes, express the time spent to study as a function of the odds.

3. *(10 pts)* Assume that the time you spent to study is equal to 2 to the power of the number of lectures ℓ ($\ell \in \mathbb{N}$) that you attended, plus a positive constant c. Give the function $g(\ell)$ that expresses the odds of getting an A as a function of the number of lectures attended ℓ. Is the function $g : \mathbb{N} \to \mathbb{R}^+$ invertible? Justify your answer.

4. *(5 pts)* Is it better to attend more lectures or less lectures if you want to increase the odds of getting an A? Justify your answer analytically.

Solution:

1. The function $f(t)$ is given by $f(t) = \frac{t^2}{36}$. The domain of f is $\mathbb{R}^+$ because the time t is a non-negative real number. The codomain of f is also $\mathbb{R}^+$ because the odds that a certain event will occur is a non-negative real number.

2. Suppose that the odds of getting an A is y, i.e., $f(t) = y$. $y = f(t) \Rightarrow t^2 = 36y$. Since $y \in \mathbb{R}^+$, the equation $t^2 = 36y$ has two solutions for t which are $t_1 = +6\sqrt{y}$ and $t_2 = -6\sqrt{y}$. However, $t_2 = -6\sqrt{y} \notin \mathbb{R}^+$, therefore the amount of time spent to study can be uniquely determined and is given by $t = +6\sqrt{y}$.

3. Let $h(\ell)$ be the function that expresses the time you spent to study as a function of the number of lectures ℓ that you attended. From the given, we have $h(\ell) = 2^\ell + c$. Therefore,

$$g(\ell) = f \circ h(\ell) = f\left(h(\ell)\right) = f(2^\ell + c) = \frac{\left(2^\ell + c\right)^2}{36}.$$

   $g : \mathbb{N} \to \mathbb{R}^+$ is not invertible because it is not onto, and thereby not a bijection. To prove that g is not onto, we can show that the element $0 \in \mathbb{R}^+$ in the codomain does not have a pre-image in the domain $\mathbb{N}$. Let $g(\ell) = 0 \Rightarrow 2^\ell + c = 0 \Rightarrow 2^\ell = -c$. This equation has no solution for ℓ because $2^\ell > 0 \ \ \forall \ell \in \mathbb{R}^+$, whereas $-c < 0$.

4. Consider $\ell_1 \in \mathbb{N}$ and $\ell_2 \in \mathbb{N}$ such that $\ell_2 > \ell_1$. Since 2^ℓ is an increasing function of ℓ, then

$$\begin{aligned} & 2^{\ell_2} > 2^{\ell_1} \\ \Rightarrow \ & 2^{\ell_2} + c > 2^{\ell_1} + c \\ \Rightarrow \ & \frac{\left(2^{\ell_2} + c\right)^2}{36} > \frac{\left(2^{\ell_1} + c\right)^2}{36} \\ \Rightarrow \ & g(\ell_2) > g(\ell_1). \end{aligned}$$

   Hence, $g(\ell)$ is a strictly increasing function in ℓ. Therefore, it is better to attend more lectures in order to increase the odds of getting an A.

Problem III: *(15 points)* Let $\{a_i\}$ and $\{b_i\}$ be the sequences defined by $a_i = 3^{-i} - 4i$ and $b_i = 2^{a_i}$, respectively, for $i \in \mathbb{N}$.

1. *(10 pts)* Determine an explicit formula for the sum $S_n = \sum_{i=0}^{n} a_i$.
2. *(5 pts)* Express the product $P_n = \prod_{i=1}^{n} b_i$ as a function of S_n.

Solution:

1. The sum S_n is given by

$$\begin{aligned} S_n &= \sum_{i=0}^{n} a_i \\ &= \sum_{i=0}^{n} 3^{-i} - 4i \\ &= \sum_{i=0}^{n} 3^{-i} - 4\sum_{i=0}^{n} i. \end{aligned}$$

   $\sum_{i=0}^{n} 3^{-i}$ is the sum of a geometric progression with ratio 3^{-1}. The explicit formula of the sum is given by

$$\sum_{i=0}^{n} 3^{-i} = \sum_{i=0}^{n} \left(\frac{1}{3}\right)^i = \frac{1 - \left(\frac{1}{3}\right)^{n+1}}{1 - \frac{1}{3}} = \frac{3}{2}\left(1 - \left(\frac{1}{3}\right)^{n+1}\right).$$

