MAT 302: LECTURE SUMMARY

0.1. **Administrative details.** We discussed the course webpage, prerequisites, marking scheme, collaboration and internet usage during assignments, schedule, office hours, and the textbook.

0.2. **The Big Picture.** Alice wants to communicate some private information to Bob. Trouble is, Oscar (the Opponent[1]) is listening in, and wants to intercept the information. Can Alice and Bob devise a means of communication so that the message arrives safely, without being understood or altered by Oscar? This is the motivating question of cryptography.

0.3. **Words and uses.** Cryptography, which comes from the Greek roots $\kappa\rho\upsilon\pi\tau o\zeta$ ("hidden") and $\gamma\rho\alpha\varphi\epsilon\iota\nu$ ("writing"), is the study of encryption and decryption algorithms. This is in contrast to cryptanalysis, which is the study of code-breaking. Some people (Paar and Pelzl among them) say that cryptography and cryptanalysis are two branches of a more general field, "cryptology". Personally, I find this word unappealing, since it could just as easily refer to the study of crypts.

Another word which will come up often in this course is "cipher". A cipher is any algorithm for encryption or decryption. The word derives from the Arabic word for zero, "sifr". (In fact, the English word zero is derived from this as well: the Arabic "sifr" became the Italian "zefiro" which became the Venetian "zero" and the French "zéro".) In most western languages other than English, the word meaning 'number' or 'digit' is derived from this Arabic root. (This is true in French, German, Greek, Italian, Polish, Romanian, Russian, Turkish ...)

0.4. **A couple of ciphers.**

(1) The ancient Greek Scytale ($\sigma\kappa\upsilon\tau\alpha\lambda\eta$, meaning "rod")

This cipher works as follows: Alice wraps a long strip of paper (or parchment or leather...) in a spiral around a rod, then writes a message, then unwraps the strip. The strip is then sent to Bob, who has a rod of the same diameter as Alice's. If Oscar sees the strip in transit between Alice and Bob, he will simply see a jumble of letters.

Unfortunately, appealing as this cipher is, it is not secure. In fact, one doesn't need a rod at all to decipher it! This was seen in class, when you easily decrypted the ciphertext

TSAOSHAMFSINPAASELMGIXEEE

(2) The Caesar (aka shift) cipher

Date: January 4th, 2011.

[1]Frequently, Evil Eve is used rather than Oscar the Opponent.

This cipher takes the alphabet and shifts it by some amount. For example, if we were to shift the English alphabet forward by four, then any occurrence of A in the original text would be replaced by E, B by F, C by G, etc.

This cipher is also not secure, since one only needs to check all possible shifts, and there aren't too many of these (26 for the English alphabet). We saw this in class when you decrypted the ciphertext

ECPAQWTGCFVJKU