

Student's Names:

Course Name: Linguistics 294L

Due in class M 21,W 23 May 2007

Teacher's Name: Chris Brew

Code design challenge

This is the final project for this class. Your task is to design a cipher system that strikes a good practical balance between security and usability. Since this is a complex multi-stage assignment, I first lay out the steps. The I give some advice about how to approach this. The overall goal is to develop your skills in executing and analysing cryptographic processes

The assignment

The set-up is the following:

- You will be working in groups of four or five. This is the smallest possible size, because I will need to split the group in two, and I do not want anyone working alone.
- Your first task is to design a cryptosystem that is reasonably secure. See below for a quick summary of the tools you have and the design considerations you will want to consider. The system must use some kind of simple shared secret (a key-word, key phrase or key number). I'll call this shared secret the key from now on.
- As a group, prepare a document that clearly describes the cryptosystem, giving enough detail that it will be possible for another group to understand and use the system, without further help. You should make two versions of the document. The first version not only describes the system but also gives two keys that can be used with it. Label the keys A and B. Version two is the same, except you don't give the keywords.
- On 21 May, we will trade system descriptions between groups. You will give feedback to the other group on (a) whether the write-up is clear enough for you to use (b) what you think of the cryptosystem itself. If the answer to (a) is "Not clear", then you may not be able to say much about (b).
- On 23 May, at the start of the class, I will split the groups in two and hand each half a message to be encoded. This will be about 200 characters in length. You will have 30 minutes to encode this message according to your cryptosystem. You need to check ahead of time that your system is efficient enough to allow you do this in the available time. When you are coding and decoding, the only external material you are allowed to refer to is version two of document that you created in the previous step. That is, you have to remember the keyword.
- Next, you will trade messages with the other half of your group, and decode. Again, you will have 30 minutes. Do not write directly on the cryptotext, because this is going to be photocopied and handed to another group after the class period is over.
- Next, I will collect in the coded and decoded messages, and you should use the remaining class time to reflect on what, worked, what didn't, and what you want to change. Maybe the system isn't as usable as you hoped. How will you fix it? The first part of the assignment for May 30th is to create a revised version of your document that fixes any problems that have emerged with the first go-round. Again you need two copies. One that just describes the system and one that additionally includes information about the shared secret

- Finally, I will give each group two 1000 character messages. Do not share this message with the other half of your group. Use your revised cryptosystem to encode the message and bring to class three sealed envelopes. The first envelope contains the cryptotext and the revised system description, but no keywords. This is for the other half of your group, The second envelope should be similar to the first, except that you must give two seven to ten-letter words from the message as a clue. The choice of these words is up to you, but you must give them, This envelope will be given to another group to try to break. The third envelope contains the cryptotext, and the revised system description, but this time the key information is provided. This is also for another group, but this time that group's task is to do an authorized decryption. This tests how usable the system really is.
- Each group now has three messages to work with. One is from the other half of your group. Decode it. A second is from another group, but with known key and system. Decode it. The third has a known system but unknown key. Try as hard as you can to break it. The final project report is a four page write-up of what you did with these three messages. It is due on June 6 (the Wednesday of exam week).

Design Considerations

You know about several kinds of cipher and several possible attacks on these ciphers. You also might be able to use ideas from the work on Korean, Linear B and Hieroglyphics, such as encoding words in syllables, or something similar. As long as you can explain it clearly in your system description, anything you choose to do is fair game.

Cipher types

Shift- Monoalphabetic - Polyalphabetic (e.g. Vigenere) - Polygraphic (e.g. Playfair, Beaufort) - Transposition.

You could use any of these, or a combination of one or more. The more complicated you make it, the harder it is going to be to use effectively under time pressure and the greater the risk of error. But if you can describe it, and you have tested it to see if you can use it, do what you want.

Attacks

Simple frequency analysis - frequency analysis on letter pairs or triples - use of possible words - use of tables of words and their patterns (as in the Army field manual approach to foursquare, or as in use of possible words in polyalphabetic).

You should say in your system description which features of your system are designed to defend against which types of attack, and explain why you think the system is going to be effective.

Step by step

You **MUST** include a detailed, step-by-step description of how the processes of encryption and decryption work. This needs to be good enough that another class member can do what you say.

