Solutions to Math 135 Prelim #1

1. The correct answers are:

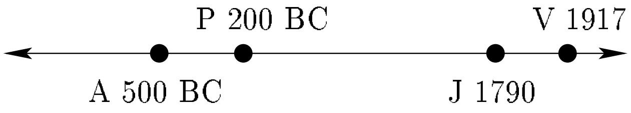
Vigenère Square	polyalphabetic substitution (PA)
Spartan Scytale	transposition (T)
Alberti's Cipher Wheel	polyalphabetic substitution (PA)
Atbash	monoalphabetic substitution (MA)

2. A *symmetric*, or private-key, cryptosystem is one in which two parties securely agree on a key for enciphering/deciphering. Any of the classical ciphers (Spartan scytale, Alberti's cipher wheel, Vigenère square, ...) gives an example of a symmetric cryptosystem. An *asymmetric* cryptosystem is one in which the two parties do not privately agree on key, but instead part of the key is made public. Security relies in the fact that it is computationally infeasible to determine the entire key. An example of such a system is RSA.

3. *Cryptography* is the art and science of concealing the content of communications between parties when the channel between them is controlled in some way by an unfriendly third party. In contrast, *cryptanalysis* is the study of methods for obtaining the plaintext from encrypted communications without access to the secret key originally used for encryption. *Cryptology* refers, in general, to the interplay between cryptography and cryptanalysis.

4. The uneducated Provenzano used the *Caesar shift* of +3 when he wrote cryptograms on little pieces of paper (known in Sicilian dialect as pizzini).

5.



6. In a cryptological context, *steganography* is the concealment of the very fact that there is a hidden message. The method of hiding the message could be as simple as writing on paper with "invisible ink," or it could be combined with another type of cipher. Bacon's bilateral cipher is an example of a cryptosystem which uses steganography (in addition to a substitution).

7. In a cryptological context, a *nomenclator* is a codebook, usually in two parts. The first shows how letters, words, and phrases are translated into code, and the second part provides the reverse look-up, namely which letters, words, and phrases correspond to a given code. The codes themselves can be transmitted either unencrypted, or encrypted with some other type of cipher.

8. An example of a cryptosystem which uses both substitution and transposition in its cipher is *ADFGVX.*

9. If $x = 3^{-1} \pmod 7$, then x is the smallest non-negative solution to the congruence $3x \equiv 1 \pmod 7$. This is equivalent to $3x - 1 \equiv 0 \pmod 7$. Noticing that -2 is a solution to the congruence, we conclude that $x \equiv -2 \pmod 7$ and so $x = 5$.

10. Since $8 = 0 \times 17 + 8$ we conclude $8 \operatorname{DIV} 17 = 0$. Since $-8 = -1 \times 17 + 9$ we conclude that $-8 \operatorname{DIV} 17 = -1$.

11. If $(5x + 1) \equiv (2x + 3) \pmod 8$, then subtracting $2x + 3$ from both sides of the congruence gives $3x - 2 \equiv 0 \pmod 8$. Noticing that -2 is a solution to the congruence, we conclude that $x \equiv -2 \pmod 8$ and so $x = 6$.

12. If we subtract $3a + b \equiv 5 \pmod 9$ from $5a + b \equiv 4 \pmod 9$, then we see that $2a \equiv -1 \pmod 9$. In other words, $2a + 1 \equiv 0 \pmod 9$. Clearly, 4 is a solution to this congruence and so $a \equiv 4 \pmod 9$. Substituting back into $3a + b \equiv 5 \pmod 9$ for a gives $12 + b \equiv 5 \pmod 9$ and so $b \equiv -7 \pmod 9$. Equivalently, $b \equiv 2 \pmod 9$.

13. If x denotes the plaintext numerical equivalent, and $y = E(x)$ denotes the ciphertext numerical equivalent, then in order to determine the plaintext message, we must compute $E^{-1}(y)$. If $y \equiv (9x + 1) \pmod{26}$, then $9x \equiv (y - 1) \pmod{26}$. Noticing that $9 \times 3 = 27$ and that $27 \equiv 1 \pmod{26}$, we see that $x \equiv 3(y - 1) \pmod{26}$ and so $E^{-1}(y) = 3(y - 1) \operatorname{MOD} 26$. Therefore,

cipher	F	B	W	X	Q	Q	M	B	W	W
y	5	1	22	23	16	16	12	1	22	22
$3(y-1)$	12	0	63	66	45	45	33	0	63	63
$3(y-1) \operatorname{MOD} 26$	12	0	11	14	19	19	7	0	11	11
plain	M	A	L	O	T	T	H	A	L	L

and so the plaintext is `MALOTT HALL`.

14. Since 4 and 26 are not relatively prime (sharing the common divisor of 2), we conclude that $E(x) = (4x + 7) \operatorname{MOD} 26$ does not define a valid affine cipher. For example, $E(12) = 55 \operatorname{MOD} 26 = 3$ and $E(25) = 107 \operatorname{MOD} 26 = 3$. On the other hand, since 7 and 26 are relatively prime, $E(x) = (7x + 4) \operatorname{MOD} 26$ does define a valid affine cipher.

15. When the ciphertext is written in $k = 19$ columns the plaintext can be read:

```
THE WOODS ARE LOVELY DARK AND DEEP
BUT I HAVE PROMISES TO KEEP
AND MILES TO GO BEFORE I SLEEP
```

This excerpt is from the poem *Stopping by Woods on a Snowy Evening* by Robert Frost.