   $\sum_{i=0}^{n} i$ is the sum of an arithmetic progression, its explicit formula is given by

$$\sum_{i=0}^{n} i = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

   Therefore,

$$S_n = \frac{3}{2}\left(1 - \left(\frac{1}{3}\right)^{n+1}\right) - 4\frac{n(n+1)}{2} = \frac{3}{2}\left(1 - \left(\frac{1}{3}\right)^{n+1}\right) - 2n(n+1).$$

2. Note that $S_n = a_0 + a_1 + a_2 + \cdots + a_n$. The product P_n is given by

$$P_n = \prod_{i=1}^{n} b_i = \prod_{i=1}^{n} 2^{a_i} = 2^{a_1} \times 2^{a_2} \times \cdots \times 2^{a_n} = 2^{a_1 + a_2 + \cdots + a_n} = 2^{S_n - a_0} = 2^{S_n - 1}.$$

Problem IV: *(30 points)* Given that 31 is prime, consider the function $f : \mathbb{Z}_{31} \to \mathbb{Z}_{31}$, given by

$$f(x) = (3^{243}x^2 - 12x + \frac{4}{7}) \bmod 31.$$

1. *(15 pts)* Prove that $f(x) \equiv 27x^2 + 19x + 5 \pmod{31}$. Justify all your steps by stating which theorem(s) you used, and why are these theorem(s) applicable.
2. *(5 pts)* Verify that $(9x - 15)(3x - 17) \equiv f(x) + 2 \pmod{31}$.
3. *(5 pts)* Use Bézout's theorem to express $\gcd(9, 31)$ as a linear combination of 9 and 31; and $\gcd(3, 31)$ as a linear combination of 3 and 31.
4. *(5 pts)* Solve the congruence relation $f(x) \equiv 29 \pmod{31}$.

Solution:

1. To prove the equivalence relation we show that the coefficients of f are equivalent, i.e., we show that $3^{243} \pmod{31} \equiv 9 \pmod{31}$; $-12 \pmod{31} \equiv 19 \pmod{31}$; $\frac{4}{7} \pmod{31} \equiv 5 \pmod{31}$.

   (a) Since 31 is prime and 3 is not divisible by 31, we can apply Fermat's little theorem to obtain $3^{30} \equiv 1 \pmod{31}$. Now, we can write

   $$3^{243} \pmod{31} \equiv 3^{240}3^3 \pmod{31} \equiv \left(3^{30}\right)^8 3^3 \pmod{31} \equiv 1^8 3^3 \pmod{31} \equiv 27 \pmod{31}.$$

   (b) $-12 \pmod{31} \equiv -12 + 31 \pmod{31} \equiv 19 \pmod{31}$.

   (c) $\frac{4}{7} \pmod{31} \equiv 4 \times 7^{-1} \pmod{31}$, where $7^{-1} \bmod 31$ is the multiplicative inverse of 7 in $\mathbb{Z}_{31}$. The multiplicative inverse exists and is unique since 7 and 31 are relatively prime, i.e., $\gcd(7, 31) = 1$. The inverse of 7 can be determined using Bézout's theorem. We have that

   $$\begin{aligned} 31 &= 4 \times 7 + 3 \\ 7 &= 2 \times 3 + 1 \\ \Rightarrow \gcd(7, 31) = 1 &= 7 - 2 \times 3 \\ &= 7 - 2(31 - 4 \times 7) \\ &= 9 \times 7 - 2 \times 31. \end{aligned}$$

   Hence, $7^{-1} \pmod{31} \equiv 9 \pmod{31}$. Therefore,

   $$\frac{4}{7} \pmod{31} \equiv 4 \times 7^{-1} \pmod{31} \equiv 4 \times 9 \pmod{31} \equiv 36 \pmod{31} \equiv 5 \pmod{31}.$$

2. By expanding the expression on the LHS we obtain

   $$\begin{aligned} (9x - 15)(3x - 17) &\equiv 27x^2 - 198x + 255 \pmod{31} \\ &\equiv 27x^2 + 19x + 7 \pmod{31} \\ &\equiv 27x^2 + 19x + 5 + 2 \pmod{31} \\ &\equiv f(x) + 2 \pmod{31}. \end{aligned}$$

3. By using Bézout's theorem we can write the following

$$\begin{aligned} 31 &= 3 \times 9 + 4 \\ 9 &= 2 \times 4 + 1 \\ \Rightarrow \gcd(9, 31) = 1 &= 9 - 2 \times 4 \\ &= 9 - 2(31 - 3 \times 9) \\ &= 7 \times 9 - 2 \times 31. \end{aligned}$$

