Antonin Thioux (s3791378) & Xiaoyu Guan (s3542807)

1.

Solution:

- AUP link: https://www.rug.nl/society-business/centre-for-information-technology /security/aup/
- Ordinary user have the responsibilities to: not use others accounts, not copy software, not use the system for commercial use, keep password secret, report holes in security and only play games when no one is waiting to use a computer.

  System manager, have the same responsibilities as ordinary users however they must also ensure that; software and hardware is available, that the system is secure, traffic is only monitored automatically, information about traffic is destroyed, not to exploit confidential information.

  Given the correct circumstances system managers can also inspect accounts.
- Ground-rule: The users of the university computer systems may not endanger these systems, nor may they hinder other users.
- Change password at least once a year.

  Don't type password when someone is watching you type.

  Do not use personal info in password.

  Mix upper/lower case letters, digits and punctuation when constructing a password.
- Unauthorized use of other person's account.

  Using the software that obtained illegally on university computer system.

  Commercial used of university computer system with no proper authorities.

  Playing games on the university computer system when other people need it in urgent.
- Suspect will be informed by the board of the faculty about investigating

  Suspect will be restricted or suspended to wait for the investigation
- The Suspect may file an objection with the chair of their department.

2. See code on Themis.

3.

Solution:

1. For shifting encryption there are 26 possibilities because there are 26 letters are allowed (from 'a' to 'z') and anyone of those letters can be the first letter.

   For mapping encryption there are 26! because the alphabet can be mixed.
2. No. All mapping and shifting encryption can be decoded with a single mapping of a special alphabet. This is because if you start with the regular English alphabet applying all shifts

and mappings on this alphabet one at a time will get you a new mapping which can be use to encrypt and decrypt the message in a single step. Because this mapping also has 26! possibilities to arrange the letters hence the difficulty to break doesn't change.

3. Yes, encryption function can be also used for decryption.

   Implement: As the definition of encryption and decryption, encryption is from plaintext to ciphertext and decryption is to recover the ciphertext to plaintext and then we can know that the number of shift will be the same. What need to do in decryption is to minus the number of shift to get the plaintext, and then we can modify the encryption function such that change the value of shifting to it negative value (e.g 2 to -2) and since minus operation dealing with the negative index issue is needed.

4. See code on Themis.

5. See code on Themis.