# Homework 5

## Due: Lesson 34

(50 pts)

**Help Policy**

**AUTHORIZED RESOURCES:** Any, except another cadet’s program.

**NOTE:**

* Never copy another person’s work and submit it as your own.
* Do not jointly create a program.
* You must document all help received from sources other than your instructor or instructor-provided course materials (including your textbook).
* **DFCS will recommend a course grade of F for any cadet who egregiously violates this Help Policy or contributes to a violation by others.**

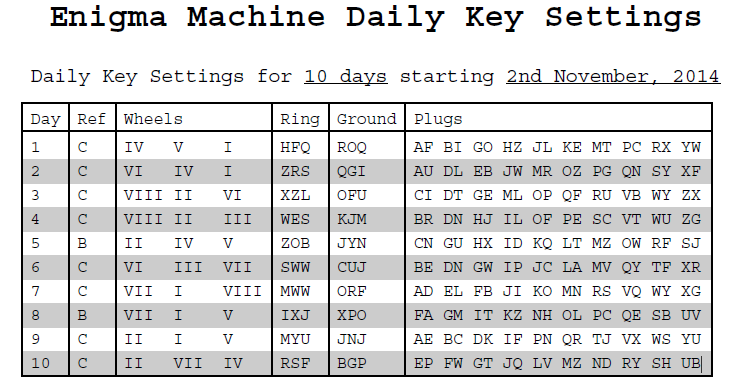
1. [5] Suppose Alice, Bob, and Carol want to establish a secret key for future

communications between all three of them. Describe and show how the Diffie-Hellman key exchange algorithm can be extended to work with three or more people.

1. [5] For the El Gamal public key cryptosystem, Bob chooses *p =* 43 and *α =* 19, and keeps secret ‘a’= 11. Alice keeps secret *k* = 25, and wants to send the message *M* = 40. Give Bob’s public key and the (*r,t*) pair Alice sends to Bob.
2. [5] In the El Gamal cryptosystem, Alice and Bob use *p* = 17 and *α =* 3. Bob chooses his secret to be ‘a’ = 6, so *β* = 15. Alice sends the ciphertext (*r*,*t*) = (7, 6). Determine the plaintext *m.*
3. [5] What are the odds two cadets in your squadron, in your same class year, have the same birthday? In your answer, be sure to include how many cadets there are in your class in your squadron and how you calculated your answer.
4. [10] You receive the following message on 6 Nov from your Cryptography teacher. You deduce that it was encrypted using the Enigma machine, and because your instructor is clever you’re certain she chose to use a message specific key. Use the emulator we used in class and the key table below to decrypt the message.

Cipher Text: FTDVF BCGTE A EOJQ HGDRK KA

(Bonus points for correct response-encrypted of course!)



If you would rather work with the real Enigma, you may do so in order to decrypt the following instead. The setup for the real machine is a little different: leave the rotors as they are situated (ie: do NOT attempt to remove them in order to re-order or set their tyre (ring) setting differently), the only plugs needed are the first three, and set the ground setting (rotor starting position as viewed from the top windows) as you would normally. The machine is wired to on already, so don’t worry about changing the power setting. If you have any questions/doubts please ask me!

Cipher text: YGJCC TBKCB OSMQI BSMJZ KM

1. [20] You are charged with decrypting intercepts from a two-rotor Enigma machine with a 4-letter alphabet {A,B,C,D}, encrypted with a two-letter day key. Intelligence has provided you with a working copy of the machine used to encrypt the intercepts, which you can see has fixed rotor order and no plugboard. Engineering reports that they have tested the rotors, and that if set to the AA position they permute in the following way:

Rotor 1: Rotor 2:

+0

+1

+1

+2

+2

+2

+3

+1

Output numbers increase from top to bottom, addition is relative to the current input and wraps around to the beginning. For example, for inputs A-B-C-D labeled top to bottom, rotor 1 implements the substitution cipher {A🡪C, B🡪D, C🡪B, D🡪A}. Similarly, rotor 2 implements {A🡪A, B🡪C, C🡪D, D🡪B}. Together in the position above, they implement {A🡪D, B🡪B, C🡪C, D🡪A}.

Each time a letter is encrypted, rotor 1 turns one position, which corresponds to the numbers shifting up and the top number moving to the bottom. Thus after encrypting one letter, rotor 1 would look like:

+2

+3

+1

+2

When D is at the top of rotor 1 and the rotor then turns one position, rotor 2 also turns one position.

* 1. How many substitution ciphers can this machine cycle through before repeating?
  2. How many rotor settings are possible?
  3. How many message keys are possible?
  4. Suppose the daily key is “AA”. What substitution ciphers are implemented for the first six letters of ciphertext (ie: what would all 4 letters encrypt to at each rotor position)?

1st cipher: DBCA (already given)

2nd:

3rd:

4th:

5th:

6th: