1. (a)

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| T | | m | c | e | t | y | | e |
| h | a | a | h | s | | | a | r |
| e | r | n | o | | o | o | n | . |
| r | e | y | i | b | n | n | s | ■ |
| e | | | c | u | l | e | w | ■ |

(b)

$$\text{Number of shaded boxes} = \lceil n/k \rceil \times k - n$$

$$\text{Number of shaded boxes} = \lceil 43/5 \rceil \times 5 - 43 = (9 \times 5) - 43 = 2$$

(c) Plaintext = `There are many choices but only one answer.`

2. (a)

```
00010 10100 11001
x+x+x ++x+x xx++x
\-\|\ |-/-\ //--/
```

(b)

```
\-\|\ |-/-\ //--/
x+x+x ++x+x xx++x
+xx+x x++++ xxx++
??\|\ ?-?-? //?-?
+x\|\ x-+-+ //x-+
```

Bob needs Alice to tell him which of the filter selections he made were correct.

(c)

```
00010 10100 11001
\-\|\ |-/-\ //--/
x+x+x ++x+x xx++x
+xx+x x++++ xxx++
??\|\ ?-?-? //?-?
  010  0 0  11 0
```

final key: 01000110

(d) Alice and Bob can check for Eve's eavesdropping by setting aside cw anumber of bits of the key for verification.

(e) No, because photons cannot be observed without changing their polarity. The speed of computation has nothing to do with it.

3. (a) $IC = (4*3*2+3*2*1+2*1*5)/(30*29) = 40/870 = 0.046$

(b) 3 is the more likely keyword length. Evidence:

- more of the repeated trigram sequences have offsets divisible by 3
- the subsequences induced by key length 3 have higher avg IC

(c) BGH probably occurs by accident, since $91 = 7 \times 13$
None of the other repeated sequences have offsets divisible by 7, and only one, GHH, by 13.

(d) keyword: DNA

(e) `the novel feature of the`

4. (a) The cipher must be of a type in which the order of encryption and decryption operations does not matter. Such ciphers include Caesar, Vigenere, and one-time pad. It would not work with a substitution cipher which is "last on, first off".

   (b)
```
C1 = VWDDSD        C1 = m + a              b = C2 - C1        (mod 26)
C2 = WAWEWW        C2 = m + a + b          a = C2 - C3        (mod 26)
C3 = LMLTIL        C3 = m + b         m = C1 + C3 - C2        (mod 26)
```

   Alice's secret key $a$ = LOL
   Bob's secret key $b$ = BET
   Alice's message $m$ = KISSES

   (c) Since Alice is using Vigenere, C1 can be cracked using techniques like Kasiski Examination and IC/IMC.

   (d) *This question was withdrawn.*

5. (a) Public key: $(n = 15; e)$
   The possibilities are d = e = 3 or 5 or 7.

   (b) Private key: $(n = 15; d)$
   The possibilities are d = e = 3 or 5 or 7.

   (c)
```
B: M = 1  C = 1^3 mod 15 = 1
A: M = 0  C = 0^3 mod 15 = 0
C: M = 2  C = 2^3 mod 15 = 8
K: M = 10 C = 10^3 mod 15 = 10
[1,0,8,10]
```

   (d)
```
M = C^d mod n % = 12^3 mod 15 = 1728 mod 15 = 3 => 'D'
M = 12^3 mod 15 = 3 => 'D'
M = 12^5 mod 15 = 12 => 'M'
M = 12^7 mod 15 = 3 => 'D'
```

   (e)
   - The numbers are too small.
   - The public and private keys are identical.
   - The block size of 1 makes it a glorified substitution cipher.

6.
```
def ngramScore(decipherment, englishText, n):
    score = 0
    num_dictionary_ngrams = len(englishText) - n + 1
    # i is the start index of the n-gram
    for i in range(len(decipherment)-n+1):
        # Get the current n-gram
        gram = decipherment[i:i+n]
        # Get the frequency of the n-gram in the englishText text
        gram_freq = englishText.count(gram) / num_dictionary_ngrams
        # Update the score
        score += gram_freq
    return score
```

7. (a) Organize the words that share inflectional patterns:

| | Word A | Word B |
|---|---|---|
| Case 1 | $\perp \triangle \sqcap$ (i-de-mu) | $\bowtie \uplus \exists \sqcap$ (do-bi-ye-mu) |
| Case 2 | $\perp \triangle \mp$ (i-de-te) | $\bowtie \uplus \exists \mp$ (do-bi-ye-te) |
| Case 3 | $\perp \bowtie$ (i-do) | $\bowtie \uplus \in$ (do-bi-yo) |

(b) Which symbols represent the bridging syllables?

$\triangle$ (*de*) $\bowtie$ (*do*) $\exists$ (*ye*) $\in$ (*yo*)

(c) Organize the symbols into the grid below.

| | Vowel 1 | Vowel 2 |
|---|---|---|
| Consonant 1 | $\triangle$(*de*) | $\bowtie$ (do) |
| Consonant 2 | $\exists$(*ye*) | $\in$ (yo) |

(d) Suppose that the following words have been correctly deciphered:

$\bowtie \exists$ = doye $\uplus \mp$ = bite $\odot \uplus \sqcap$ = lubimu

Reconstruct the case endings for all three cases in the table below.

| | |
|---|---|
| Case 1 | -emu |
| Case 2 | -ete |
| Case 3 | -o |