Name:

Directions:

Complete all eight questions.

Show your work. A correct answer without any scratch work or justification may not receive much credit.

You may not use any notes, calculators, or other electronic devices.

You have 75 minutes.

Problem 1: _____ / 13
Problem 2: _____ / 12
Problem 3: _____ / 13
Problem 4: _____ / 12
Problem 5: _____ / 13
Problem 6: _____ / 12
Problem 7: _____ / 13
Problem 8: _____ / 12

Total: _____ / 100
1. The following cipher text was produced using a shift cipher. Decipher it.

FBUQI UIXEM OEKHM EHA

One can break a shift cipher by brute force. We try all possible shifts to decipher the text and get

FBUQI UIXEM OEKHM EHA
GCVRJ VJYFN PFLIN FIB
HDWSK WKZGO QGMJO GJC
IEXTL XLAHP RHNKP HKD
JFYUM YMBIQ SIOLQ ILE
KGZVN ZNCJR TJPMD JMF
LHAWO AODKS UKQNS KNG
MIBXP BPRLT VLRQO LOH
NJQYQ CQFMU WMSPU MPI
OKDZR DRGNV XNTQV NQJ
PLEAS ESHOW YOURW ORK
QMFBT FTIPX ZPVSX PSL
RNGCU GUJQY AQWRY QTM
SOHDV HVKRZ BRXUZ RUN
TPIEW IWLSA CSYVA SVO
UQJFX JXMTB DTZWB TWP
VRKGY KYNUC EUAXC UXQ
WSLHZ LZOVD FVBYD VYR
XTMIA MAPWE GWCZE WZS
YUNJB NBQXF HXDAF XAT
ZVOKC OCRYG YEBG YBU
AWPLD PDSZH JZFCH ZCV
BXQME QETAJ KAGDI ADW
CYNF RFUBJ LBHEJ BEX
DZSOG SGVCK MCIKF CFY
EATPH THWDL NDJGL DGZ

The only one of these that is readable as English states “Please show your work”.
2. An affine cipher enciphers B as O and enciphers D as W. What letter does it encipher E as?

Since $B = 1$, $O = 14$, $D = 3$ and $W = 22$ we know that

$$22 \equiv 3 \cdot a + b \pmod{26}.$$  
$$14 \equiv 1 \cdot a + b \pmod{26}.$$  

Subtracting tells us that

$$8 \equiv 2 \cdot a \pmod{26}.$$  

At this point the majority of solutions continued by observing that $a = 4$ which means that $14 \equiv 4 + b \pmod{26}$, so $b = 10$. Hence E, which is 4, enciphers as $4 \cdot 4 + 10 \equiv 26 = 0 \pmod{26}$. This would give a final answer of A. However, this is wrong - $a$ can not be 4 since 4 is not relatively prime to 26. Those who did this got 6 out of 12 points.

Some noticed that 4 and 26 were not relatively prime and answered that this meant there was no possible answer. This was worth more than 6, but is still not correct.

Another possible answer for $a$ is 17. This can be found by observing that

$$8 \equiv 34 \pmod{26}.$$  

This means that

$$14 \equiv 17 + b \pmod{26},$$

and hence $b$ is 23 (or $-3$). So now E enciphers as

$$17 \cdot 4 + 23 \pmod{26} = 91 \pmod{26} = 13$$

which translates to N.
3. Use a keyword columnar transposition substitution cipher with keyword HOMOLOGY to encipher the plaintext GROUP.

We make the table as follows:

<table>
<thead>
<tr>
<th>H</th>
<th>O</th>
<th>M</th>
<th>L</th>
<th>G</th>
<th>Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
<td>F</td>
</tr>
<tr>
<td>I</td>
<td>J</td>
<td>K</td>
<td>N</td>
<td>P</td>
<td>Q</td>
</tr>
<tr>
<td>R</td>
<td>S</td>
<td>T</td>
<td>U</td>
<td>V</td>
<td>W</td>
</tr>
<tr>
<td>X</td>
<td>Z</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

We read down columns to put the letters in order and get a substitution table of

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| H | A | I | R | X | O | B | J | S | Z | M | C | K | T | L | D | N | U | G | E | P | V | Y | F | Q | W |

This gives us the cipher text “BULPD”.
4. Encipher the plaintext

DO NOT FORGET TO COUNT

using a keyword columnar transposition with keyword FOUND.

2 4 5 3 1
F O U N D

———
D O N O T
F O R G E
T T O C O
U N T

Reading the columns in the given order gives:
TEODFTUOGCOOTNNORT

Putting in extra characters in the last row is also correct and gives a slightly different answer depending on what you used.
5. The ciphertext ZBTWGAVH was produced by a Vigenère cipher with key HOT. Decipher it.

    ciphertext: Z B T W G A V H
    key word:   H O T H O T H O
    plaintext:  S N A P S H O T
6. Two fair dice are rolled. Find the probability that the number on one die is exactly one greater than the number on the other die.

There are six possible outcomes for each die, so there are $6 \times 6 = 36$ possible outcomes for the pair of dice. Outcomes that have one die exactly one greater than the other are (1, 2); (2, 3); (3, 4); (4, 5); (5, 6); (2, 1); (3, 2); (4, 3); (5, 4); and (6, 5). There are 36 possible outcomes, 10 of which have the property we are looking for, so the probability is $\frac{10}{36} = \frac{5}{18} \approx 0.2778$. 
7. The following ciphertext was produced using a Vigenère cipher, with a key of length less than ten. Find the length of the key used. (You do not need to recover the plaintext.)

KIVQX TCQQV RPQOS GWEKV MTRYN HJVUV VKBMD PKVHK WBUWF VZFNO PQOSG WEKVM TRYNH JGDPK OV

The string of characters “PQOSGWEKVMTRYNHJ” appears twice, starting at characters 12 and 51, respectively. One comes 39 characters after the other, so by the Kasiski test, the key length is almost certainly a factor of 39. The factors of 39 are 1, 3, 13, and 39. A key length of 1 would be a shift cipher, so that leaves a key length of 3 as the only other option.

Incidentally, the plain text was “If you want to solve this problem, try the Kasiski test. It will solve this problem easily.”

Using the Friedman test and then rounding to the nearest integer would also give the correct answer here. That was not the intended solution, as that would be much harder.
8. Is the composition of two Vigenère ciphers necessarily another Vigenère cipher? The first two ciphers do not have to have the same key, or even the same key length. Explain your answer.

Here is rough description of how this was graded. If you answered along the lines of “... a shift of a shift is a shift”, then you got about 6 points. If you also noticed that when keywords were not of the same length, then you would be shifting by different amounts and said no, it is not a Vigenère, then you got around 9 points. To get full credit you had to say that it is still a Vigenère, but the key length is now the least common multiple of the key lengths of the two key words. You also got full credit if you said the key length was the product of the two key lengths, as this is true (but not optimal).