Similarly,

$$\gcd(3, 31) = 1 = -10 \times 3 + 31.$$

4. To solve the congruence relation $f(x) \equiv 29 \pmod{31}$, we replace $f(x)$ by 29 in part 2 to obtain

$$(9x - 15)(3x - 17) \equiv 29 + 2 \pmod{31} \equiv 0 \pmod{31}.$$

Therefore,

$$9x - 15 \equiv 0 \pmod{31} \text{ or } 3x - 17 \equiv 0 \pmod{31} \Rightarrow x \equiv \frac{15}{9} \pmod{31} \text{ or } x \equiv \frac{17}{3} \pmod{31}.$$

Hence,

$$x \equiv 15 \times 9^{-1} \pmod{31} \text{ or } x \equiv 17 \times 3^{-1} \pmod{31}$$

From part 3 we know that

$$9^{-1} \pmod{31} \equiv 7 \pmod{31} \text{ and } 3^{-1} \pmod{31} \equiv -10 \pmod{31} \equiv 21 \pmod{31}.$$

Therefore, the two solutions of $f(x) \equiv 29 \pmod{31}$ are

$$x \equiv 15 \times 7 \pmod{31} \equiv 12 \pmod{31} \text{ or } x \equiv 17 \times 21 \pmod{31} \equiv 16 \pmod{31}.$$

Problem V (BONUS): *(10 points)* The number of students in a school is between 500 and 600. If we group them into groups of 3, 1 student is left over. If we group them into groups of 5, 3 students are left over. If we group them into groups of 7, 2 students are left over. How many students are in this school? Justify your answer analytically.

Solution:

We need to determine the number of students x, $500 \leq x \leq 600$, that satisfies $x \equiv 1 \pmod 3$, $x \equiv 3 \pmod 5$, and $x \equiv 2 \pmod 7$. Note that $3, 5$, and 7 are pairwise relatively prime. Therefore, this problem can be solved using the back substitution method; or using Chinese remainder theorem.

Method 1: Back substitution

The first congruence $x \equiv 1 \pmod 3$ can be written as $x = 1 + 3t$, where t is an integer. Substituting into the second congruence yields $1 + 3t \equiv 3 \pmod 5$. Hence,

$$t \equiv \frac{2}{3} \pmod 5 \equiv 2 \times 3^{-1} \pmod 5 \equiv 2 \times 2 \pmod 5 \equiv 4 \pmod 5,$$

where $3^{-1} \pmod 5 \equiv 2 \pmod 5$ is the multiplicative inverse of 3 in $\mathbb{Z}_5$. So we can write $t = 4 + 5u$, where u is an integer. Substituting in $x = 1 + 3t$ yields

$$x = 1 + 3(4 + 5u) = 13 + 15u.$$

Next, we substitute into the third congruence and get $13 + 15u \equiv 2 \pmod 7 \Rightarrow 6 + u \equiv 2 \pmod 7$. Hence,

$$u \equiv -4 \pmod 7 \equiv 3 \pmod 7.$$

So we can write $u = 3 + 7v$, where v is an integer. Substituting in $x = 13 + 15u$ yields

$$x = 13 + 15(3 + 7v) = 58 + 105v.$$

Since the number of students is between 500 and 600, then $x = 58 + 105(5) = 583$ students.

Method 2: Chinese remainder theorem

Let $a_1 = 1, a_2 = 3, a_3 = 2$. Let $m_1 = 3, m_2 = 5, m_3 = 7$, and $m = 3 \times 5 \times 7 = 105$. From the proof of the CRT, we know that the solution of the congruence relations is given by

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3,$$

where $M_1 = m/m_1 = 35$, $M_2 = m/m_2 = 21$, and $M_3 = m/m_3 = 15$. Furthermore, $y_1 \equiv M_1^{-1} \pmod{m_1} \equiv 35^{-1} \pmod 3 \equiv 2^{-1} \pmod 3 \equiv 2 \pmod 3$. Similarly, $y_2 \equiv 21^{-1} \pmod 5 \equiv 1^{-1} \pmod 5 \equiv 1 \pmod 5$ and $y_3 \equiv 15^{-1} \pmod 7 \equiv 1^{-1} \pmod 7 \equiv 1 \pmod 7$. Therefore,

$$x \equiv 1 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \pmod{105} \equiv 163 \pmod{105}.$$

Since the number of students is between 500 and 600, then $x = 163 + 105(4) = 583$ students.